Issue & Beyond

- Extremists: Censoring radical content online.
- Passwords: Practicing good cyber hygiene.

28 Preventive Investigations

38 Resilience

44 Museums

52 Discrimination
LET ME BE FRANK.

In 2017, our revenue run rate will be approximately $200 million, making us one of the top 7 security companies in the U.S.

We have a national footprint. We want to be on your bid list. If given a chance to bid on your account, our goal will be to reduce your total spend and provide better service!

HAVE YOU HEARD THE LATEST JOKE GOING AROUND THE INDUSTRY?

A security professional says to the customer, “My security company has just merged with another security company, and that is going to be great for you!”

The customer then says, “I heard you had to cut your service delivery team in half.”

The security professional responds, “Yes, but trust me, this is going to be great for you!”

For the first ten people to reach out and tell me they’ve heard this joke, I will donate $1,000 to the charity of the choice. For anyone who actually believes this joke, email me; I want to sell you some land in Arizona.

LETMEBEFRANK@SECURAMERICALLC.COM

WWW.SECURAMERICALLC.COM
THE ART OF VIDEO SURVEILLANCE

The ability to adapt and scale are essential in the security industry. The fact that we manufacture our own products and invest heavily in R&D, enables us to be VERSATILE and responsive to the demands of the industry.
“An assessment found that there were issues affecting 10 to 20 percent of the national system.”

The 2011 results of the first test of the U.S. Emergency Alert System, which was installed in 1997. PAGE 15

**BY THE NUMBERS**

**35**
The percentage of Muslim women who are employed in the United Kingdom, as compared to 69 percent of all working-age women. PAGE 53

**8M**
The number of items in the collection of the British Museum, all of which must be protected by the museum’s security team. PAGE 45

**138**
The number of attacks worldwide targeting food and water supplies between 1994 and 2014, according to the Global Terrorism Database. PAGE 39

**“You cannot mitigate a risk that you have not anticipated.”**

Joseph M. LaSorsa, CPP, on using intelligence gathering to prevent workplace violence. PAGE 30

**“I have access to the president’s office if I need it. But I really do not like to exercise that option. I prefer to work with my peers.”**

Incoming ASIS President Thomas J. Langer, CPP, on working effectively with the C-suite. PAGE 37

**“I think we can all agree that removing the worst content is a good starting place and should be uncontroversial.”**

Mark Wallace, CEO of the Counter Extremism Project, on removing radical content from the Internet. PAGE 19

BY THE NUMBERS

35
The percentage of Muslim women who are employed in the United Kingdom, as compared to 69 percent of all working-age women. PAGE 53

8M
The number of items in the collection of the British Museum, all of which must be protected by the museum’s security team. PAGE 45

138
The number of attacks worldwide targeting food and water supplies between 1994 and 2014, according to the Global Terrorism Database. PAGE 39

“An assessment found that there were issues affecting 10 to 20 percent of the national system.”

The 2011 results of the first test of the U.S. Emergency Alert System, which was installed in 1997. PAGE 15

**BY THE NUMBERS**

35
The percentage of Muslim women who are employed in the United Kingdom, as compared to 69 percent of all working-age women. PAGE 53

8M
The number of items in the collection of the British Museum, all of which must be protected by the museum’s security team. PAGE 45

138
The number of attacks worldwide targeting food and water supplies between 1994 and 2014, according to the Global Terrorism Database. PAGE 39

“An assessment found that there were issues affecting 10 to 20 percent of the national system.”

The 2011 results of the first test of the U.S. Emergency Alert System, which was installed in 1997. PAGE 15

**BY THE NUMBERS**

35
The percentage of Muslim women who are employed in the United Kingdom, as compared to 69 percent of all working-age women. PAGE 53

8M
The number of items in the collection of the British Museum, all of which must be protected by the museum’s security team. PAGE 45

138
The number of attacks worldwide targeting food and water supplies between 1994 and 2014, according to the Global Terrorism Database. PAGE 39

“An assessment found that there were issues affecting 10 to 20 percent of the national system.”

The 2011 results of the first test of the U.S. Emergency Alert System, which was installed in 1997. PAGE 15

**BY THE NUMBERS**

35
The percentage of Muslim women who are employed in the United Kingdom, as compared to 69 percent of all working-age women. PAGE 53

8M
The number of items in the collection of the British Museum, all of which must be protected by the museum’s security team. PAGE 45

138
The number of attacks worldwide targeting food and water supplies between 1994 and 2014, according to the Global Terrorism Database. PAGE 39

“An assessment found that there were issues affecting 10 to 20 percent of the national system.”

