cover story
By Megan Gates

PERIMETER
PROTECTION
FAKE NEWS
FALLING FOR
EMPLOYEE
MONITORING
TELEWORK
Vulnerabilities
Should governments share information with the private sector?

Problem:

Human Trafficking
Smuggling people over borders can turn deadly.

Solution:

34
FALLING FOR
FAKE NEWS

24
EMPLOYEE
MONITORING
42
TELEWORK
48
PERIMETER
PROTECTION

Issue & Beyond
FRANK ARGENBRIGHT, SECURITY GUARD WANNABE
$1,000,000
CHARITY CHALLENGE:
SECURITY GUARD “TAP OUT”

To: “The Big Four” Man-Guarding Companies in the US

In my last ad, I challenged the owners (or CEOs if company is owned by private equity) of the Big Four man-guarding companies to a “Security Guard Tap Out” for charity. They were to pick their toughest guard post anywhere in the US, and then we would put on uniforms and stand guard until one of us taps out or walks off the post. Whoever taps out first has to donate $250,000 to the charity of the winner’s choice.

As of publication, none of the 4 CEOs contacted me. I know they were all busy working the ASIS Conference in Dallas. I am hoping they will call me in the next couple of weeks. I ask any of the customers who use the Big Four man-guarding companies to put in a word for me and see if we can get one of the CEOs to take me up on my challenge.

Again, this security guard tap out will be fun. It will take us back to our roots and remind us of the core of our business. It will show our security officers that they truly are the most important people in our companies. It will show our customers where our priorities truly lie. And lastly, it will raise $1,000,000 for charity!

For the first 5 customers that will call the CEOs that you do business with and ask him if he will help raise money for charity, I will donate $1000 to the charity of your choice.

I am still waiting to hear back from the 4 CEOs. Please accept my challenge for fun and a great cause. You can call me on my cell at 404-536-1140. And yes, that is my actual cell phone number!
Cybersecurity?

Buckle up.

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

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

Visit axis.com/about-axis/cybersecurity and find out how to stay protected!
“The most engaged workers were those who spent 60 to 80 percent of their week working from home.”

Findings from the 2017 Gallup report, The State of the American Workplace. PAGE 47

“They will look for rest stops and other areas that are not well lit, without visible security.”

On the modus operandi of human traffickers. PAGE 15

If all the countries with capabilities to collect vulnerabilities had a policy of leaning toward disclosure, it would be valuable to the protection of critical infrastructure and consumers alike, as well as U.S. corporate interests.

Cyber experts Ari Schwartz and Rob Knake on government sharing of network vulnerabilities. PAGE 31
ACHIEVE THE HEIGHTS OF SUCCESS

Partner.Win.

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

#PartnerWin

hikvision.com
MANAGING THE FUTURE IS FLEXIBLE
Effectively managing a teleworking program can be a strategic way to boost your firm’s retention and engagement while improving employee satisfaction.
By Mark Tarallo

PERIMETER PROTECTION THE UNSEEN THREAT
When conducting a facility threat assessment, inspectors must consider both physical perimeters and electronic perimeters to prevent soft target vulnerabilities.
By Ernie Hayden, PSP

FAKE NEWS, REAL THREATS
While primarily political in nature, fake news has been used against various institutions and poses a real and increasing threat to private sector organizations of all sizes.
By Jeremy E. Plotnick

On the Cover:
Illustration by Michael Austin
FREE PRODUCT INFORMATION

USE YOUR SMARTPHONE AND SCAN THE QR CODE TO REQUEST INFORMATION ON ANY AD IN THIS ISSUE

SECURITY MANAGEMENT
New online this month: the transfer of military equipment to police, and hacking election infrastructure.

Can you spot a fake?

Employee monitoring helps a restaurant owner reduce theft.

Should governments report network vulnerabilities to the private sector?

ASIS presents annual awards.

Thwarting human traffickers and ensuring fair elections.

U.S. courts rule on data breaches and security officer liability, while a new Russian law restricts the use of anonymous messaging apps.

ASSA ABLOY helps protect U.S. Bank Stadium, home of the Minnesota Vikings.

Measuring risk perception around the globe.

NOVEMBER 2017
SECURITY MANAGEMENT

EDITORIAL STAFF
Teresa Anderson
teresa.anderson@asisonline.org
Mark Tarallo
mark.tarallo@asisonline.org
Megan Gates
megan.gates@asisonline.org
Holly Stowell
holly.stowell@asisonline.org
Lilly Chapa
lilly.chapa@asisonline.org
Flora Szatkowski
flora.szatkowski@asisonline.org

PRODUCTION & CREATIVE SERVICES STAFF
Tyler Stone
tyler.stone@asisonline.org
Keith Schilling
keith.schilling@asisonline.org
Caitlin Donohue
caitlin.donohue@asisonline.org
Molly Fu
molly.fu@asisonline.org
Matthew Kreider
matthew.kreider@asisonline.org
Jeremy Orloski
jeremy.orloski@asisonline.org

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

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

LEGAL REPORT
U.S. courts rule on data breaches and security officer liability, while a new Russian law restricts the use of anonymous messaging apps.

INDUSTRY NEWS
ASSA ABLOY helps protect U.S. Bank Stadium, home of the Minnesota Vikings.

MARKETPLACE

ADVERTISER INDEX

SNAPSHOT
Measuring risk perception around the globe.

CHECK OUT MORE ONLINE at www.securitymanagement.com
FAKE NEWS TECHNOLOGY
In a Vanity Fair article, Nick Bilton writes about new technologies that can change audio and video in the same way that photos can be altered. He fears that “governments can weaponize fake news.” The article includes videos that show these technologies in action.

SEEING=BELIEVING
Humans are predisposed to believe fake news. A Yale University study found that even one exposure to a false news story predisposed the reader to believe that the story was true. The more times the reader was exposed, the more he or she believed it. Another study uncovered a tendency to believe clearly untrue information, even if the reader previously knew that the information was false.

MILITARY SUPPLIES
Investigators posing as a fictitious federal agency were able to acquire excess military equipment, and the U.S. Defense Department needs to do more to track equipment it provides to Iraq.

DRIVER TESTING
The Federal Motor Carrier Safety Administration and Federal Railroad Administration withdrew a proposed rule to require truck drivers and train operators be tested for sleep apnea.

DISCLOSURE
In Government’s Role in Vulnerability Disclosure: Creating a Permanent and Accountable Vulnerability Equities Process, experts recommend that the United States formalize the process it uses to disclose cyber vulnerabilities.

SECURE ACCESS
A study conducted among IT professionals explores organizational security threats. Among its findings, The Secure Access Threat Report 2017 from Bomgar reveals that while 90 percent of security professionals trust employees with privileged access most of the time, only 41 percent have “complete trust” in those users.

DATA BREACHES
The heightened risk of future identity theft is sufficient to show standing to sue at the pleading state in a lawsuit, a U.S. court of appeals ruled.
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.
Humans are predisposed to believe fake news. In August 2017, researchers at Yale University released a study finding that even one exposure to a false news story, such as on a Facebook feed, predisposed the reader to believe that the story was true. The more times the reader was exposed, the more he or she was sure the information was accurate. This phenomenon held even if the story was clearly labeled as questionable. The study illustrates the concept of illusory truth. Well known to researchers since the 1970s, this tendency to believe clearly untrue information is at play even if the reader previously knew that the information was false.

Advancements in computer software might soon erase the line between truth and lies. Current controversy swirls around written material online, but audio and video editing technology could make it impossible to believe anything you read, hear, or see.

On a recent episode of the Radiolab podcast, Producer Simon Adler discussed VoCo, a new audio manipulation software developed by Adobe. Dubbed “photoshop for audio,” the new technology needs only 20 minutes of a person’s speech to recreate the person’s voice. Software puts up a transcript of the audio recorded. Then by changing the text, the speaker’s words change. The words can be rearranged and they can also be altered. These new words, which were never actually uttered by the speaker, are transmitted in the speaker’s voice.

Another new software product, Face2Face, does similar things to video. The software tracks facial expressions on an existing video and can then transpose the expressions of the software operator onto the person in the video. With this software, anyone can alter the video of a real event. For example, a user can take a video of Barack Obama giving a speech to Congress and alter it to contain nothing but golf references. The viewer sees Obama speaking and hears Obama’s voice, but it’s all fake.

“If you join the video manipulation with VoCo voice manipulation,” Adler emphasizes, “you are the ultimate puppeteer. You can create anyone talking about anything you want in their own voice.”

This technology is especially dangerous in a time when the news is already manipulated by state actors. In his article in Vanity Fair, “Fake News Is About to Get Even Scarier than You Ever Dreamed,” Nick Bilton writes that this new technology means that “governments can weaponize fake news as an act of digital terror.”

An optimist might argue that watermarking and other detection techniques will be employed to tag altered audio and video. The public, meanwhile, will be armed with the knowledge that manipulation exists, making everyone more skeptical than before.

A realist might argue that the future of news is its past. Soon, the only reliable information will be written and produced by trusted sources and delivered to your doorstep. In print.
Mobile Access for Increased Productivity

The open platform of Pro-Watch® 4.3.5 integrates seamlessly with third-party systems, while the latest identity management and mobile credential enhancements provide greater efficiency, productivity and a superior user experience. Plus, the new Android mobile app lets users manage time-sensitive access rights, control doors and more—anytime, anywhere.

Build on the possibilities at http://hwll.co/pro-watch.

© 2017 Honeywell International. All rights reserved.

For product info #6 securitymgmt.hotims.com
A particularly horrid example of this came about last July, when authorities found the gruesome results of a criminal smuggling enterprise: 39 undocumented immigrants, nine dead (a tenth died later) and the rest needing hospitalization, lying in a tractor-trailer parked at a Walmart in San Antonio, Texas. The trailer had contained an estimated 70 to 200 illegal aliens total during its journey, according to court records.

A few weeks later, U.S. Immigration and Customs Enforcement (ICE) officials reported that the San Antonio incident was only one of four that had occurred in nearby areas, all within a few weeks’ time. Although the other three did not involve loss of life, they were still disquieting; in one of the incidents in July, border agents in Laredo, Texas, found 72 people from Mexico, Ecuador, Guatemala, and El Salvador locked inside a trailer. Border security leaders pledged to fight the problem.

“This horrific crime...ranks as a stark reminder of why human smuggling networks must be pursued, caught and punished,” ICE Acting Director Thomas Homan said after the San Antonio incident. “[ICE] works year-round to identify, dismantle, and disrupt the transnational criminal networks that smuggle people into and throughout the United States. These networks have repeatedly shown a reckless disregard for those they smuggle.”

How do these human smuggling operations work? Often, the process begins a few months before the smuggling, in a country such as Mexico, Guatemala, or Honduras, where sizable numbers of people are looking to emigrate, according to an investigation and review of court
An increase in human smuggling activity could have ramifications for supply chain security.

documents by the Associated Press. Those seeking to cross the border get to the Mexican–U.S. border region, and then cross by foot or river raft. They are then picked up by a tractor trailer somewhere past the border. The stressful traveling conditions make them vulnerable—dehydration, hyperthermia, and asphyxiation have been among the causes of death in truck cases.

One analyst, the U.K.-based global risk firm Verisk Maplecroft, warns companies that an increase in human smuggling activity could have ramifications for supply chain security. “Under the Trump administration, businesses with supply chains that rely on low-skilled, temporary migrant labour will face increasing risks of modern slavery in their workforce,” the firm says in one of its risk reports for 2017.

Verisk Maplecroft outlines the risk involved as follows. The construction of a U.S.–Mexico border wall, or stricter enforcement of deportation rules, will not reduce the appeal of migration for thousands of Latin Americans. But it could increase trafficking costs and deepen migrant worker debt, making migrants more vulnerable to exploitation. Suppliers in agriculture, construction, manufacturing, hospitality, and transport would be most exposed to supply chain risk.

Emigration-related schemes are not the only form of human smuggling that ICE and its allies are fighting. Human trafficking for the purposes of coerced sex trade operations also continues—a practice that groups like Truckers Against Trafficking (TAT) are trying to help eradicate.

The group, a 501c(3) nonprofit, takes an all-hands-on-deck approach and partners with members of the trucking and truck stop industries, law enforcement officers, and trafficking survivors to fight human trafficking. The group’s educational efforts include a 36-minute video that offers an overview of the trafficking issue, as well as four-hour training sessions for law enforcement officers such as the state highway patrol, according to Kylla Lanier, deputy director and cofounder of TAT.

Included in this training are case studies from officers who stopped a truck for a violation, and then upon closer inspection detected a trafficking incident. In the case studies, officers give a breakdown of the indications that tipped them off, and offer advice and best practice guidance for other officers.

For example, the passengers in the truck may exhibit some telling signs and behaviors, Lanier explains. “If the passengers are young, are they afraid to look at you? Are they acting like normal kids, or are they looking really scared?” she says. Sometimes, the passengers may have branding tattoos or bruises from physical abuse, and may be carrying many hotel key cards. Officers who speak with the driver and passenger separately sometimes find out that their respective stories do not match, or even make much sense.

Traffickers also exploit locations as well as victims, she adds. They will look for rest stops and other areas that are not well lit, without visible security, and which have a captive audience of drivers rolling through. “That’s where they will bring their victims to,” she says.

BOOK REVIEW

BULLY-PROOF WORKPLACE

BY PETER J. DEAN AND MOLLY D. SHEPARD. McGraw-Hill; mhpprofessional.com; 320 pages; $25.

UNDERSTANDING the impact of workplace-related violence and having the knowledge to take a proactive and organized approach to mitigating it is essential for any security leader. Workplace violence comes in many forms. In The Bully-Proof Workplace, authors Peter J. Dean and Molly D. Shepard focus on the specific issue of bullying behavior and how it negatively impacts the work environment. The underlying premise of the book is that bullying behavior can and does occur at all levels of an organization, and that this behavior is just as psychologically and emotionally damaging to workers in a business setting as it is to students in a school environment.

The book examines four types of bullies—Belter, Blocker, Braggart, and Brute—and the behaviors they exhibit. It provides recommendations for proactively identifying these individuals, plus strategies on how to counteract the impact of these behaviors in the workplace. The authors cite numerous data sources and case examples that support their assertions.

Many security leaders will find the information in this book helpful because it builds upon and amplifies information that is widely available from many sources in terms of workplace related-violence trends over the last several years. It would be useful for HR professionals, managers, and employees dealing with a workplace bully. New security leaders who are looking to build their knowledge base regarding workplace violence issues, as well as seasoned security leaders, will find the information relevant and timely.

REVIEWER: Keith G. McGlen, CPP, CHPA (Certified Healthcare Protection Administrator) is the associate vice president of system security services for the Memorial Hermann Health System in Houston, Texas. A proven security leader with more than 28 years of experience in healthcare settings, McGlen is a member of the ASIS International Healthcare Security Council.
explains. TAT works with truck stop industry partners to help make their facilities more safe and secure.

TAT also works closely with sex trafficking survivors; the group has two on staff. Survivors are key in the antitrafficking movement, because they can change perceptions about the sex trade. Prostitution is “a vicious evil system” that has been whitewashed as a victimless crime, Lanier says, in part through unrealistic portrayals like the movie *Pretty Women*. In reality, the vast majority of those in the trade are being prostituted against their will, in hotels, motels, and rest areas, and are “cruelly raped and beaten within an inch of their lives,” she explains.

“It’s not the oldest profession,” Lanier says, “it’s the oldest oppression.” One study found that the rate of post traumatic stress disorder among prostitutes is equal to that of war veterans, she adds.

Given this, having the survivor’s voice in the issue is vitally important, because they can discuss the victim’s experience and point of view and “what’s going on behind the scenes,” Lanier explains. So, when people assume the survivor turned to prostitution to support a drug habit, the survivor can tell them it was just the opposite—being forced into the sex trade made the victim turn to drugs and alcohol.

Such compelling stories from survivors have helped the antitrafficking cause spread awareness, and the cause has made inroads. And on the legislative front, other advocacy groups such as Polaris pressured the U.S. House of Representatives into reauthorizing the Trafficking Victims Protection Act, which was created in 2000, in July 2017.

But in the end, demand for prostitution needs to be reduced so that further inroads can be made, and that will take “a societal paradigm shift,” Lanier says.

SECURING ELECTIONS

THE RUSSIAN HACKING of the U.S. 2016 presidential election was an “assault” on election infrastructure, and it likely augurs a greater attack in the 2018 or 2020 elections, says a former director of the CIA.

“I am confident the Russians will be back, and that they will take what they have learned last year to attempt...
FOR US, life safety and security door hardware isn’t just a job. We live, breathe and even sleep this stuff. That’s why your Detex tech support team is ready to address any installation question, or solve your unique troubleshooting issues quickly and thoroughly. Whether you need guidance with a challenging installation, are inquiring about training or want help making a hardware decision, we’ll tackle any issue you can imagine. Just call 800-729-3839.

When she sleeps, she dreams of panic hardware.

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

For product info #8 securitymgmt.hotims.com
to inflict even more damage in future elections,” writes James Woolsey, former CIA director, in the foreword to a recent report, *Securing Elections from Foreign Interference*, issued by the Brennan Center for Justice at the New York University School of Law.

Some members of the U.S. Congress hold similar views. The two cochairs of the Congressional Task Force on Election Security, Rep. Bennie G. Thompson (D-MS) (who is also the ranking member on the Homeland Security committee) and Rep. Robert Brady (D-PA) say that Russia’s targeting of voting infrastructure in at least 21 states was a direct attack on our democracy. “We are taking the steps to begin an investigation into what we can do to secure our election infrastructure and prevent what transpired last year from happening again,” Thompson and Brady said in a joint statement.

The task force was formed earlier this year. It will serve as a forum for members of Congress to hear from election infrastructure experts on physical security and cybersecurity challenges, and identify actions that should be taken to guard against future attacks.

In the meantime, the Brennan Center report also offers specific actions that Congress and local election officials can take to protect future elections from continued foreign interference. The report’s recommendations include:

**Replace antiquated voting machines with new, auditable systems.** For example, the Brennan Center recommends that states and counties replace the old direct-recording electronic voting machines that are still used in 14 states around the country.

**Conduct audits of paper ballots.** Currently, only 26 states require that election officials conduct post-election audits of paper records. The Brennan Center recommends that all of them do.

**Support the Election Assistance Commission.** Since 2005, the EAC has helped increase the reliability of voting machines by setting standards and providing guidance for electoral systems and their security.

**Adopt general security best practices.** Many of the security problems facing election systems are similar to those facing other large distributed systems, for which there are already well-established security protocols.

**Harden database systems by updating threat awareness.** Many experts agree that the first step that governments should take in securing voter registration systems is to regularly identify the potential avenues for attack, mapping out all of the entities that interact with a particular voter registration system, and developing mitigation strategies where weaknesses are identified.

**SUSPECT ACTIVITY**

The five top predicate offenses behind suspicious transaction reports filed with Financial Intelligence Units in the European Union from 2013 to 2014

<table>
<thead>
<tr>
<th>SUSPECT ACTIVITY (%)</th>
<th>0</th>
<th>20</th>
<th>40</th>
<th>60</th>
<th>80</th>
<th>100</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tax Fraud</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Cybercrime</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Drug Trafficking</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Fraud and Swindling</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Corruption</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

**SOURCE:** From Suspcion to Action, EUROPOL, July 2017

**SECURITY JOBS AND CAREER CENTER**

https://securityjobs.asisonline.org

The first step...is to regularly identify the potential avenues for attack.
• Our exclusive canopy options fit single, multiple or space-saving double units.
• Power assist is activated with a slight push and adjusts to the speed of the individual entering the turnstile.

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

Setting boundaries makes access in life smart and secure.

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

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

For product info #10 securitymgmt.hotims.com

Set your boundaries.
The U.S. Department of Defense (DoD) Law Enforcement Support Office (LESO) program was reined in by then President Obama in 2015 after a spate of killings by police sparked public outrage.

Law enforcement agencies could still acquire medical supplies, training devices, protective gear, and some lethal weapons through the reduced LESO program, but the full range of excess military equipment was unavailable.

The program has been fully reinstated. Concerns about the program’s ability to properly disseminate the military equipment were raised even before Trump expanded the policy. While investigating the LESO program, a congressional watchdog agency stumbled upon an “ineligible entity” that had categorized itself as a federal agency and successfully gained access to military equipment. The U.S. Government Accountability Office (GAO) notified DoD and learned that the case was already being investigated.

But at one point the entity had been approved to use the LESO program. So in late 2016, GAO decided to figure out how this happened by creating its own fraudulent federal agency and applying to the LESO program. The investigation ended up going much further than researchers initially expected.

“We noticed that one of the participants in the program had a somewhat unusual name, and we weren’t aware of a federal agency having that particular name,” explains Zina Merritt, director of GAO’s Defense Capabilities and Management Team. “We kept looking at the processes through which DoD provided this

Federal, state, and local law enforcement agencies will soon have their pick of surplus U.S. military gear, including grenade launchers and high-caliber weapons, after U.S. President Donald Trump rolled back an Obama-era action curtailing the transfer of military equipment to police.
equipment to federal agencies, and we decided that it would be appropriate to task the internal controls through using our investigative capabilities to see how vulnerable the program potentially was.”

The Defense Logistics Agency (DLA) manages the LESO program, which has provided more than $6 billion in excess DoD property to more than 8,600 agencies since 1991. While GAO was investigating the program, before Trump expanded access to equipment, about 4 to 7 percent of the property was sensitive and could not be released to the public. GAO has studied the LESO program before, and upon the most recent review found that most policy enhancements had occurred at the state and local level; few had been made in regard to federal agencies.

GAO researchers submitted a fake application that included a fictitious agency name, number of employees, point of contact, and physical location. They were surprised when, in early 2017, the nonexistent agency was approved to participate in the LESO program.

“We thought they would have noticed that our Web address was not a .gov address,” Merritt says. “We thought they would probably call us and verify some of the information, and they did not—correspondence was mostly by email. They asked us for the statute that our Web address was not a .gov program. They were surprised when, in mission and procedures allowed information about the perpetrator to slip through the cracks. Instead of capturing warning signals, the systems scattered them.

Similar lessons were learned from the post-9/11 anthrax attacks in the United States. The author says that the suspect gained access to anthrax through “a complicated mix of evolving regulations, organizational culture, red flags ignored, and happenstance.”

A real strength of this book is its root-cause analysis approach. Blame is rarely laid at the feet of incompetent people, but assigned to factors like the unintended consequences of organizational design and known psychological tendencies.

The last chapter brings together all the lessons learned and cites 10 worst practices. For example, number seven is: “Forget that insiders may know about security measures and how to work around them.” This chapter will be the most valuable to security practitioners because it offers a roadmap towards building an insider threat mitigation plan.

Insider Threats is well-written, even literary. Its chief lesson: organizations are rarely designed to catch the insider, and much work needs to be done to protect them.

Merritt notes that in the midst of the GAO investigation, however, DLA officials had already begun to strengthen the LESO application process.

“They were creating memorandums of understanding with the federal agencies applying; that’s something they didn’t have prior,” Merritt tells Security Management. “However, they just had not gone a step further to actually have federal coordinators for the federal participating agencies. That’s a step they did after we completed the review.”

Following the GAO report’s release in July, Merritt testified before a U.S. House of Representatives subcommittee about the findings and further recommendations, including revising procedures for
Merritt has seen other improvements to the program already, including in-person visits to LESO-involved agencies and making sure applicants are eligible to take part in the program.

“I think now, at least with the process of applications, they are ensuring they’re legitimate agencies—that’s where the principal breakdown was,” Merritt explains. “The first step was at least having better oversight and processes to prevent entities that were not eligible to participate to gain access in the first place.”

The flow of military equipment isn’t just a problem in the United States. DoD runs another program that provides military equipment to Iraqi security forces, including the Kurdistan Regional Government forces, to fight ISIS.

Since 2015, about $2 billion in equipment, such as weapons and vehicles, was funded through the Iraq Train and Equip Fund (ITEF), sent overseas, and transferred to the governments. However, another GAO report found that the transfer of equipment has not been properly documented due to data reporting and interoperability issues.

The report, DoD Needs to Improve Visibility and Accountability Over Equipment Provided to Iraq’s Security Forces, looks at how DoD tracks the status of the equipment from acquisition through transfer to foreign governments.

Jessica Farb, director of internal affairs and trade at GAO, tells Security Management that personnel were not properly using the Security Cooperation Information Portal (SCIP), a Web-based tool that tracks the equipment flow.

“What we found was that by not using the SCIP, which is not just for Iraq but all cooperation matériel that we provide to partnered nations, DoD broadly could not have complete visibility and be able to account for everything that was going on because the system had missing information,” Farb says.

Of the 566 requisitions marked complete that GAO studied, fewer than half had the arrival date of the equipment at the point of departure in the United States recorded, and none had information on when the equipment was shipped from the United States, when it arrived in Kuwait or Iraq, or when it was transferred to the foreign governments.

Additionally, the report found missing documentation from equipment transfers to Iraq and Kurdistan governments—more than half of the forms were missing the date of transfer and case identifier information. Officials said they issued verbal orders requiring case identifier information to be included on the forms, but GAO noted that the program’s standard operating procedures do not include that requirement.

“By not capturing the transfer dates of ITEF-funded equipment..., DoD components’ visibility over the amount of ITEF-funded equipment transferred to the government of Iraq is limited,” the report explains. The missing transit information means that DoD cannot ensure that the equipment has reached its intended destination.

GAO didn’t issue any recommendations because it could not pin down why
SCIP was not being used to document the transfer of equipment. The system itself may not be importing data correctly from other DoD data systems, but there is also a lack of clear procedures for reporting the data, the report notes.

“Essentially, that’s why we made a recommendation about DoD looking at the root causes, because it wasn’t easy for them or for us to identify what the single cause was,” Farb explains. “Was it people not entering information, or was it interoperability issues? We didn’t really come to the conclusion that one is the biggest or the single most important issue.”

Greg Schneider, CPP, president of security consultation company Battle Tested Solutions, LLC, says both reports demonstrate the lack of control measures in such military equipment supply chains. Transferring American-made weapons to foreign governments has been a quagmire for many decades, he says, because of how easily they can fall into the wrong hands.

“Sometimes weapons that are funded for one cause can get retasked and repurposed, or sometimes go missing, because sometimes no one wants to leave any traces if they want to get arms into the hands of other people,” Schneider notes. “In Iraq and Kurdistan, there are so many different parties at play, and you have other parties on the outside that are watching with great interest the whole process of the United States delivering weapons to the Kurds because maybe they don’t like the Kurds.”

Meanwhile, Farb says GAO will continue to help DoD figure out why transfer dates for ITEF-funded equipment aren’t being recorded. Current ITEF funding ends next fall, and Farb notes that the new administration has set up a program that would both equip and train Iraq and Syria to oppose adversaries.

As for the LESO program, Merritt says GAO does not take a position on the recent change in policy, but reaffirms that as long as the program continues, the agency will be paying close attention to DOD’s efforts to rectify the lapses in security.

“The way we view it is one item of this type getting into the wrong hands is one item too many,” she says. “We just can’t emphasize that enough.”

@ To view the reports mentioned in this article, visit SM Online.
Because employees often work solo shifts in the store, Jordan has experienced food theft, which drives up business costs. “The greatest loss to my business is employee theft, whether it may be someone walking out the door with a case full of steak, stealing products, or giving away products,” she explains.

While Jordan knew that video surveillance would help, the infrastructure for individual security systems at each store would have been burdensome from a financial and management perspective, she says. That’s when she turned to Hokes Bluff, Alabama-based security integrator Lee Investment Consultants, LLC, to determine the best solution for preventing the theft and robbery plaguing the restaurant.

After evaluating a number of manufacturers, the decision was made to choose two camera models and a video management system from Hanwha Techwin America. With this system, the end user can view live video remotely or from individual store locations, and easily review recorded footage.

The install at the first store location was completed in May 2015, and over the next year and a half the other stores were outfitted. The last installation, at the store located inside a Walmart, was completed in November 2016.

To keep infrastructure costs down, the integrator provides long-term video storage at its hosting facility. It keeps footage for 30 days for the Subway stores before overwriting it.

Given the limited bandwidth Subway restaurants use mainly for their point of sale (POS) systems, local SD...
recording has been a major benefit of the system. For redundancy purposes, recording is performed right on the device using an SD card, and the video is uploaded overnight to the storage servers.

Most store locations have two cameras—one pointed at the sandwich line and register, and another pointed at the back portion of the store where the coolers are. One of the larger stores has three cameras, and the Walmart location only has one camera at the entrance.

“We’ve had problems where employees are voiding out transactions at the register,” Jordan says. “Once employees get clever with the computer system, they might void out an order they just transacted...and stuff that money in their pocket.”

Now the problem with employee theft at the register has gone down, Jordan says, because they can view the cameras which are pointed at the POS terminals. “We can go back and view the video at the time that void was made, so we can see if the transaction is legitimate or not.”

Many of her individual store managers have access to the camera feeds, and Jordan entrusts them with reporting any cases of theft or unwanted employee behavior. For example, one of her managers performed an inventory check and realized several bags of sandwich sauce were
missing. Suspecting one employee in particular as the culprit, that manager decided to watch a live video feed the next time that employee was working. “She just sat there...and actually watched the employee sneaking out the front door with the sauces,” Jordan says. The employee was immediately fired. “If someone’s going to steal a bag of sweet onion teriyaki sauce, they’re not trustworthy.”

The cameras have also led to the arrest of employees in more serious incidents. “A few months ago a customer had come in and had left her wallet behind, so my manager put it in a filing cabinet and told an employee that was coming in it was there,” she explains.

“And when the lady came to pick up her wallet, she had a credit card and cash that was missing.”

Video revealed that the employee who knew where the wallet was had stolen a credit card, and used it to buy a bag of chips in the store. The security integrator helped Jordan upload the footage onto a thumb drive to take to the police. “We got a warrant, and they arrested her for using that credit card,” Jordan tells Security Management. “We could not have proved it if it weren’t for the cameras.”

Even more recently, Jordan noticed about $5,000 was missing from the franchises’ bank deposits that a manager was supposed to be putting in the bank. “Our cameras provided the evidence that she did get the deposits out of the safe and walked out of the store with them,” Jordan says. The manager was arrested and charged with felony embezzlement.

“I never give someone a second chance to steal,” Jordan says. “To me if they steal a bag of chips or give a sandwich to a friend, then they’ll take home five sandwiches for themselves when they get the chance.”

The return on investment from a business perspective has also been huge, Jordan notes. “At one location, our food cost for months had been above 40 percent,” she notes. “After we got those cameras, within a week our food cost came down within the margin we needed.”

The cameras have also led to a greater sense of security among her workers. “I have had employees say they feel safer because of the cameras,” she notes. “Especially with some younger employees, 16 or 17 years old, it’s been a comfort to their parents having the cameras when their child is closing alone.”

“...Minimum Size!

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

See these products & more @ ISC East 2017,
Nov. 15th thru 16th - Javits Center, NYC - Booth #655

GAI-TRONICS®
A Hubbell Company

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

For product info #14 securitymgmt.hotims.com
WHEREVER YOU ARE

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

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

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

SOCIAL
Join the discussion on Facebook and Twitter.

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

PODCAST
Hear what security professionals are talking about.

E-MAIL
Subscribe to the SM Daily and Weekly Newsletters.
In August 2017, FireEye released new threat research confirming with “moderate confidence” that the Russian hacking group APT28, also known as FancyBear, was using an exploit to install malware on hotel networks that then spread laterally to target travelers.