The 2011 results of the first test of the U.S. Emergency Alert System, which was installed in 1997. PAGE 15

**BY THE NUMBERS**

35
The percentage of Muslim women who are employed in the United Kingdom, as compared to 69 percent of all working-age women. PAGE 53

8M
The number of items in the collection of the British Museum, all of which must be protected by the museum’s security team. PAGE 45

138
The number of attacks worldwide targeting food and water supplies between 1994 and 2014, according to the Global Terrorism Database. PAGE 39

“An assessment found that there were issues affecting 10 to 20 percent of the national system.”

The 2011 results of the first test of the U.S. Emergency Alert System, which was installed in 1997. PAGE 15

**BY THE NUMBERS**

35
The percentage of Muslim women who are employed in the United Kingdom, as compared to 69 percent of all working-age women. PAGE 53

8M
The number of items in the collection of the British Museum, all of which must be protected by the museum’s security team. PAGE 45

138
The number of attacks worldwide targeting food and water supplies between 1994 and 2014, according to the Global Terrorism Database. PAGE 39

“An assessment found that there were issues affecting 10 to 20 percent of the national system.”

The 2011 results of the first test of the U.S. Emergency Alert System, which was installed in 1997. PAGE 15

**BY THE NUMBERS**

35
The percentage of Muslim women who are employed in the United Kingdom, as compared to 69 percent of all working-age women. PAGE 53

8M
The number of items in the collection of the British Museum, all of which must be protected by the museum’s security team. PAGE 45

138
The number of attacks worldwide targeting food and water supplies between 1994 and 2014, according to the Global Terrorism Database. PAGE 39

“An assessment found that there were issues affecting 10 to 20 percent of the national system.”

The 2011 results of the first test of the U.S. Emergency Alert System, which was installed in 1997. PAGE 15

**BY THE NUMBERS**

35
The percentage of Muslim women who are employed in the United Kingdom, as compared to 69 percent of all working-age women. PAGE 53

8M
The number of items in the collection of the British Museum, all of which must be protected by the museum’s security team. PAGE 45

138
The number of attacks worldwide targeting food and water supplies between 1994 and 2014, according to the Global Terrorism Database. PAGE 39

“An assessment found that there were issues affecting 10 to 20 percent of the national system.”

The 2011 results of the first test of the U.S. Emergency Alert System, which was installed in 1997. PAGE 15

**BY THE NUMBERS**

35
The percentage of Muslim women who are employed in the United Kingdom, as compared to 69 percent of all working-age women. PAGE 53

8M
The number of items in the collection of the British Museum, all of which must be protected by the museum’s security team. PAGE 45

138
The number of attacks worldwide targeting food and water supplies between 1994 and 2014, according to the Global Terrorism Database. PAGE 39

“An assessment found that there were issues affecting 10 to 20 percent of the national system.”

The 2011 results of the first test of the U.S. Emergency Alert System, which was installed in 1997. PAGE 15

**BY THE NUMBERS**

35
The percentage of Muslim women who are employed in the United Kingdom, as compared to 69 percent of all working-age women. PAGE 53

8M
The number of items in the collection of the British Museum, all of which must be protected by the museum’s security team. PAGE 45

138
The number of attacks worldwide targeting food and water supplies between 1994 and 2014, according to the Global Terrorism Database. PAGE 39

“An assessment found that there were issues affecting 10 to 20 percent of the national system.”

The 2011 results of the first test of the U.S. Emergency Alert System, which was installed in 1997. PAGE 15

**BY THE NUMBERS**

35
The percentage of Muslim women who are employed in the United Kingdom, as compared to 69 percent of all working-age women. PAGE 53

8M
The number of items in the collection of the British Museum, all of which must be protected by the museum’s security team. PAGE 45

138
The number of attacks worldwide targeting food and water supplies between 1994 and 2014, according to the Global Terrorism Database. PAGE 39

“An assessment found that there were issues affecting 10 to 20 percent of the national system.”