“Once inside the network of a hospitality company, APT28 sought out machines that controlled both guest and internal Wi-Fi networks,” FireEye said in a blog post. “No guest credentials were observed being stolen at the compromised hotels; however, in a separate incident that occurred in fall 2016, APT28 gained initial access to a victim’s network via credentials likely stolen from a hotel Wi-Fi network.”

After APT28 accessed corporate and guest machines connected to the hotel Wi-Fi networks, it deployed a malware that then sent the victims’ usernames and hashed passwords to APT28-controlled machines. “APT28 used this technique to steal usernames and hashed passwords that allowed escalation of privileges in the victim network,” FireEye explained.

This new method is worrisome for security experts because the exploit APT28 was using to infiltrate hotel networks in the first place was EternalBlue, the same vulnerability used to spread ransomware such as WannaCry and NotPetya. It was also allegedly stolen from the U.S. National Security Agency (NSA).

A group of hackers, dubbed the Shadow Brokers, posted the EternalBlue exploit online in April 2017 after claiming to have stolen it from the NSA. The leak was just one
An equivalent scenario with conventional weapons would be the U.S. military having some of its Tomahawk missiles stolen.

An equivalent scenario with conventional weapons would be the U.S. military having some of its Tomahawk missiles stolen.

of many the group has made over the past year detailing NSA vulnerabilities that exploited Cisco Systems, Microsoft products, and others.

The leaks prompted renewed debate on whether the NSA should change its vulnerabilities equities process (VEP) to disclose cyber vulnerabilities to the private sector more frequently to prevent future cyberattacks.

Some of the harshest criticism came from Microsoft itself. In a blog post, President and Chief Legal Officer Brad Smith wrote that the WannaCry attack provided an example of why "stockpiling of vulnerabilities by governments" is a problem.

"An equivalent scenario with conventional weapons would be the U.S. military having some of its Tomahawk missiles stolen," Smith explained. "And this most recent attack represents a completely unintended but disconcerting link between the two most serious forms of cybersecurity threats in the world—nation-state action and organized criminal action."

The VEP began to take form under the George W. Bush administration when then President Bush issued a directive instructing the director of national intelligence, the attorney general, and the secretaries of state, defense, and homeland security to create a "joint plan for the coordination and application of offensive capabilities to defend U.S. information systems."

Based on this directive, the respective agencies recommended that the government create a VEP to coordinate the government's "offensive and defensive mission interests," according to a memo by the Congressional Research Service (CRS) in February 2017.

The Obama administration then created the current VEP, which became publicly known in 2014 in response to the Heartbleed vulnerability—a bug in the OpenSSL cryptographic software that allowed protected information to be compromised.

The VEP, as it is known to exist today, provides the process for how the U.S. government chooses whether to disclose vulnerabilities to the vendor community or retain those vulnerabilities for its own use.

"Vulnerabilities for this purpose may include software vulnerabilities (such as a flaw in the software which allows unauthorized code to run on a machine) or hardware vulnerabilities (such as a flaw in the design of a circuit board which allows an unauthorized party to determine the process running on the machine)," according to the CRS memo sent to U.S. Representative Ted Lieu (D-CA).

To be eligible for the VEP, however, a vulnerability must be new or not known to others. Vulnerabilities are referenced against the Common Vulnerabilities and Exposures Database to determine if they are new or unknown.

When choosing to disclose a vulnerability, there are no clear rules but the U.S. government considers several factors, according to a blog post by former White House Cybersecurity Coordinator Michael Daniel that was written in
response to allegations that the NSA knew about the Heartbleed vulnerability prior to its disclosure online.

For instance, the government considers the extent of the vulnerable system’s use in the Internet’s infrastructure, the risks and harm that could be done if the vulnerability is not patched, whether the administration would know if another organization is exploiting the vulnerability, and whether the vulnerability is needed for the collection of intelligence.

The government also considers how likely it is that the vulnerability will be discovered by others, if the government can use the vulnerability before disclosing it, and if the vulnerability is, in fact, patchable, according to Daniel.

In the post, Daniel wrote that the government should not “completely forgo” its practice of collecting zero-day vulnerabilities because it provides a way to “better protect our country in the long run.”

And while the process allows the government to retain vulnerabilities for its own use, it has tended to disclose them instead. NSA Director Admiral Michael Rogers, for instance, testified to the U.S. Senate Armed Services Committee in September 2016 that the NSA has a VEP disclosure rate of 93 percent, according to the memo which found a discrepancy in the rate.

“The NSA offers that 91 percent of the vulnerabilities it discovers are reported to vendors for vulnerabilities in products made or used in the United States,” the memo said. “The remaining 9 percent are not disclosed because either the vendor patches it before the review process can be completed or the government chose to retain the vulnerability to exploit for national security purposes.”

Jonathan Couch, senior vice president of strategy at ThreatQuotient, says that the U.S. government should not be expected to disclose all of the vulnerabilities.
Our government, just like other governments out there, is reaching out and touching people when needed; they leverage tools and capabilities to do that.

Our government, just like other governments out there, is reaching out and touching people when needed; they leverage tools and capabilities to do that,” says Couch, who prior to working in the private sector served in the U.S. Air Force at the NSA. “You don’t want to invest a ton of money into developing capabilities, just to end up publishing a patch and patching against it.”

However, Couch adds that more could be done by agencies—such as the U.S. Department of Homeland Security (DHS)—that work with the private sector to push out critical patches on vulnerabilities when needed.

“Right now, I think they are too noisy; DHS will pass along anything that it finds—it doesn’t help you prioritize at all,” Couch says. “If DHS could get a pattern of ‘Here’s what we need to patch against, based on what we know and are allowed to share,’ then push that out and allow organizations to act on that.”

Other critics have also recommended that the government be more transparent about the VEP by creating clear guidelines for disclosing vulnerabilities and to “default toward disclosure with retention being the rare exception,” the CRS explained.

One of those recommendations was published by the Harvard Kennedy School’s Belfer Center for Science and International Affairs in Government’s Role in Vulnerability Disclosure: Creating a Permanent and Accountable Vulnerability Equities Process.

The paper, written by Ari Schwartz, managing director of cybersecurity services for Venable LLP and former member of the White House National Security Council, and Rob Knake, Whitney Shepardson senior fellow at the Council on Foreign Relations and former director for cybersecurity policy at the National Security Council, recommended the VEP be strengthened through formalization.

“By affirming existing policy in higher-level, unclassified governing principles, the government would add clarity to the process and help set a model for the world,” the authors explained. “If all the countries with capabilities to collect vulnerabilities had a policy of leaning toward disclosure, it would be valuable to the protection of critical infrastructure and consumers alike, as well as U.S. corporate interests.”

However, the authors cautioned that affirming this process does not mean that the government should publicize its disclosure decisions or deliberations.

“In many cases, it likely would not serve the interests of national security to make such information public,” according to Schwartz and Knake. “However, the principles guiding these decisions, as well as a high-level map of the process that will be used to make such decisions, can and should be public.”

U.S. lawmakers also agree that the VEP should be overhauled to boost transparency. In May, U.S. Senators Brian Schatz (D-HI), Ron Johnson (R-WI), and Cory Gardner (R-CO), and U.S. Representatives Ted Lieu (D-CA) and Blake Farenthold (R-TX) introduced legislation that would require a Vulnerabilities Equities Review Board comprising permanent members. These members would include the secretary...
of homeland security, the FBI director, the director of national intelligence, the CIA director, the NSA director, and the secretary of commerce.

Schatz said that the bill, called the Protecting Our Ability to Counter Hacking (PATCH) Act, strikes the correct balance between national security and cybersecurity.

“Codifying a framework for the relevant agencies to review and disclose vulnerabilities will improve cybersecurity and transparency to the benefit of the public while also ensuring that the federal government has the tools it needs to protect national security,” he explained in a statement.

Additionally, the secretaries of state, treasury, and energy would be considered ad hoc members of the board. Any member of the National Security Council could also be requested by the board to participate, if they are approved by the president, according to the legislation.

The bill has not moved forward in Congress since its introduction, which suggests that many do not see a need for an overhaul of the current disclosure system.

“Codifying a framework for the relevant agencies to review and disclose vulnerabilities will improve cybersecurity and transparency.”

Additionally, the secretaries of state, treasury, and energy would be considered ad hoc members of the board. Any member of the National Security Council could also be requested by the board to participate, if they are approved by the president, according to the legislation.

The bill has not moved forward in Congress since its introduction, which suggests that many do not see a need for an overhaul of the current disclosure system.

“It’s just not realistic for NSA, CIA, or the military or other international governments to start disclosing these tools they’ve developed for cyber espionage,” Couch says.

To read the reports mentioned in this article, visit SM Online.
LET YOUR VOICE BE HEARD.
WITHOUT SAYING A WORD.
FOLLOW US ON SOCIAL MEDIA

Follow us on facebook at:
facebook.com/SecMgmtMag

Follow us on twitter at:
@SecMgmtMag

Keep in touch with Security Management - digitally. Voice your opinions by commenting or tweeting. You can also like us or follow us to get up-to-date notifications about breaking news, events, and access to the invaluable content Security Management provides online and in print.
While primarily political in nature, fake news has been used against various institutions and poses a real and increasing threat to private sector organizations of all sizes.

In November 2016, a man armed himself with an assault rifle and drove six hours from North Carolina to Washington, D.C. His goal was to storm Comet Ping Pong, a D.C. pizza restaurant, and rescue children being held captive and abused by Hillary Clinton. Once inside, the man fired on the restaurant, but no one was hurt.

The Comet Ping Pong story was one of many deliberately false news stories circulating in 2016. After the story was exposed as a hoax, “a post on Twitter by Representative Steven Smith of the 15th District of Georgia—not a real lawmaker and not a real district—warned that what was fake was the information being peddled by the mainstream media. It was retweeted dozens of times,” according to The New York Times.

The concept of fake news entered the popular vocabulary during the U.S. presidential election in 2016. While intentionally spreading false news reports...
TRANSMISSION
There has been an explosion in the creation and distribution of fake news through various online channels, including blogs, websites, discussion forums, and especially social media platforms. According to a 2017 survey, *A Real Plague: Fake News*, conducted by Weber Shandwick, Powell Tate, and KRC Research, approximately 7 in 10 American adults reported having read a fake news story in 2016. Research conducted by Hunt Allcott and Matthew Gentzkow and published in the spring 2017 edition of *The Journal of Economic Perspectives* also found that a database of 38 million shares of fake news stories on social media translated to about 760 million instances of clicking on, and reading, fake news stories.

The subject matter of these stories has run the gamut from political conspiracies to alleged criminal conduct by high-profile individuals to allegations of corporate political bias. A unique aspect of the current situation is that these stories are shared more widely, and more quickly, than ever before due to the ubiquity of social media. According to Allcott and Gentzkow, the list of fake news websites compiled by Stanford University received 159 million visits during the month of the election, while some 41.8 percent of individuals reported that they were exposed to fake news via social media.

Another important aspect of the current situation is that many of these fake news stories have gained a level of credibility among segments of the population that is surprising considering the sometimes bizarre nature of the claims made. In a study by Ipsos Public Affairs for BuzzFeed, 75 percent of respondents who reported remembering a fake news headline believed it to be accurate. In the study by KRC Research, 74 percent of individuals surveyed reported that it is difficult to determine what news is real and what is not.

The increased acceptance of baseless rumors and extreme conspiracy theories is due in no small part to a widespread decline in trust in media, government, academia, and most other forms of traditional authority. The falling levels of trust in media have been well documented by Gallup, Pew Research, and the Edelman Trust Barometer. This collapse of trust has led to the increased importance of the “people like me” category as a trusted source of news and information. According to Edelman’s 2017 global report. Because of these developments, sources such as Reddit, personal blogs, Facebook accounts, and quasi-official websites have gained credibility, while trust in traditional news media and government sources has declined. The fact that these fake news stories are rebroadcast many times, through cross-links and reposts on social media, further adds to the illusion of credibility.

If fake news were limited to stories about Area 51 or the JFK assassination, it would represent an interesting sociological case, but with limited relevance to corporate security. However, both the subject matter and the intensity of emotion elicited make fake news a real threat to corporations in terms of potential financial losses, reputational damage, and the physical security of facilities and personnel. This enhanced threat environment will require adaptation by corporate security professionals and the incorporation of new defensive and offensive capabilities to existing corporate security plans.

The increasingly widespread use of false or misleading information to cause confusion or harm to an individual or organization is not likely to disappear in the near term. The
efficiency of this technique has been clearly demonstrated and the tools facilitating it are becoming ever more powerful, accessible, and easy to use. It is also difficult to imagine a significant increase in trust in traditional authority figures in the near future.

For corporations, some of the most serious fake news risks relate to stock manipulation, reputational damage, and the related loss of business—through boycotts for example—and direct threats to staff and property.

**STOCK MANIPULATION**

At the macro level, fake news has been used to move entire stock exchanges. This was the case in April 2013 when a tweet that appeared to come from the Associated Press (AP) Twitter account reported that there had been an explosion at the White House and that U.S. President Barack Obama was injured. The Dow Jones Index lost 145 points in two minutes, while the S&P lost $136.5 billion. The news was quickly disproved and the market corrected within minutes, but the potential for large-scale disruption was demonstrated. In this instance, the fake news attack was claimed by the Syrian Electronic Army, according to *The Washington Post*.

In October 2009, the Stock Exchange of Thailand (SET) fell 7.2 percent because of an online rumor related to the health of the Thai king. The market made up about half of the loss within the next trading day, and the Thai police made several arrests related to the case later that month, as reported by Reuters.

Fake news has been used to manipulate the shares of individual companies as well. In May 2015, a fake offer to purchase Avon Products led to a surge in trading and a significant increase in the share price, according to *The New York Times*. Then in November 2016, a fake offer to acquire Fitbit shares led to a spike in activity, and a temporary halt to the trade in Fitbit stocks as reported by *The Financial Times*. In 2013, a fake press release was posted claiming the Swedish company Fingerprint Cards AB would be acquired by Samsung. Company shares surged until trading was halted.

In the United States, the Securities and Exchange Commission (SEC) has taken an increasingly aggressive stance in combating this threat to market integrity. It has filed enforcement actions against 27 companies and individuals involved in “alleged stock promotion schemes that left investors with the impression they were reading independent, unbiased analyses on investing websites.
while writers were being secretly compensated for touting company stocks,” according to an SEC statement.

**REPUTATION**

False stories, rumors, or statements taken out of context have led to both reputational harm, as well as to threats to corporate personnel and property. In this type of threat, a corporate statement or action that would be innocuous under normal circumstances has taken on an increased risk due to hyper-sensitive stakeholders.

A case in point was New Balance, when Matthew LeBretton, vice president for public affairs said, “The Obama administration turned a deaf ear to us and frankly, with President-elect Trump, we feel things are going to move in the right direction,” during an interview with The Wall Street Journal. The statement related specifically to President Trump’s plan to withdraw from the TransPacific Partnership (TPP), but was widely misinterpreted. This caused a twofold issue for New Balance. First, anti-Trump individuals saw the statement as an endorsement of the candidate and everything he was purported to believe. This in turn led to calls for a boycott, and many social media posts depicting the destruction of New Balance products as reported by CNBC. A few days later the same statement led Andrew Anglin, a blogger associated with the white supremacist movement, to write on his popular Daily Stormer blog that New Balance shoes were the “Official Shoes of White People.” New Balance was blindsided by the intensity of reactions to a single statement related to a proposed international trade agreement and was forced into reactive positions throughout the crisis.

Another executive statement that was taken out of context and twisted to fit a partisan narrative was made by Indra Nooyi, CEO of PepsiCo in her interview with Andrew Sorkin of The New York Times on November 9, 2016. Her statement included congratulations to President-elect Trump on his victory, while also indicating that some of her employees expressed concerns about their safety as a result of the election. Numerous fake media outlets exaggerated the statement by claiming that she and her employees were “terrified” of Donald Trump and his supporters. This led to a firestorm of social media protests against Pepsi, including calls for a boycott and threats against the company.

**DIRECT THREATS**

As noted above, one of the most serious cases of threats to an organization based on fake news were the reports of child abuse allegedly masteredmind by Hillary Clinton and carried out at a D.C. pizza parlor. While the story was repeatedly debunked, it nevertheless continued to circulate and was supported by Michael Flynn, Jr., son of then National Security Director General Michael Flynn, according to The Washington Post. The shooter was arrested immediately after leaving the pizzeria, where he found no evidence of any abuse. He later pled guilty to the interstate transportation of ammunition and a firearm, a federal charge, in addition to a D.C. charge of assault with a dangerous weapon, according to The Hill.

This case indicates that even the most ridiculous story, if repeated often enough, will find an audience that believes it, and possibly someone who is willing to take action based on its claims. It is possible that a less extreme story focusing on a corporate executive or brand would lead to similar examples of direct action.

**COUNTERMEASURES**

Countering fake news is difficult when the target audience finds it easy to discount facts and the usual sources of information are distrusted. However, there are a number of actions that corporate security teams can take to mitigate the risks posed by this new threat.

**Risk assessment.** As with any threat to corporate security, the place to start is with a detailed risk assessment. The corporate security team needs to look at both internal and external factors to determine both the level of risk, as well as the most likely points of attack. Internal factors include employee demographics, employee morale, and computer use policies. The external factors include the competitive environment, the current perception of the organization and its management, the level of openness and transparency, and the nature of current conversations about the organization. With this information, corporate security will be in a much stronger position to establish policies and procedures to mitigate the risks from fake news attacks.

A white paper by Accenture focusing on social media compliance and risk in the international financial industry highlights the importance of identifying areas where an institution has vulnerabilities and incorporating the findings into its risk mitigation plans. A survey of executives cited in the white paper, A Comprehensive Approach to Managing Social Media Risk and Compliance, found that 59 percent of respondents reported having no social media risk assessments in place, while only 36 percent reported being offered any training on social media risk mitigation.

**Monitoring.** To have any hope of effectively countering fake news, the corporate security team needs to have
as close to real-time visibility of its appearance as possible. This points to the requirement for a comprehensive monitoring program that builds on any existing media or social media monitoring capability the organization already possesses.

It is important that this monitoring program specifically focus on channels that are outside the organization’s norm. These channels may be antithetical to the values of the organization, targeted to a demographic that is generally not associated with the company, or linked to apparently phony information sources. It is also important to look specifically for negative references to the organization.

After experiencing a number of negative stories driven by news and social media, Dell Computer adopted an “everyone is listening” approach to social media monitoring. A Framework for Social Analytics by Susan Etlinger of the Altimeter Group discusses Dell’s hybrid model for media monitoring, which gives a large number of its 100,000 plus workforce some responsibility for monitoring social media channels related to their lines of business. The company also has a Social Media Listening Command Center, which employs sophisticated social media monitoring software to complement its traditional media monitoring program.

A company’s monitoring system should also include an analysis component that helps vet the material, determining how it should be classified and its importance from a risk management perspective. This component would then ensure that any important material is routed to the key decision makers for immediate action.

Finance, investment, and hedge fund companies have been taking a lead in the area of monitoring and identifying fake news stories. The growth of organizations that can deploy multiple content generators focusing on specific companies poses a significant risk to stock market investors. According to reporting in Forbes, companies are also seeking to develop algorithms that can sort through large quantities of content and identify malicious fake news campaigns. One such company that has been widely cited in this regard is Houston-based Indexer LLC.

**RESPONSE PLANS**

Based on the results of the risk audit, the most likely fake news scenarios should be identified and used to create detailed response protocols that can be activated in the event of an actual fake news situation. At a minimum, these plans should include contact information for all crisis team members, checklists for key actions, prepared statement templates to be used with internal and external stakeholders, and escalation...
metrics in the event that the fake news situation is not immediately contained.

The importance of incorporating the social media environment into a robust crisis response system is shown in the Nuclear Energy Institute’s Implementing and Operating a Joint Information System planning document. The plan covers the importance of preassignment of roles and responsibilities, training and readiness exercises, and media monitoring and engagement. The last item includes specific information on the importance of ensuring that information on social media regarding nuclear facilities and incidents is accurate, and that rumors and falsehoods are flagged and corrected.

TRAINING

The weaponization of news represents an evolving threat for many organizations and is not often included in corporate crisis management plans or training programs. As examples of fake news incidents increase, corporate security professionals should build this new threat into security training that is offered in conjunction with the corporate communications and human resources functions. Members of the senior leadership team should also be involved in any fake news response training.

Countering fake news requires fast decision making and decisive action on the part of the organization. To be able to execute effectively, the relevant personnel should be exposed to these scenarios in a simulated environment.

The communications function at DePaul University in Chicago, recognized the importance of building a mix of true and false information on social media into its crisis response training program. The result was a multi-party simulation exercise involving real-time interactions with traditional media, Twitter, and Facebook, as well as direct stakeholder communications. One of the key challenges in this type of training is sorting through incoming information quickly while still ensuring that key facts are not overlooked.

CROSS-FUNCTIONAL TEAMS

By its nature, the threat posed by fake news needs to be met by a comprehensive organizational response. This implies a cross-functional approach to fake news management. While corporate security may take point, the expertise and resources available to the corporate communications, human resources, and legal teams will prove critical.

An executive from an international bank reported to Accenture that it was important for all key functions to participate in risk management planning, especially when it concerns social media. “However, it is always important to have a representative from risk sitting at the table—someone from compliance, someone from legal, and so forth, to provide guidance to key facts are not overlooked.

COMMUNICATIONS

Because of the potentially serious morale and operational ramifications fake news can have on an organization, it is vital that employees are provided with clear and accurate facts and counter messages as quickly as possible.

Beyond reacting to a fake news incident, the organization should seek to inoculate its staff against its effects by undertaking a comprehensive internal communications and employee engagement program. This can be incorporated into the concept of encouraging employees to be brand ambassadors.

Organizations that are most vulnerable to fake news are those about which little is known. Without a base of preexisting knowledge, stakeholders who are exposed to fake news cannot immediately discount it, which is where the seeds of doubt take root. It is thus important that the organization be as transparent as possible, which includes regular proactive external communications. Corporate actions and policies should be communicated, explained, and contextualized to establish the reality of the situation before a fake news story can present a false narrative.

It is especially important to get in front of any bad news stories and ensure that the organization is seen as working to resolve the issue, rather than hiding it. The idea of a first mover advantage with releasing properly
contextualized negative information is a central tenet of contemporary public relations practice, and it can help thwart attempts to create a scandal by fake news outlets.

TRUST

While a full discussion of trust-based relationships is beyond the scope of this article, it should be noted that the establishment of trust with key stakeholders is one of the best defenses against fake news attacks. Creating trust goes beyond simply telling the truth. It involves a range of factors including organizational reliability, competence, and benevolence, along with honesty and transparency. Because trust building involves all aspects of organizational behavior, it must be seen as a strategic initiative and be driven by senior management. Trust’s relationship to fake news defense is likely to be a collateral benefit rather than a primary driver of the initiative.

The use of intentionally false or misleading information distributed through online and social media channels to disrupt or harm organizations is likely to increase dramatically in the years ahead. These actions are increasingly easy and cheap to execute, and take advantage of current weaknesses in organizational capabilities and the fact that societal trust in most traditional authority figures is at a historically low level. It is thus imperative that responsible corporate security professionals develop the internal capabilities and protocols to deal with this new threat environment before they are faced with a fake news attack. The good news is that most of the necessary resources already exist to some degree within the organizational structure and only need to be oriented around the fake news threat. This will include proactive measures such as audits, monitoring, training, and proactive communications, as well as moving quickly to react to the emergence of damaging fake news to contain it and neutralize its ability to damage the organization.

In today’s hyperconnected global information environment no organization is safe from a fake news attack. We have had ample warnings that the threat is real and is likely to get worse. There is no time to waste in hardening the organization against this new type of assault.

JEREMY E. PLOTNICK, PH.D., IS FOUNDER OF CRICOM LLC. HE HAS WORKED IN INTERNATIONAL COMMUNICATIONS CONSULTING, PUBLIC AFFAIRS, AND PUBLIC RELATIONS FOR MORE THAN 20 YEARS.
Mention teleworking, and some managers immediately feel at sea. How can I supervise employees I can’t see? Will staffers be sending check-in emails while watching Netflix? Can professionalism be maintained in pajamas? Yet behind these fears lay opportunities. Teleworking, if planned and managed successfully, can be thought of as an opportunity for an organization to build trust and productivity among employees. It can also be employed as a strategic talent management initiative that improves employee attraction, engagement, and retention while reducing costs for both the firm and the workers.

In the security field, there are some jobs that are not conducive to telework, such as physical security positions that require an on-site presence. But others are more location flexible, and some positions have elements of both—they require on-site availability on some days, but they also include duties that can be conducted at home, such as report writing, security officer scheduling, or customer service interactions that take place over email and phone. Security managers who dismiss telecommuting because not every position in their department is telework-friendly may be losing out on the broader organizational benefits of telework.

The aim of this article is twofold. It will offer some best practice guidance, mined from expert opinion and
recent research, for managing teleworkers. It will also explore how a telework program can be used by a manager so that it plays a key role in the organization’s talent management strategies.

Growing Trend
About 43 percent of U.S. workers work remotely in some capacity, even if that means telecommuting only once a week or less, according to the 2017 version of Gallup’s annual report, The State of the American Workplace. That percentage is up from 39 percent in 2012, which indicates a moderate but steady increase in teleworking.

As telecommuting becomes more popular, the average amount of time each teleworker spends at home or in another remote location increases. The percentage of U.S. teleworking employees who spend 80 percent or more of their time (equivalent to four days per week or more) working remotely has increased from 24 percent in 2012 to 31 percent in 2016. The number of employees who work remotely 40 to 80 percent of their time has also slightly increased, while the number of employees working remotely less than 20 percent of the time has decreased.

In addition, in more than half of the largest U.S. metro areas, telecommuting beats public transportation as the preferred commuting option, according to another report, 2017 State of Telecommuting in the U.S. Employee Workforce. Telecommuting has grown far faster than any other commuting mode, according to the study, which was issued by FlexJobs and Global Workplace.

One of the drivers of the growth of telework has been the U.S. federal government. In 2010, the U.S. Telework Enhancement Act became law, and it required the head of each executive agency to establish and implement a policy under which employees could be authorized to telework. The U.S. General Services Administration (GSA) serves as the lead agency for the government’s initiative; in its latest annual report to Congress, GSA said that federal teleworking continues to increase, with participation growing from 39 percent to 46 percent of eligible employees from 2013 to 2015.

Another telework driver is the increasing pressure from younger workers for more work options. “The millennial generation, which values flexible work, has risen to prominence in the workforce. They are influencing and encouraging remote work policies,” says Robert Arnold, a principal with management consultancy Frost & Sullivan’s Digital Transformation-Connected Work Industry practice. With developments like advanced cloud services, technology continues to evolve and offer more reliable support for remote work, Arnold adds.

Nonetheless, barriers remain. “Federal agencies have made considerable progress (in teleworking), but they also continue to report challenges such as management resistance, outdated cultural norms, and technology limitations,” the GSA said in its latest annual report to Congress.

Often, this management resistance simply boils down to lack of trust, says Kate Lister, president of Global Workplace Analytics. “Some managers have this attitude—if they’re not looking at [workers] in the office, they’re at home on the sofa eating bonbons,” she says. Ironically, she adds, being in sight does not always mean being productive; for telework. And some employees, regardless of position requirements, simply do not want to telecommute. “Many people already know this about themselves—given the choice, they will opt to go into an office every day for the companionship, sense of purpose, or because they don’t trust themselves to be productive at home,” say consultants from Frost & Sullivan in their report, Best Practices for Managing Teleworkers: Changing Attitudes, Changing Ways.

However, those holding jobs with part-time on-site requirements may be eligible. Lister cites the example of a group of park rangers she worked with. Although they spent much time patrolling the park, they also had administrative responsibilities such as report writing, allowing many to successfully telecommute part time.

For guidance, some organizations use the model of concentrative versus collaborative work, Lister explains. Concentrative work, which is best conducted alone and without interruptions, can be done well remotely; collaborative work, such as meetings and group projects, is often best tack-
Best Practices
Once it is decided who might be working remotely, teleworking managers should keep in mind the following best practices, which come from various experts, including those quoted above, and from program guidance offered by GSA.

Co-create. A teleworking policy should be developed by the entire team. To set the tone and foster confidence before a new teleworking program begins, managers should engage in dialogue with their teams and address any questions about teleworking. Asking team members to discuss and achieve consensus on solutions to these questions can help the team become more invested in making a teleworking initiative a success.

While the specific answers will differ for each organization, managers should be prepared for questions such as:

• How will we connect with each other?
• How will teleworking affect my performance evaluations and the way my work is assessed?
• What are the procedures for coordinating team projects?
• Will teleworking affect my career path?
• How can we manage customer expectations while teleworking?
• How can we use technology to help us telework better?
• Can we create a sense of workplace and community when we are working away from the office?

Teamwork. If more than one employee is telecommuting, treat telework as a team activity rather than an individual one, whenever possible. Develop a team schedule, rather than an independent schedule, and a teleworking system that is consistent with the needs of the department and organization. This may mean that if an important team meeting needs to be held in person, employees normally scheduled to telework led in the firm’s office, with other team members present.

Teleworking Security Guidance

Employees who telework may be using their own PCs, laptops, tablets, and smartphones for work purposes. As a result, a telework program will often require setting up, or at least considering, another layer of security, so that the company’s sensitive data is protected.

Security managers facing this issue may want to consult the Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security, issued by the U.S. Department of Commerce’s National Institute of Standards and Technology (NIST). Here is some guidance based on the NIST report.

PLAN
All telework-related security policies and controls should be based on the assumption that external environments contain hostile threats. Some options for protection include encrypting the device’s storage, encrypting all sensitive data stored on devices, or prohibiting the storage of sensitive data on devices.

SECURE DEVICES
Organization-controlled devices must be continually secured against common threats. Generally, security controls for teleworking should include all the local security controls used in the organization’s secure configuration baseline.

RESTRICT FURTHER
But since devices are generally at a greater risk in external environments than in internal environments, additional security controls may be necessary. For example, a personal firewall may be not restrictive enough, so it may have to be adjusted.

DEVELOP A POLICY
This should address requirements for teleworking, which forms of remote access are permitted, the type of access for each worker and device, and the administration of remote access servers.

ENSURE ACCESS
Remote access servers must be protected effectively, correctly configured, and aligned with telework security policies. Organizations should ensure that remote access servers remain fully patched and that they can be managed only by authorized administrators.

CONSIDER ANOTHER NETWORK
If external device use is permitted within the organization’s facilities, strongly consider establishing a separate, external, and dedicated network for this use. Risk can be mitigated by setting up a separate wired or wireless external network dedicated to outside devices.
that day may have to come to the office on a scheduled telework day.

**Virtual presence.** Instant messaging systems can be used by team members to check in each morning, and change status when they will be away from the computer for more than a few minutes. Using a rotating system, one team member can also lead a virtual water cooler chat with a question or comment for team members to respond to once or twice a day. Transparent communication tools like shared calendars can also be useful.

In addition, advanced collaboration tools like video conferencing may also be considered. “They help to bridge the gap by building trust and intimacy that is conveyed by eye contact, body language, and other nonverbal communication cues,” Arnold says.

**Customer service.** If your team members interact with customers, make sure service-level support requirements in communicating with customers are clearly defined. All team members need to agree to meet the same service levels to ensure transparency to the customer. Commit with each other to an acceptable response period for email inquiries or phone calls.

**IT support.** A common reason for teleworking dissatisfaction is IT failure. Teleworkers are dependent on fast, reliable, consistent connections. Work with your IT group to ensure the technology is effective, efficient, operates consistently, and provides excellent customer service. IT department involvement and support is critical to your success.

**Trust.** In talking with teleworkers on the phone, managers should avoid comments like, “Hey, I hear a washing machine. Are you doing your laundry, or working?” Instead, managers should use telework as an opportunity to foster trust between employees and management. Established daily check-ins can be useful, but rigid micro-monitoring of daily activities hinders productivity and creates an environment of distrust.

**Get together.** The value of in-person community office time increases when working in a mobile environment. Collectively decide what types of events and activities will build a sense of cohesion and community. A regular social event might be included.

**Office space options.** In some organizations, teleworkers are encouraged to share their space while teleworking, and relinquish their in-office space when working in the office. This will require coordination with other employees, and sometimes the development of shared space protocols. Hoteling software, which can help administrators keep track of space booking and scheduling, can also assist in this process.

**Manage by results.** For managers used to passing offices where employees are working away, telework can be disconcerting. But apparent worker activity should not be confused with the results those activities produce. Establish a clear definition of objectives and performance indicators, and keep track of those indicators.

**Monitor performance measures.** One measure might be team sick days and absenteeism—have they decreased as your teleworking program progresses? Customer satisfaction might be another measure—has the needle moved in any direction since some team members started teleworking?

**Keep evolving.** Managers should think of a telework program as a continual work in progress. Teams are unlikely to get all arrangements right the first time. Evolving work groups and projects may also force changes in the original arrangements, regardless of how successful they may have been. Remain flexible, evaluate frequently, and adjust the arrangements as needed.

**Telework as Strategic Initiative**

The potential value of a well-managed teleworking program becomes even more clear when it is contextualized in the broader state of the current workplace. And as Gallup’s *The State of the American Workplace* finds, “the modern workforce knows what’s important to them and isn’t going to settle.” More than half of U.S. employees (51 percent) are searching for new jobs or watching for openings, and 47 percent say now is a good time to find a quality job.

But in this environment, teleworking options can boost an organization’s employee retention efforts. “Gallup consistently has found that flexible scheduling and work-from-home opportunities play a major role in an employee’s decision to take or leave a job,” the report says.

GSA has found that teleworking can have a positive impact, in various ways, on the worker. In research comparing teleworkers with nonteleworkers, GSA found that teleworkers report more job satisfaction and higher engagement levels. They are also less likely to want to leave their current organization than nonteleworkers.

Private sector experts have found similar effects. “We do find that job satisfaction and loyalty continue to be
Teleworking options can boost an organization’s employee retention efforts.

positively impacted by remote work. Work-life balance is a big emphasis by employers in many sectors that wish to recruit and retain top talent and employees with increasingly scarce skill sets,” Arnold says.

Indeed, when it comes to employee engagement, the Gallup report showed that the most engaged workers were those who spent 60 to 80 percent of their week—or roughly three to four days—working from home. While four days out of the office may be a bit extreme for some organizations, Lister says that many employers are finding two to three days a week as the telecommuting “sweet spot,” with workers benefitting from both in-office camaraderie and out-of-office concentrative sessions. And Gallup has found that workers who say they have privacy when they need it are 1.7 times more likely to be engaged than workers who do not have that luxury.

Organizations are also finding other benefits to telework. Some organizations have combined an increase in telework with a transition to a smaller office space, thus reducing overhead costs. And the 2017 State of Telecommuting in the U.S. Employee Workforce report found that employers, on average, save roughly $11,000 per half-time telecommuter per year. In addition, firms are often getting more out of their telecommuters. A half-time teleworker gains back an average of 11 days a year in commuting time, and will devote about 60 percent of that gained time toward work, Lister says.

Finally, as the benefits of teleworking become apparent to more employees and more organizations, they are also forcing change, Gallup finds. Organizations are being forced to reconsider how to best manage and optimize performance. Even the basic idea of when and where people work is evolving.

“The workplace is changing,” Gallup says, “at unprecedented speed.”

CONTACT SENIOR EDITOR MARK TARALLO AT MARK.TARALLO@ASISONLINE.ORG. CONNECT WITH HIM ON LINKEDIN.

Teleworking options can boost an organization’s employee retention efforts. For product info #24 securitymgmt.hotims.com

See SM online for a link to the NIST guide.

PINPOINT THE THREAT with the world’s most trusted metal detectors.

Garrett’s hand-held, walk-through and ground search metal detection products have been trusted in security screening applications for more than 25 years.

SuperWand™

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

For product info #24 securitymgmt.hotims.com
Traditionally, factory security assessments have been directed towards the inside of the factory or plant and not to the more exposed perimeter, including the perimeter wall of the factory structure and the fence line. Similarly, assessors often look at the factory’s cyber network and examine the configuration of servers, switches, and human-machine interfaces, but may pay less attention to the outside of the facility walls and physical grounds because they tend to fall outside the classic cyber and physical security boundaries. However, with the increased awareness of the security weaknesses that industrial control systems face, there has been a growth in requests to security and consulting companies for combined cyber and physical security assessments of factories and critical infrastructure. The North American Electric Reliability Corporation (NERC) puts out Critical Infrastructure Protection (CIP) standards that strengthen the cybersecurity of North American
electric grid operations, and recent updates emphasize the importance of strengthening both physical and electronic security perimeters.

A shift in the industry toward enterprise security risk management (ESRM)—which focuses on using risk assessments to inform an organization’s security approach—moves beyond assessing physical security. However, this can be a difficult shift for facilities that do not have a clear risk profile.

This gap in the security assessment process offers an opportunity for plant managers to take an ESRM-inspired approach and better understand their security and infrastructure vulnerabilities to both physical and cyber threats.

**DRAWING THE LINES**

Two security concepts raised in the NERC CIP are related to electronic security perimeters (ESPs) and physical security perimeters (PSPs). The ESP is an imaginary perimeter drawn around a set of critical cyber assets and is usually defined by the location of perimeter access points such as firewalls and modems. The PSP is typically defined as a six-sided border that surrounds critical assets. In the NERC model, the border is intended to totally enclose the ESP.

Although the ESP is a logical, imaginary depiction, it gives a sense of the electronic traffic flowing into and out of a critical set of digital assets as well as the physical plant. This assessment is normally performed by evaluating
A structured but more unusual way to approach a facility assessment is to start with the ESP and PSP concepts in mind and to apply them to the footprint of the facility being examined.

Begin with an overhead view of the facility and the corresponding fence line if possible. One technique is to obtain the satellite view of the facility from an online mapping tool such as Google Earth. Alternatively, a plan view drawing of the facility and surrounding grounds obtained from the facility service manager may be used.

Using this overhead view, draw a border around the facility perimeter with an optional border at the fence line. Once the analysis boundary has been identified, pinpoint both tangible and invisible services and activities, including underground, airborne, or surface vectors. Consider services that cross this boundary and place them on the map where they enter the facility. Infrastructure to consider includes electric power feeds from substation or emergency generators, natural gas or propane, water, sewer, enterprise and public fiber connections, telephone and cable television lines, and other commercial services. Inbound services such as product feeds from other facilities and deliveries like mail or packages, as well as outbound shipments, should also be taken into consideration.

Electronic signals that cross in and out of the facility include Wi-Fi, cellular, radio, and satellite communications, and these should be included on the risk map. For example, while performing an assessment of a client’s facility, including a wireless security inspection, Wi-Fi service was detected but was not owned or provided by the enterprise. The investigation revealed that the signal was from a nearby house and was not secured, allowing employees and visitors at the factory to connect to the rogue Wi-Fi. Such a connection could contaminate the individual’s laptop or mobile phone, as well as other Wi-Fi–equipped devices, with a worm, virus, or ransomware from the unknown and uncontrolled Wi-Fi.

A similar vulnerability was discovered at another power plant: a contractor’s trailer adjacent to the plant fence line had an insecure Wi-Fi set up, which was available inside the power plant. Depending on the age and type of property, identifying these services may be a challenge. Older facilities may not have the necessary drawings, infrastructure diagrams, or employee knowledge to identify where the underground lines are for some of these services. Older facilities also suffer from abandoned equipment and systems that tend to be ignored because they are no longer in service. If the client has recently purchased the property, it may not know where these services enter or exit the plant.

An additional complication is that some services have dual feeds from separate locations. For example, a data center will normally have redundant power and communications at different perimeter locations. These should be reflected on the analysis mapping.

Once these various activities and services have been identified and listed, begin looking at the vulnerabilities each poses to the plant and to the availability of the facility operations.

The perimeter assessment should be more holistic than simply walking down a fence line or the perimeter of a building. For example, while performing this analysis for a client, a problem was identified with the underground water feed into the plant. The plant had only one line entering the plant supplying potable water, service water, and fire protection/sprinkler water. The line ran under the fence, across a large field between the fence and the factory itself, and then into the building with some feeders going to the fire pumps located outside the factory in a field. The line could be subject to backhoe or digging damage because it was not effectively marked, but the larger problem was outside of the fence.

Beyond the fence line was the water service building—a small, unmarked wooden structure that contained the tap into the local city water supply, as well as several isolation valves and a flow meter for billing and volume calculations. The inspector discovered the building open and unoccupied—the door padlock was hanging open on the hasp. This would have allowed an
We build security booths stronger than blasts and bullets

Should terror approach your critical location, you want to protect security personnel on your perimeter so they can execute emergency procedures, saving lives and property. B.I.G.’s ready-to-use booths can be built from Level 1 up to Level NIJ-IV and 50 caliber armor piercing—the highest rated booths in the industry. Our clients take no risks with security; that’s why they trust booths from B.I.G. Enterprises.

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.
Conducting an integrated, ESRM-based analysis helps bring awareness of what crosses facility boundaries.

The inspector needs to look at all tell-tale signs and artifacts—many of which are prominently placed—that could tell an attacker where a softer and more vulnerable service feeding the plant is located. For example, site and facility architects use underground vault covers that explicitly label the service. That practice can be helpful for maintenance and emergency response but it also provides an easy target for criminals.

Similarly, the way these vault covers are secured could be problematic. The covers should be locked, but an added layer of security includes using tamper-resistant fasteners or proprietary screw heads and bolts.

Conducting an integrated, ESRM-based analysis helps bring awareness of what crosses facility boundaries, whether it be in electronic or physical form. It encourages plant managers to document underground infrastructure and fill gaps in knowledge, and provides enhanced planning for both physical and wireless attacks from modes ranging from surface injections to airborne threats. By mapping out both the physical and electronic perimeters, a facility’s security approach can be based on what can and cannot be seen.

ERNIE HAYDEN, PSP, CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL (CISSP), CERTIFIED ETHICAL HACKER (CEH), SANS GLOBAL INDUSTRIAL CYBER SECURITY PROFESSIONAL (GICSP), IS THE ICS CYBERSECURITY LEAD AT BBA, A CANADIAN ENGINEERING COMPANY. HE IS A MEMBER OF ASIS.
ASIS EUROPE 2018
FROM RISK TO RESILIENCE
ROTTERDAM NETHERLANDS 18–20 APRIL 2018

CYBER, PHYSICAL OR INSIDER THREAT?
ALL OF THE ABOVE?

EARLY BIRD RATES
UNTIL 15 NOVEMBER

www.asiseurope.org
THOSE WE CHEER
THIS YEAR

ASIS PRESENTED MANY AWARDS at the ASIS International 63rd Annual Seminar and Exhibits to celebrate members and partners with noteworthy accomplishments in 2017. These honored members and supporting organizations exemplify the determination and capability of all involved with the Society.

ASIS is pleased to recognize these outstanding accomplishments. The Don Walker Award for Enterprise Security Executive Leadership celebrates an individual who demonstrates a commitment to promoting security management education, certification, and standards. This year, it was presented to Raymond T. O’Hara, CPP. A former ASIS president, O’Hara currently serves as executive vice president at AS Solution. Throughout his career, he has supported lifelong learning, board certification, and the development of the next generation of security leaders.

The Presidential Award of Merit is presented to individuals who contribute to ASIS as exemplary volunteer leaders. The 2017 recipients of the award are Joseph N. Masciocco and Les Cole, CPP. Masciocco, president of Security Integrations, is a 33-year member of ASIS who is a senior regional vice president. He has been involved in ASIS volunteer leadership since 1995.

Cole, who passed away on September 15, 2017, was an ASIS member for 41 years, and served as a council vice president from 2011 to 2016. Don Knox, CPP, a fellow council vice president, accepted the award on behalf of Cole and his family.

The Certification Organization Award of Merit goes to entities that have made strides advancing the professionalism of the security field through board certification. The award was presented to Guidepost Solutions and Tech Systems.

In addition, the Certification Regional Award recognizes individuals who help advance ASIS board certification. Winners this year are Randolph C.D. Brooks, CPP, Region 6C; Mushtaq Khan, CPP, PCI, PSP, Region 13A; J.D. Killeen, CPP, Region 6B; Allan L. McDougall, CPP, PSP, Region 6B; Garfield A. Owen, PSP, Region 7B; Percy J. Ryberg, CPP, Region 8C; Jasvir Singh Saini, CPP, Region 13A; Gwee Khiang Tan, CPP, Region 13B; Larry D. Woods, CPP, PSP, Region 4A; and Richard J. Wright, PSP, Region 3C.

The I.B. Hale Chapter of the Year Award recognizes chapters of ASIS who excel in membership growth, educational programming, publications, and the advancement of the security profession. The chapters recognized in 2017 were the Mexico City Chapter and the National Capital Chapter.
The Roy N. Bordes Council Member Award of Excellence, presented to Doug Powell, CPP, PSP, distinguishes an ASIS council member who helps engage the next generation of security professionals through sharing their knowledge and expertise with ASIS educational programs and publications.

The E.J. Criscioli, Jr., CPP Volunteer Leadership Award was presented to Dr. Rolf Sigg. This award acknowledges the contributions made by one member to ASIS’s chapter and regional levels over an extended period of time.

The Matthew Simeone P3 Excellence Award is administered by the ASIS Law Enforcement Liaison Council and recognizes programs that promote cooperation between public and private sectors. The 2017 award was presented to the Columbus Police Department’s Capital Crossroads and Discovery SID Program.

The Transitions Ad Hoc Council, with the support of the ASIS Foundation, confers three Council Certification Scholarships to individuals serving in law enforcement who are seeking ASIS board certification. In 2017, the scholarships were awarded to Lieutenant Chapin T. Jones of the Louisville (Kentucky) Metro Police Department, Officer Henry K.S. Chong of U.S. Customs and Border Protection, and Lieutenant Brian T. Woods of the Los Angeles Police Department.

The ASIS Foundation also supports Military Liaison Council Certification Scholarships. The 2017 recipients of these scholarships are Lieutenant Colonel Robert Kwegyir Sagoe, who serves at Headquarters Northern Command in Ghana; Master Sergeant Liviu Ivan and Lieutenant Colonel Eric Minor, who both serve in the U.S. Army at the Mission Command Center in Ft. Leavenworth, Kansas; and Lieutenant Colonel Richard Cobba-Eshun, who serves in the Department of International Peace Support Operations for the Ghana Armed Forces.

This year is the 40th anniversary of the ASIS International Board Certification Program, initiated in 1977 with the Certified Protection Professional® (CPP) designation. Four individuals have been active CPPs since the program’s inception. They were recognized at the Opening Luncheon on Monday, September 25. They are Dr. James D. Calder, CPP, professor at University of Texas; Don W. Walker, CPP, chairman of Securitas Security Services USA, Inc.; Dr. Kenneth G. Fauth, CPP, senior consultant at K. Fauth, Inc.; and James P. Carino, Jr., CPP, senior consultant at Executive Security Consultants.

ASIS salutes all these award winners for their valuable contributions to the security profession.

A DIGITAL TRANSFORMATION

Remaining relevant in today’s on-demand, content-driven world means that associations must be data-driven, customer-obsessed, hyper-connected, and agile. The need for innovation has never been greater.

With a clear directive to transform the organization through the strategic use of technology, ASIS strives to remain at the vanguard of the evolving security profession. It is currently engaged in a broad range of innovative projects, including a major redesign of the primary website and the underlying technologies that support both rapid content creation and the online and mobile member experiences that users expect in the consumer world.

In early 2018, ASIS will launch phase one of a multi-year transformation project focused on improved and personalized content access, user-centric search and commerce, online community, and integrated systems for learning and certification.

Building on a world-class enterprise system for commerce and content...
management, the new website will use a taxonomy structure to drive better content organization. Users will enjoy an intuitive and dynamic navigation structure to browse the site, and they will be presented with streamlined, personalized content.

One of the key strategies is to create a powerful search function that will unify content from a variety of ASIS sources (Web, learning, Security Management, and events, for example). By creating a search-centric site that allows users to filter results, ASIS will be able to meet its goal of helping members in their

“moment of need” by providing resources of all types in a single interface.

There will be a major facelift for the website, incorporating a more graphical and modern interface with relevant imagery, infographics, and videos to present content in a variety of ways on both desktop and mobile devices.

The “mobile first” initiative also ensures that all online experiences—from search to joining the organization—are simple and engaging on any device, regardless of size. In addition to the website overhaul, ASIS will be upgrading its membership database, including new functionality for engagement, certification, profile management, and data analytics.

The system will be tightly integrated with the website to ensure a positive user experience across platforms. ASIS will be asking members to fully update their online profiles, both to help drive online personalization and to comply with the EU General Data Protection Regulation, which takes effect in 2018.

Finally, ASIS will launch an online community platform aimed at providing its customers, members, and prospects with one secure location to interact and build value within the security profession. By providing an online home where members can network, share ideas, answer questions, and stay connected, ASIS will empower them to engage in real time with their peers, chapters, ASIS staff, and industry experts. The online community tools will also allow the Society to provide more engagement for committees, councils, and chapters, and serve as a dynamic online membership directory.

LIFE MEMBER

Michael A. Khairallah, a member of the New Orleans Chapter since 1981, has been granted Life Member status. He has served ASIS as a regional vice president, assistant regional vice president, and chapter chair.

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

MEMBER BOOK REVIEW

Implementing Physical Protection Systems: A Project Management Guide. By David G. Patterson, CPP, PSP.

CreateSpace Publishing; available from ASIS; item #2335; 330 pages; $58 (members); $63 (nonmembers).

Author David G. Patterson, CPP, PSP, drew on decades of experience in physical security project management to write Implementing Physical Protection Systems: A Project Management Guide. The book is a comprehensive guide to the processes involved in setting up various elements of physical security plans.

As a follow-up to the author’s prior text, Implementing Physical Protection Systems, this book is geared towards the project management aspects of any physical security endeavor. It provides a clear review of the many topics under the umbrella of physical security. While covering many of the basic elements of physical security (lighting, fencing, alarming, and cameras), it also goes into the more technical aspects of cabling and necessary support networks.

If you are not a physical security specialist, but aspects of the technology side of security still fit within your area of responsibility, this book may be appealing. The text is simple to understand and the more complex parts of these projects are explained in terms that most security generalists will be familiar with.

A longtime member of the ASIS Physical Security Council, Patterson compiled information and concepts from experts in the technology aspects of security, delineating steps of the project in easy-to-read references. From risk assessments to deliverables and all action steps in between, his book serves as a valuable guide. Borrowing from the simple explanations he provides may help security practitioners explain
William J. Powers, III, CPP, is director of facilities at the Clark Art Institute in Williamstown, Massachusetts. The Clark’s 140-acre campus includes five buildings that house museum galleries, an art history library, an auditorium, research facilities, a sophisticated physical plant, and offices. The campus also has an expansive landscape, including a reflecting pool, woodland meadows, and walking trails. The Clark’s permanent collection includes American and European art amassed during the first half of the 20th century by Francine and Sterling Clark.

To secure this eclectic campus, Powers oversees 12 full-time employees and a 60-person contract security staff. In his 22 years at the Clark, Powers has seen much growth in the institute’s programs and facilities, including a recent $170 million expansion and renovation. “I worked very closely with the security consultant on product selection,” says Powers. “I am proud to say that the installation and implementation of the choices were seamless.” The result, he adds, is a system that is a model for other institutions.

Powers’ biggest challenge is responding to HVAC alarms. “The museum requires very stable climate control 365 days a year,” he says. “I have found that if you follow acknowledged best practices you can have peace of mind.” He credits his affiliation with ASIS International for giving him access to the latest best practices, as well as subject matter experts.

Two achievements helped Powers reach his current status. The first was completing his master’s degree. At the time, Powers was supporting two children in college, and attaining that degree seemed impossible. But he applied for and was selected as a recipient of an ASIS/University of Phoenix scholarship. The second was when Powers received his Certified Protection Professional© (CPP) certification. “These two events really lifted my confidence and proved that I was a true professional,” he says.

Powers was an ASIS volunteer leader for many years before pursuing the CPP, and knew peers who had their CPPs. As past chair of the ASIS Cultural Properties Council and current member of the Awards Committee, “I wanted to be recognized that I am in those positions for a reason.”

Studying for the CPP also pushed Powers to review guidelines and best practices that he otherwise might have overlooked. In his position, he must understand all facets of security—physical, electronic, and cyber. By earning his CPP, he says, “I confirmed my competence in all aspects of security management,” he adds.

Powers never expected to be in his current position. A trained auto mechanic, his first job was in the facilities department of a museum. He eventually became director of facilities at that institution, which included oversight of security.

Today, Powers mentors young professionals coming into the field, reminding them that private security can provide a career path that is personally and financially rewarding if they work towards professional certifications. To that end, Powers advises taking a CPP review course and investing time in studying for the test. The payoff, for Powers, is obvious: “I am now a more effective, well-rounded security professional.”

PROFILE BY MARY ALICE DAVIDSON, PRINCIPAL, DAVIDSON COMMUNICATIONS
From the first preseminar workshop to the last exhibitor visit, attendees at ASIS 2017 in Dallas expanded their knowledge and awareness, extended their professional networks, and experienced Texas hospitality during the last week in September.

In Monday’s opening keynote, 43rd U.S. President George W. Bush spoke with ASIS CEO Peter J. O’Neil, CAE, about leadership, lessons learned while in the White House, and current affairs. Members of the ASIS Board of Directors gather with Bonnie Michelman, CPP (in white shawl), the 2017 Karen Marquez honoree.
Clockwise from below: The President’s Reception at AT&T Stadium. ASIS presented awards to members and partners (see page 54). Siggi accepts Volunteer Leadership Award. Masciocco receives Presidential Award of Merit. Keynote speaker Mark Cuban talks with press. Guidepost Solutions and Tech Systems receive the Organization Award of Merit. Powell wins Council Member Award. The welcome reception at Gilley’s Dallas included mechanical bull riding, with proceeds going to the ASIS Foundation.

View all ASIS 2017 photos at flickr.com/asisinternational.
LEGAL REPORT | BY MEGAN GATES

JUDICIAL DECISIONS

DATA BREACHES. The heightened risk of future identity theft is sufficient to show standing to sue at the pleading stage in a lawsuit, a U.S. court of appeals ruled—becoming the second appellate court to reach this conclusion.

Health insurance company CareFirst experienced a cyberattack in 2014 and its customers’ personal information was allegedly stolen. Several CareFirst customers attributed the breach to the company’s “carelessness” and brought a punitive class action lawsuit against it, according to the suit.

The plaintiffs raised 11 state-law causes of action, including breach of contract, negligence, and violation of state consumer-protection statutes. They also argued that they suffered “an increased risk of identity theft as a result of the data breach,” court documents said.

A district court dismissed their case, however, because it said the risk of future injury was too speculative to establish injury—which would give them standing to sue CareFirst.

The plaintiffs appealed the decision, which reached the U.S. Court of Ap-

LEGAL HIGHLIGHTS

TERRORISM
The EU Court of Justice overturned a General Court ruling, allowing Hamas to remain on the EU bloc’s terrorism blacklist. The lower court had ruled in 2014 that there was not sufficient evidence to keep travel bans and asset freezes on Hamas in place. The Court of Justice, however, found that the General Court had not relied on “national decisions by competent authorities” to remove Hamas from the blacklist. The Court of Justice referred the case back to the General Court so it could “examine the facts and arguments on which it did not rule” in its previous judgment, according to a press release. (Council v. LTTE and Council v. Hamas, EU Court of Justice, Nos. C-599/14 P and C-79/15 P, 2017)

DISCRIMINATION
A U.S. federal judge rejected a $22.8 million settlement between Lockheed Martin Corp., and a group of 5,500 black workers to resolve a proposed class race discrimination lawsuit. Judge Ketanji Brown Jackson wrote that the settlement raised “fairness-related red flags” for the workers because it would force them to give up all race bias claims against Lockheed, not just those that were the focus of the lawsuit. The lawsuit claimed that Lockheed’s performance review system had a disparate impact in the pay, promotion, and retention of salaried black workers below the level of vice president during a three-year period. (Ross v. Lockheed Martin Corp., U.S. District Court for the District of Columbia, No. 1:16-cv-02508-KBJ, 2017)

HARASSMENT
Ford Motor Company agreed to pay up to $10.1 million to settle a sex and race harassment investigation by the U.S. Equal Employment Opportunity Commission (EEOC). In an investigation, the EEOC “found reasonable cause to believe that personnel at two Ford facilities in the Chicago area...had subjected female and African American employees to sexual and racial harassment,” the EEOC said in a press release. It also found that Ford retaliated against employees who spoke out about the treatment. In addition to monetary relief, Ford will conduct regular training at the two facilities, disseminate anti-harassment and anti-discrimination policies and procedures, report to the EEOC harassment and discrimination complaints, and monitor its workforce for issues of alleged sexual or racial harassment and discrimination.

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

ISSUE: Human Trafficking
BILL: S. 1693
VENUE: U.S. Senate
STATUS: Under Consideration
SIGNIFICANCE: Would hold websites liable for information published on their sites that is “designed to facilitate sex trafficking.”
peals for the D.C. Circuit, to determine whether they had standing to sue.

“To demonstrate standing, a plaintiff must show that she has suffered an ‘injury in fact’ that is ‘fairly traceable’ to the defendant’s actions and that is ‘likely to be redressed’ by the relief she seeks,” the appellate court wrote.

Based on its assessment, the appellate court found that the plaintiffs had “plausibly alleged a risk of future injury that is substantial enough to create...standing.”

The plaintiffs claimed that the sensitive data that CareFirst stored on them that was compromised placed them at high risk of financial fraud.

“CareFirst does not seriously dispute that plaintiffs would face a substantial risk of identity theft if their Social Security numbers were accessed by a network intruder, and, drawing on ‘experience and common sense,’ we agree,” the appellate court said.

“No long sequence of uncertain contingencies involving multiple independent actors has to occur before the plaintiffs in this case will suffer any harm; a substantial risk of harm exists already, simply by virtue of the hack and the nature of the data that the plaintiffs allege was taken,” the appellate court said.

The appellate court also ruled that Slough, Liberty, and Heard’s 30-year mandatory minimum sentence violated the Eighth Amendment prohibition against cruel and unusual punishment. It remanded their cases for resentencing.

The four men were contracted through Blackwater in 2007 to provide security for the U.S. Department of State in Baghdad. While out on patrol in response to a car bombing, prosecutors said the defendants went on a shooting spree that killed 14 people and injured 17. The defense, however, argued that the guards feared they were under attack and fired in self-defense. (U.S. v. Slatten, U.S. Court of Appeals for the D.C. Circuit, #15-3078, 2017)


The U.S. Court of Appeals for the D.C. Circuit ruled that lower court judge Royce Lamberth should not have barred a statement by a codefendant during Nicholas Slatten’s original trial that said Slatten did not fire the first shot in what came to be known as the Nisur Square massacre.

The statement, the court of appeals said, should have been allowed and Slatten should have been tried separately from his three codefendants—Paul Slough, Evan Liberty, and Dustin Heard, also former Blackwater security personnel stationed in Iraq.

Instead, they were tried together and Slough, Liberty, and Heard were convicted of voluntary manslaughter, attempted manslaughter, and using and discharging a firearm in relation to a crime of violence. Slatten was convicted of first-degree murder.

Slatten was sentenced to life in prison, and Slough, Liberty, and Heard were sentenced to a mandatory minimum of 30 years in prison.

Slatten appealed the ruling, and through the court process his case reached the appellate court where he challenged the lower court’s decision not to sever his trial from that of a co-defendant and try him alone.

“Slatten argued for severance because he sought to introduce exculpatory evidence—the codefendant’s admission that he, not Slatten, initiated the Nisur Square attack by firing on [a vehicle]—evidence inadmissible in a joint trial with a codefendant,” the appellate court wrote in its opinion.

The district court denied Slatten’s request, which the appellate court said was wrong because the codefendant’s admissions were “vital to Slatten’s defense and possessed sufficient circumstantial guarantees of trustworthiness,” the appellate court explained. “Accordingly, because the district court erroneously denied severance, we reverse Slatten’s first-degree murder conviction...and remand his case for a new trial.”

The appellate court also ruled that Slough, Liberty, and Heard’s 30-year mandatory minimum sentence violated the Eighth Amendment prohibition against cruel and unusual punishment. It remanded their cases for resentencing.

The four men were contracted through Blackwater in 2007 to provide security for the U.S. Department of State in Baghdad. While out on patrol in response to a car bombing, prosecutors said the defendants went on a shooting spree that killed 14 people and injured 17. The defense, however, argued that the guards feared they were under attack and fired in self-defense. (U.S. v. Slatten, U.S. Court of Appeals for the D.C. Circuit, #15-3078, 2017)

**REGULATIONS**

**United States**

**MEDICAL TESTING.** The Federal Motor Carrier Safety Administration and Federal Railroad Administration withdrew a proposed rule to require truck drivers and train operators be tested for obstructive sleep apnea (OSA).

The agencies initially published the rule in March 2016 because OSA “can cause unintended sleep episodes and resulting deficits in attention, concentration, situational awareness, and memory, thus reducing the capacity to...”
safely respond to hazards when performing safety sensitive duties.”

Instead of requiring tests, the agencies said the issue can be addressed through existing safety programs and rules, and that private companies can decide whether to test employees.

The National Transportation Safety Board, however, criticized the decision to withdraw the proposed rule because OSA has been linked to 10 highway and rail accidents in the last 17 years, according to National Public Radio.

**LEGISLATION**

**Russia**

**ANONYMITY.** Russian President Vladimir Putin signed into law amendments that prohibit the use of Internet proxy services and cut down the use of anonymous instant messaging services.

The amendment to the Federal Law on Information requires that Internet providers block websites that offer virtual private networks (VPNs) and other proxy services. The measure goes into effect on November 1, 2017.

Another amendment requires that instant messaging services create methods to identify users by their phone numbers. It also requires service providers to restrict access to their services, at the request of authorities, if users are sharing content considered illegal in Russia. The amendment goes into effect on January 1, 2018.

**United Kingdom**

**DATA PROTECTION.** U.K. Digital Minister Matt Hancock announced that the government will introduce new legislation aligning U.K. law more closely with the EU General Data Protection Regulation.

The Data Protection Bill is designed to give individuals greater control over their data by making it easier to withdraw consent for the use of personal data, allowing people to ask that their personal data held by companies be erased, and enable parents and guardians to give consent for their child’s data to be used.

The bill also expands the definition of personal data to include IP addresses, Internet cookies, and DNA; makes it easier and free for individuals to require an organization to disclose the personal data it holds on them; and makes it easier for customers to move data between service providers.

The bill will also phase out the use of “opt-out” boxes, which many organizations rely on their users to select should they not want their personal information collected. Instead, organizations will have to have “explicit” consent to process sensitive personal data.

The U.K. Information Commissioner’s Office (its data protection regulator) will also be given more power to defend consumer interests and issue fines of up to £17 million (about $22 million) or 4 percent of global turnover for the most serious data breaches.

“Our measures are designed to support businesses in their use of data, and give consumers the confidence that their data is protected and those who misuse it will be held to account,” Hancock said in a statement.

**United States**

**RECOVERY.** U.S. President Trump signed into law legislation that authorizes the U.S. Capitol Police Board to make payments to the U.S. Capitol Police Memorial Fund.

The Wounded Officers Recovery Act of 2017 (P.L. 115-45) allows these payments to then be given to families of U.S. Capitol Police employees who were killed in the line of duty or sustained serious line-of-duty injuries.

The legislation was passed and enacted in response to a shooting in Alexandria, Virginia, that targeted members of Congress who were practicing for the annual Congressional Baseball Game.

“In light of the attack on Congressional Republicans’ baseball practice last month, in which two Capitol Police officers were wounded while bravely working to stop the gunman, we believe that the law should be amended to allow the fund to provide similar support to U.S. Capitol Police officers seriously injured in the line of duty,” said U.S. Representative Mike Doyle (R-PA), who cosponsored the bill.

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

**FOR MORE INFORMATION:**

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

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

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

**COURT CASES**

**CASE:** OPM Breach
**ISSUE:** Discrimination
**CASE:** EEOC v. Vicksburg Healthcare, LLC
**VENUE:** U.S. District Court for the Southern District of Mississippi
**STATUS:** Settled
**SIGNIFICANCE:** Judge found that because the OPM data was stolen, not disclosed, plaintiffs had not suffered harm and did not have standing to sue the agency.

Vicksburg Healthcare will pay $100,000 to settle a disability discrimination suit alleging it failed to provide accommodation for an employee to return to work after surgery.
REACH NEW HEIGHTS

Earn an ASIS board certification, recognized worldwide as the mark of excellence in security management.

The gold standard, ASIS certifications are transferable across all industry sectors and geographic borders. Today, security professionals in 85 countries proudly maintain their ASIS board certifications.

Distinguish yourself as the best of the best by earning the CPP, PCI, and PSP! Get started today at asisonline.org/reach.

“It’s imperative to understand the challenges facing a company’s security department and speak the same language. The CPP and PSP certifications allow me to have the intelligent conversations needed to ensure we’re properly addressing their specific requirements.”

Anjali B. Sniadowski, CPP, PSP
Director, Global Programs
iJet International
VIKINGS STADIUM OPENS DOORS

THE NEW U.S. BANK STADIUM—home of the Minnesota Vikings—hosted more than 66,000 fans at the first Monday night game of the 2017 season. Completed last year, the 1.5 million-square-foot stadium campus is flexible enough to serve as a true multipurpose stadium that can host football, soccer, baseball, basketball, motorsports, major concerts, and other events.

ASSA ABLOY was tapped to provide more than 1,500 doors and openings for the state-of-the-art stadium. A truncated construction timeframe provided the impetus for using preassembled openings. The ready-to-install openings improved onsite management of multiple components and saved time through a streamlined installation process.

The openings included products from ASSA ABLOY Architectural Door Accessories, including McKinney hinges, Pemko accessories, and Rockwood door trim, as well as Curries hollow metal doors and frames; Sargent locks, exit devices, and door closers; Medeco high-security cylinders and keys; and Securitron access control components.

PARTNERSHIPS AND DEALS

Dahua Technology is partnering with Anixter International to market Dahua products throughout the United States and Canada.

Anomali and NSS Labs, Inc., announced a strategic partnership that provides enterprise customers with a unified view of unmitigated threats and empirical data regarding the effectiveness of security controls.

Bold Technologies completed the integration of ManitouNEO with innoVi from Agent Video Intelligence to provide monitoring centers with a video intrusion system.

Boon Edam product data and customized specifications for the Americas are available through the ARCOM software platform to architects, engineers, and design professionals.

Brady announced that its Brand Protection business partnered with Kezziidor Honeywell to bring product authentication labeling and tracking to Genetron 134, a refrigerant.

ByteGrid Holdings LLC announced an agreement with Empowerment through Technology and Education to provide greater compliance and control of hosted business-critical data.

Baltimore Cyber Range LLC and Cyberbit Ltd. announced the opening of the new Baltimore Cyber Range cybersecurity training and simulation center in Baltimore, Maryland.

Camden Door Controls retained manufacturer’s representative J.Clemente & Associates to service its southern California territory.

Celebreite is joining the National Center for Missing & Exploited Children and Project VIC in the global fight against child exploitation.

Claroty and Schneider Electric are partnering to address safety and cybersecurity challenges for the industrial infrastructure sector.
Conformance Technologies announced that Pivotal Payments selected its solutions to enhance business effectiveness and protection of its North American merchant portfolio.

The addition of deversus, Inc., background checking software to the ICIMS partner ecosystem will provide cost savings and improved speed to customers.

EventTracker announced that its SIEM platform was implemented at OneBlood, Inc.

Exabeam and ThreatConnect, Inc., announced a product integration designed to improve overall cybersecurity and incident response.

EyeLock LLC entered into a partnership with CSD (Central Security Distribution) to deliver EyeLock’s product suite in Australia. EyeLock is also developing iris authentication solutions to work with Qualcomm Mobile Security.

Farpointe Data helped Secure Our City, Inc., improve security access for a parking garage.

Galaxy Control Systems completed an integration with IP-enabled solutions from ASSA ABLOY.

Genetec and Alutel Mobility partnered to offer extended access control capabilities to open areas without having to rely on physical readers or installations.

Hikvision Canada Inc., provided cameras for the JPPS Children’s Centre in Montreal that were installed by integrator Alarne Sentinelle. Petite Echelle Centre in Montreal worked with integrator Inteligest to upgrade its security system with Hikvision.

Honeywell and eDist Security expanded their relationship around the Genesis Series Cable product line.

Hutttig Building Products selected TierPoint to provide colocation and data center migration services.

Imagination Technologies and Sierraware are collaborating to make Sierraware’s SierraTEE available for devices based on Imagination’s MIPS CPUs.

ISONAS Inc. announced that Transportation Impact selected the ISO-NAS Pure IP access control solution to secure its corporate headquarters.

Johnson Controls announced that its American Dynamics victor Video Management Software integrates with the Guardian Indoor Active Shooter Detection System from Shooter Detection Systems.

Karamba Security joined the Automotive Grade Linux (AGL) Project and The Linux Foundation to help develop its cybersecurity best practices.

The Legrand On-Q Digital Audio System has been integrated with Alarm.com.

Netwrix Corporation announced that its Netwrix Auditor empowers Guadalupe Valley Electric Cooperative to minimize insider threats and improve database security.

OnSSI and Seagate teamed up to provide a robust recording solution designed for more efficient system expansion and scalability.

Ever and Pinn formed a technology partnership to integrate Ever’s facial recognition into Pinn’s secure attribution platform.

Enterprise Performance Consulting joined the PSA Business Solutions Program to offer business consulting and operations team training programs to PSA integrators.

Point Blank Enterprises and Special Ops Bunker made an exclusive global marketing agreement to offer Special Ops Bunker products through the Point Blank global network.

Golden Lion Marbella, a casino in Panama, selected Qognify VisionHub to upgrade its security, safety, and operations.

RapidSOS is partnering with WiseWear, Fusar, Kairos, Lumenus, and ROAR for Good to provide a rich data link to 911 from wearable products, so users can connect to 911 by pushing a panic button or by detection from a wearable device during a crash or medical emergency.

Sky and Cisco have a multi-year digital security agreement to support the expansion of Sky video services across any screen.

Suprema announced that its Bio-Sign mobile fingerprint authentication algorithm was selected by Samsung for two smartphone models.

Traka UK joined forces with Edesix, to ensure that equipment used across the U.K. Prison Service is safely stored and managed.

TruTag Technologies’ signature authentication solution will be used by Hongyang Biotechnology Co. to protect the livestock supply chain from counterfeiting and diversion.
Visual Management Systems Ltd. was invited to join the Airports Centre of Excellence, which aims to improve the passenger experience.

Vodafone Group joined the prpl Foundation to focus on enabling the security and interoperability of embedded devices.

VTT Technical Research Centre of Finland Ltd. and ITS Russia signed a partnership agreement concerning the development of intelligent transport systems for border crossings.

Watermark Risk Management International, LLC, and TEAM Software, Inc., created a strategic partnership where Watermark will be a preferred provider of consulting services on TEAM software solutions.

WestJet Airlines realized improved efficiency and streamlined communication by partnering with Send Word Now.

Government Contracts

AirMap and the Kansas Department of Transportation will deploy Unmanned Traffic Management technology across Kansas to support the growth of the state’s drone economy and ensure safer skies.

WHO	WHAT	OF/WITH	RESULT

eFolder	Merger	Axcient	The combined product portfolio will simplify the way businesses protect data, ensure IT infrastructure availability, and maximize employee productivity.

SecurityMatters	Partnership	Archer Security Group	The two companies will offer comprehensive solutions that will strengthen critical infrastructure in North America.

Konica Minolta Business Solutions U.S.A., Inc.	Acquisition	TLS.NET	TLS.NET technology expands Konica Minolta’s workplace solutions, allowing clients to securely move their company’s voice services to the cloud.

Motorola	Partnership	Neurala	The partnership will develop intelligent cameras for public safety users, so police officers can efficiently search for objects or persons of interest.

***

STRATEGIC MOVES IN THE NEWS

**THINGS TO WATCH:**

**In the Air:**

- **Airports Centre of Excellence**
- **prpl Foundation**
- **VTT Technical Research Centre of Finland Ltd.**
- **ITS Russia**
- **Watermark Risk Management International, LLC.**
- **TEAM Software, Inc.**
- **WestJet Airlines**

**On the Ground:**

- **Vodafone Group**
- **Visual Management Systems Ltd.**
- **WestJet Airlines**
- **Send Word Now**

**In the Cloud:**

- **Amplify AI**
- **CloudMinds Robotics**
- **Deepstraps**
- **Fusion AI**
- **Oculoc**
- **Pr.ng**
- **Silverstream Technologies Inc.**

**On the Menu:**

- **Aerojet Rocketdyne**
- **Atlas II**
- **Commercial Spaceflight**
- **Exoskeletons**
- **Fusion AI**
- **GlobalSat**
- **High Code**
- **Interstellar**
- **L3Harris Technologies**
- **Maxar Technologies**
- **MicroSpectrum**
- **Newbolts**
- **Project TM**
- **Quanta Labs**
- **Rapid Space**
- **SpaceIL**
- **Starlink**
- **Theia**
- **Unmanned Systems**

**Looking Ahead:**

- **Aerojet Rocketdyne**
- **Bezos Space**
- **Blue Origin**
- **Commercial Spaceflight**
- **CyberPower Systems**
- **Deepstraps**
- **Georgia Tech**
- **Interstellar**
- **L3Harris Technologies**
- **Maxar Technologies**
- **MicroSpectrum**
- **Newbolts**
- **Project TM**
- **Quanta Labs**
- **Rapid Space**
- **Starlink**
- **Theia**
- **Unmanned Systems**
- **Vulcan Space**

**In the Air:**

- **Airports Centre of Excellence**
- **prpl Foundation**
- **VTT Technical Research Centre of Finland Ltd.**
- **ITS Russia**
- **Watermark Risk Management International, LLC.**
- **TEAM Software, Inc.**
- **WestJet Airlines**
U.S. Army, have used eSignLive from VASCO Data Security for secure and compliant electronic signing of documents using Personal Identity Verification cards or Common Access Cards.

AWARDS AND CERTIFICATIONS

Atomic Data attained SOC 3 certification for the seventh year in a row from the American Institute of Certified Public Accountants. Conduent Incorporated was awarded a U.S. patent for technology that automatically recognizes facial expressions using images from low-resolution cameras. Consolidated Communications Holdings, Inc., achieved MEF CE 2.0 certification for carrier grade, interoperable Ethernet services. Day & Zimmermann earned a ranking of 188 on the Forbes America’s Largest Private Companies list. It is also on the Defense News Top 100 List. Everest Technologies received ISO 27001:2013 accreditation for its information security management system. Fornetix, LLC, gained a U.S. patent that covers breakthrough solutions for the management of encryption keys and other security objects. Hesco was placed in the Commander’s Choice category and recognized as a Superior Supplier to the U.S. Defense Logistics Agency. Frost & Sullivan recognized iRiTech, Inc., with the 2017 North American Frost & Sullivan Award for New Product Innovation.


ANNOUNCEMENTS

AngelTrax relocated all operations into a renovated facility that serves as its new headquarters and manufacturing, inventory, and distribution centers. ASSA ABLOY acquired SMI (Shree Mahavir Metalcraft), a leading OEM manufacturer of architectural hardware in India. The Association of Public-Safety Communications Officials (APCO) International and IBM announced that APCO International’s new guide card software will use IBM Watson Speech-to-Text and Watson Analytics. CEDIA and The Electronic Security Association announced a strategic reciprocal training relationship that will expand the educational opportunities for members of both associations. Columbus State University received a grant from the U.S. National Security Agency to develop a new tool for rapid cybersecurity training and curriculum development. EventTracker introduced the EventTracker Partner Program. EY opened its advanced cybersecurity center in Dallas, Texas, to help clients stay ahead of emerging threats. Lantronix, Inc., joined the Kepware IoT Alliance Program. Marks USA, a division of NAPCO, launched a new website at marksusa.com. NXP Semiconductors N.V. is expanding its operations in the United States, enabling its U.S. facilities to manufacture security chips for government applications.

ONVIF announced the final release of Profile T, a draft specification with advanced streaming capabilities that adds in support for H.265 video compression. Proficio expanded into Hong Kong to broaden its presence in the Asia-Pacific region. PSA is working with Matterhorn Consulting to enable PSA members to hire military veterans. Stanley Black & Decker opened a new Breakthrough Innovation center in Boston dedicated to advancing technological innovation in its security business. The Protection Bureau awarded scholarships to 10 children of company employees. Thetaray opened its first U.K. office in London. Top Notch Distributors updated its website at topnotchinc.com. Toshiba Surveillance & IP Video Products Group launched its Safe Scholar program to help schools reduce the total cost of video surveillance system ownership. WatchGuard Technologies acquired Datablink, a provider of advanced authentication solutions. Webroot acquired the assets of Securecast, a security awareness training platform, and launched Webroot Security Awareness Training as a beta program.

Protection of Assets

Protection of Assets (POA) is the premier reference for the security professional. POA is available as an online subscription, an eight-volume set, as individual books, and on Kindle. Individual titles and the set are also available in Spanish.

For details or to order, visit www.protectionofassets.com/sm.
JOHNSON CONTROLS of Westford, Massachusetts, introduced comprehensive automated visitor management as a core component of the C•CURE 9000 security and event management platform with a new self-service Kiosk Application and optional stand offerings that connect through the C•CURE Portal. The release provides for more efficient management of access credential requests. Visitors can self-register using the visitor management Kiosk Application for iOS iPad devices. Once the visit is confirmed by the system and a credential is created, a temporary identification label or card can be printed from the C•CURE 9000 client. An email notification of the visitor’s arrival is promptly sent to the host.

ELECTRIC STRIKES

CAMDEN DOOR CONTROLS of Mississauga, Ontario, Canada, announced that its burglar-resistant electric door strike models CX-ED2079, CX-1079L, and CX-ED1079DL are now UL1034 Certified. The universal electric strikes for cylindrical locksets are supplied with three stainless steel faceplates designed for ANSI square, round, and wood frames. The CX-ED1079L low-profile and CX-ED1079DL standard-depth Grade 1 ANSI strikes offer selectable 12/24V AC/DC and fail-safe/fail-secure operation. They have full horizontal adjustment and built-in latch monitoring. The CX-ED2079 low-profile Grade 2 ANSI electric strike provides the same features.

ENTRY SENSOR

Chicago-based FIBARO is now shipping the Door/Window Sensor 2, a Z-Wave Plus certified smart home device. A slim, smart sensor that can be installed on any door, window, or gate in the home or office, it can be connected to Fibaro’s Home Center ecosystem or a Z-Wave hub and accessed through the accompanying smart app on a phone, tablet, or browser. It monitors the status of the opening and reports any change in open/close status. New features include an internal temperature sensor and features that come with the upgraded Z-Wave platform, including longer battery life, faster operation, better RF coverage, and easier installation.

CHEMICAL AND NOISE SENSOR

Addressing two challenges for schools, Fly Sense is a cloud-based platform that detects and sends alerts to school officials when bullying or vaping is taking place in bathrooms and other parts of a school. Made by DIGITAL FLY of Hauppauge, New York, Fly Sense identifies chemicals from vaping and cigarettes instantaneously and alerts officials within three to five seconds. It also tracks decibels of noise and alerts users to changes that might indicate that bullying or fighting is occurring. The Fly Sensor edge detection sensor works with a back-end logic processing server. Each Fly Sensor can work independently or in conjunction with a network of sensors.
SECURITY ROBOT

SFC ENERGY of Brunthal/Munich, Germany, announced that its EFOY Pro fuel cells are integrated into Roboguard, an autonomous security robot developed by Singapore-based ONEBERRY TECHNOLOGIES. Roboguard can operate autonomously and maintenance-free for up to a month without intervention. Then a one-minute hot-swap of the fuel cartridge allows the robot to return to operation quickly. The unit addresses the manpower shortage in the Singapore security sector and raises the level of security for clients. 1108

SECURITY MANAGEMENT

MAVIN TECHNOLOGIES of Rochester, New York, introduced version 5.2 of its Mavin Security Management Platform. The new version gives users the ability to deploy client workstation upgrades from a central location, decreasing the amount of time required to deploy new software. When enabled, it automatically downloads and installs the latest version. It also can automatically delete old database backups for efficient storage. Version 5.2 supports an updated system integration to the FLIR DVTel Latitude 7.0 video management system. New script reports and people-related filters have also been implemented in this release. 1107

INCIDENT SUPPORT

In the event of a major incident, companies need to account for employees who might be affected. To accomplish this and provide other support for traveling employees, INTERNATIONAL SOS of Trevose, Pennsylvania, and CONTROL RISKS of Washington, D.C., collaborated to launch TravelTracker Incident Support. It automatically initiates communications with potentially impacted mobile workers immediately after any major incident. The International SOS global network of security experts investigates and validates reports of major incidents in less than 30 minutes. As soon as the validation is complete, the service will automatically contact members through multiple communication methods, including email, SMS, and text-to-speech protocols. Collated responses are provided to customers within the following hour, and assistance will begin if needed. 1108

ACCESS CONTROL

A new site security system from CREDENTIAL VERIFICATION SERVICE of Rockville, Maryland, lets security managers track in real time all employees and contractors who are entering a worksite or building. To enter, the individual places an RFID-enabled photo ID card within an inch of a reader. The card connects to a cloud-based database to give security staff the information needed to determine whether to admit or deny entry. The readers record the time and location of each tap, and can record each exit. The system can be connected to turnstiles for automated entry. Readers can be secured to a fixed physical location or used as mobile devices, and multiple entry/exit points can be configured. 1109

IP DOME CAMERA

TOSHIBA SURVEILLANCE & IP VIDEO PRODUCTS GROUP of Irvine, California, introduced a new line of five-megapixel IP dome cameras that deliver advanced networking and viewing capabilities. Available as a vandal-resistant outdoor model (IK-WR51A) or an indoor version (IK-WD51A), the new cameras enhance security, safety, and operational strategies with full-frame HD video at 30 frames per second, adaptive infrared illuminators that automatically adjust LED intensity, and Hallway View that lets users rotate their cameras’ perspectives to accurately capture narrow vertical areas such as tunnels, retail aisles, or corridors. Smart Codec H.265 compression assists in reducing video storage and bandwidth costs without compromising critical image quality. 1105
PARKING ENFORCEMENT

GENETEC INC. of Montreal, Canada, introduced the Genetec AutoVu Motoscan, a new scooter-mounted parking enforcement solution. Designed for the traditionally narrow streets of European cities, Motoscan is a lightweight, low-power, fully-featured license plate recognition unit that can be mounted on a smaller vehicle such as a scooter. Equipped with automatic number plate recognition cameras, the system automatically scans license plates and sends the information to the parking authority, which will identify parking violations and issue tickets as required. The compact unit combines all critical components onto a single device to keep the weight low. 1110

NOTIFICATION DEVICES

EATON of Long Branch, New Jersey, launched its Wheelock Exceder LED notification appliances that comply with the latest National Fire Protection Association (NFPA) code requirements for flash duration. Eaton’s energy-efficient LED design requires less power, allowing more devices to be connected to fewer power supplies and reduce overall costs. The line includes strobes, horns, speakers, speaker strobes, low-frequency sounder strobes, and sounders for both ceiling and wall-mount indoor applications. The high-fidelity speakers provide leading intelligibility for mass notification and emergency communications. Because the units meet NFPA’s 20-millisecond flash duration requirements for strobes, customers can mix xenon and LED devices in the same field of view. 1111

PERIMETER SENSOR

SOUTHWEST MICROWAVE of Tempe, Arizona, expanded its high-reliability digital microwave sensor array with the INTREPID Model 336-33464, a standalone volumetric perimeter sensor for maximum-security sites such as nuclear power plants and military installations. Combining proven detection performance with advanced embedded digital signal processing to discriminate between intrusion attempts and environmental disturbances, the sensor mitigates risk of site compromise and prevents nuisance alarms. Designed for maximum protection against physical tampering and harsh environmental conditions, the sensor features heavy-duty components and packaging, integrated radome tamper switches, and optional steel enclosures for external connections. Advanced shielding protects electronics against electromagnetic or radio frequency interference. Standalone configuration and on-board relay alarm outputs for monitoring deter the risk of hacking or other digital compromise. 1112

HYBRID ILLUMINATORS

RAYTEC of Ashington, Northumberland, United Kingdom, released new VARIO2 IP Hybrid Illuminators that combine four key technologies in a single package. Each illuminator combines infrared, white light, IP connectivity, and power over Ethernet technology to deliver the right light for any situation. They use PLATINUM Elite twin-core SMT LEDs, which are individually 200 percent more powerful than previous generation LEDs. Fully IP addressable, the illuminators are operated remotely with a user-friendly interface that allows users to control lighting at any time to respond to live events or make easy remote adjustments. They can also be fully integrated with video management systems and other third-party devices. 1113
Professional development is a key driver for career advancement. In addition to staying on top of the latest threats and risk management strategies, a solid understanding of core security principles and field-tested best practices is essential. This is the type of vital information you’ll find in our March line-up of educational programming.

CPP Review Program  
March 12-13, 2018  
This program provides an accelerated, high-level overview of the security concepts and practices assessed on the Certified Protection Professional (CPP®) exam. It allows you to identify your areas of strength and weakness in the seven key domains of the exam, so you can develop a personalized study plan.

PSP Review Program  
March 12-13, 2018  
Intended to supplement your other certification exam preparation activities, the program provides a high-level overview of the three key domains assessed on the Physical Security Professional (PSP®) exam. Identify your areas of strength and weakness to build a study plan focused on the areas you need the most.

Assets Protection Course™: Principles of Security  
(APC I)  
March 12-15, 2018  
You can’t advance in the profession without a strong foundation. Make sure your fundamental knowledge of assets protection and its universal principles is rock-solid. Acquire a broad strategic overview of key security principles and best practices, from A to Z, for thriving in the security environment.

Learn more and register at asisonline.org/education
**Marketplace**

**Bullet Camera**

**Lilin Americas** of Arcadia, California, part of Merit LILIN, strengthened its line of IP cameras with the MR832 outdoor bullet camera, which features a 4-millimeter fixed lens with an IP66 environmental rating, an operating range of –40 to +122 degrees Fahrenheit, and day/night imaging. The IP outdoor cameras are easy to install, configure, and maintain. They integrate seamlessly, offer high-resolution HD images even in complete darkness, and are competitively priced. The cameras feature 2D wide dynamic range and 3D Noise Reduction for maximum clarity in low light conditions. Energy-efficient infrared LEDs automatically illuminate scenes in complete darkness for discovering subjects at a range of up to 30 meters. 1114

**Biometric Access**

**ZKAccess** of Fairfield, New Jersey, launched the ProBio-ID, a multi-biometric access control device with SilkID technology. It offers both security and convenience in a single, easily installed standalone device. ProBio-ID connects directly to door locks or panels like a common keypad or RFID card reader. ProBio-ID can read faces, fingerprints, RFID cards, PIN codes, and any combination of those four credentials. Its face recognition camera provides true hands-free access control. ProBio-ID also includes a ZKAccess next-generation SilkID fingerprint sensor which provides superior accuracy and speed matching. 1115

**Designer Turnstiles**

**Delta Turnstiles** of Concord, California, introduced its new Designer Series turnstiles. The new models offer the same functionality and high level of security provided by standard Delta models, but are designed for style. Their circular shape makes them especially distinctive and adds an aesthetic dimension to any space. The Infinity model uses bidirectional optical technology and features the additional deterrence of swinging glass/acrylic barriers. Designed with a seamless unibody construction and made of cold rolled steel, it is available in a variety of colors or a chrome finish. 1116

**Statement of Ownership, Management, and Circulation**

1. Title of Publication: Security Management
2. Pub. No. 263540 / ISSN#0145-9406
3. Filing Date: September 19, 2017
4. Frequency of Issue: Monthly
5. Number of Issues Published Annually: 12
6. Annual Subscription Price: $60 (from dues)
7. Location of Publication: ASIS International, 1625 Prince Street, Alexandria, VA 22314
9. Name and Address of Publisher, Editor, and Managing Editor: Publisher: Nello Caramat; Editor: Teressa Anderson; Managing Editor: Matthew Kreider; ASIS International, 1625 Prince Street, Alexandria, VA 22314
10. Owner: ASIS International, 1625 Prince Street, Alexandria, VA 22314
11. Known bondholders, mortgagees, and other security holders owning or holding one percent or more of total amount of bonds, mortgages, or other securities: None.
12. The purpose, functions, and nonprofit status of this organization and the exempt status for federal income tax purposes has not changed during the preceding 12 months.
13. Issue Date for Circulation Data: 09/01/2017
14. Extent and Nature of Circulation:
15. Average # of copies each issue during preceding 12 months
   Actual # of single issues published nearest to filing date

A. Total no. of copies printed: 34,808 39,674
B. 1. Paid/requested outside-county mail subscriptions 21,665 21,619
   2. Paid in-county subscriptions 0 0
   3. Sales through dealer and carriers, street vendors, countersales, and other non-USPS paid distribution 8,570 8,569
   4. Other classes mailed through USPS 85 82
C. Total paid and/or requested circulation 30,321 30,270
D. 1. Free dist. by mail outside-county 3,033 450
   2. Free dist. by mail in-county 0 0
   3. Free dist. by mail other classes through USPS 50 50
   4. Other classes mailed through USPS 956 8,481
E. Total free distribution 4,038 8,981
F. Total distribution 34,359 39,251
G. Copies not distributed 449 423
H. Total 34,808 39,674
I. Percent paid and/or requested circulation 88% 77%
J. I certify that all information furnished on this form is true and complete. I understand that anyone who furnishes false or misleading information on this form or who omits material or information requested on the form may be subject to criminal sanctions (including fines and imprisonment) and/or civil sanctions (including civil penalties).
   Nello Caramat, Publisher
REQUEST DETAILED PRODUCT INFORMATION THROUGH OUR MONTHLY E-RESPONSE, VISIT HTTP://SECURITYMGMT.HOTIMS.COM, OR USE YOUR SMART PHONE TO ACCESS THE QR CODE ON THIS PAGE.

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

ADVERTISERS ONLINE

Abloy Security, Inc.
www.abloyusa.com

Ameristar Security Products
www.ameristarsecurity.com

Axis Communications
www.axis.com

B.I.G. Enterprises
www.bigbooth.com

Comport Technologies
www.comm-port.com

Detex Corporation
www.detex.com

dormakaba
go.dormakaba.com/PAS-SMMag

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

DSX Access Systems, Inc.
www.dsxinc.com

GAI-Tronics Corporation
www.gai-tronics.com

Garrett Metal Detectors
www.garrett.com

Hikvision USA
www.hikvision.com

Honeywell
www.honeywell.com

Mission 500
www.mission500.org

NC4
www.nc4.com

Research Electronics, Int’l
www.reiusa.net

SDC - Security Door Controls
www.sdcsecurity.com

SecurAmerica
www.securamericallc.com

Special Response Corporation
www.specialresponse.com

WM Security Services, Inc. (WMSSI)
www.wmssiwin.com

CIRCLE #  PAGE #
11  Abloy Security, Inc. .................................. 22
22  Ameristar Security Products .............. 41
02  Axis Communications ....................... 04
25  B.I.G. Enterprises ......................... 57
20  Comport Technologies .................. 37
08  Detex Corporation .............. 17
10  dormakaba ......................... 19
13  DSI (Designed Security Inc.) ....... 25
32  DSX Access Systems, Inc. .......... 76
14  GAI-Tronics Corporation ............ 26
24  Garrett Metal Detectors ............. 47
03  Hikvision USA ......................... 06
06  Honeywell ......................... 13
31  Mission 500 ......................... 75
16  NC4 ................................ 30
17  Research Electronics, Int’l ....... 31
07  SDC - Security Door Controls ........ 16
01  SecurAmerica .............. 03
12  Special Response Corporation ...... 23
21  WM Security Services, Inc. (WMSSI) ..... 39
ISIS and climate change are the leading threats to national security across the globe, according to a Pew Research Center survey of people in 38 countries. In 18 of those countries—mostly those in Europe, the Middle East, Asia, and the United States—individuals named ISIS as the top threat, while respondents from Latin American and African nations identified global climate change as the topmost threat.

ISIS is the top concern in the U.S. and across much of Europe

Those with less education feel more threatened by refugees

<table>
<thead>
<tr>
<th>Country</th>
<th>More Education</th>
<th>Less Education</th>
<th>DIFF</th>
</tr>
</thead>
<tbody>
<tr>
<td>Greece</td>
<td>54</td>
<td>72</td>
<td>+21</td>
</tr>
<tr>
<td>Hungary</td>
<td>57</td>
<td>68</td>
<td>+20</td>
</tr>
<tr>
<td>Italy</td>
<td>52</td>
<td>67</td>
<td>+18</td>
</tr>
<tr>
<td>Poland</td>
<td>51</td>
<td>63</td>
<td>+16</td>
</tr>
<tr>
<td>Spain</td>
<td>46</td>
<td>61</td>
<td>+15</td>
</tr>
<tr>
<td>France</td>
<td>45</td>
<td>61</td>
<td>+14</td>
</tr>
<tr>
<td>U.K.</td>
<td>42</td>
<td>61</td>
<td>+14</td>
</tr>
<tr>
<td>U.S.</td>
<td>40</td>
<td>59</td>
<td>+12</td>
</tr>
<tr>
<td>Netherlands</td>
<td>30</td>
<td>56</td>
<td>+11</td>
</tr>
<tr>
<td>Germany</td>
<td>32</td>
<td>53</td>
<td>+11</td>
</tr>
<tr>
<td>Canada</td>
<td>29</td>
<td>52</td>
<td>+10</td>
</tr>
<tr>
<td>Sweden</td>
<td>26</td>
<td>53</td>
<td>+7</td>
</tr>
</tbody>
</table>

Source: Globally, People Point to ISIS and Climate Change as Leading Security Threats, Pew Research Center, August 2017
Together we can

Educate

Inspire

Heal

Nourish

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

Supporting Families Across America
CREATING THE FUTURE OF SECURITY... TODAY

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

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

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

DSX Access Systems, Inc.

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

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


For product info #32 securitymgmt.hotims.com