The 2011 results of the first test of the U.S. Emergency Alert System, which was installed in 1997. PAGE 15

**BY THE NUMBERS**

35
The percentage of Muslim women who are employed in the United Kingdom, as compared to 69 percent of all working-age women. PAGE 53

8M
The number of items in the collection of the British Museum, all of which must be protected by the museum’s security team. PAGE 45

138
The number of attacks worldwide targeting food and water supplies between 1994 and 2014, according to the Global Terrorism Database. PAGE 39

“An assessment found that there were issues affecting 10 to 20 percent of the national system.”

The 2011 results of the first test of the U.S. Emergency Alert System, which was installed in 1997. PAGE 15
We care.

Staying with you all the way.

Axis Technical Support provides efficient assistance for your Axis product – from extended warranties and repair, to our Helpdesk and Chat. With 23 support personnel based locally in North America speaking 7 languages, and over 90 support personnel across the globe speaking more than 15 languages, you can rest assured that you’ll receive assistance wherever you are, whenever you need it.

Visit www.axis.com/support
AN INTELLIGENT SOLUTION

As concerns about workplace violence rise, companies should adopt protective intelligence strategies to prevent attackers from succeeding.

By Joseph M. LaSorsa, CPP
Celebrating our 25 years in business, Mercury Security has perfected the hardware platform of choice for some of the best names in the industry.
Reliable, flexible, and open, the Authentic Mercury platform along with our partners can help you achieve a solid, systemic solution.

Open-up the possibilities. Make sure it’s Merc.
www.mercury-security.com

Give your access control solution wings.
10 SECURITY MANAGEMENT ONLINE
New reports online this month cover issues such as wildlife trafficking, password protection, and water scarcity.

12 EDITOR’S NOTE
Timing is everything.

18 HOMELAND SECURITY
Countries move to ban extremist content online.
By Lilly Chapa

22 CASE STUDY
A bank invests in wireless locks.
By Holly Gilbert Stowell

24 CYBERSECURITY
Build better passwords.
By Megan Gates

56 LEGAL REPORT
A recap of legislation considered by the 114th U.S. Congress.
By Megan Gates

62 INDUSTRY NEWS
Thomas J. Langer, CPP, shares his vision for the future of ASIS International.
By Flora Szatkowski

63 ASIS BOARD OF DIRECTORS

70 MARKETPLACE

73 ADVERTISER INDEX

74 Q&A
Mo Canady discusses school resource officers.

NEWS & TRENDS
Testing an emergency alert system, and protecting wildlife.
By Mark Tarallo
PASSWORDS
Sixty-three percent of confirmed data breaches in 2015 involved leveraging weak, default, or stolen passwords, according to the 2016 Verizon Data Breach Incident Report. Attackers used stolen passwords to steal more credentials, export data using malware, and to conduct phishing.

AIRPORTS
The U.S. Congress passed legislation to verify that airports have working plans in place to respond to security incidents inside their perimeters. Plans must include procedures for responding to active shooters, acts of terrorism, and incidents that target passenger-screening checkpoints.

INFORMATION SECURITY
As part of its Global State of Information Security Survey 2017, Price-waterhouseCoopers asked financial institutions about cyberattacks, cloud adoption, and the Internet of Things. Among the findings: 35 percent of institutions cited “threats from outside the country” as their biggest IT security challenge.

WATER SCARCITY
How will water problems impact U.S. national security interests over the next 30 years? The U.S. Office of the Director of National Intelligence studied this question. Its report describes possible water shortages, poor quality, and floods that could cause political and economic instability.

TERRORISM INSURANCE
The U.S. Congress reauthorized the Terrorism Risk Insurance Program, which allows the federal government to repay business costs following a catastrophic attack that costs more than $200 million.

DISCRIMINATION
Muslim women face a triple penalty job searching in Europe—race, gender, and religion—according to a report issued by the U.K. Parliament’s Women and Equalities Committee.

NEW ONLINE THIS MONTH at www.securitymanagement.com

WILDLIFE TRAFFICKING
Terrorist groups, transnational crime organizations, and even rogue security personnel are all contributing to the growing international problem of wildlife trafficking, a multibillion-dollar international criminal activity. Besides endangering rare species, wildlife trafficking contributes to instability and violence. A recent study of the issue by the U.S. Government Accountability Office, Combating Wildlife Trafficking, examines the problem and some potential remedies. Read the report and watch video related to the report via SM Online.
When the situation turns dark, you can respond at the speed of light.

Quick one-button lockdown secures front doors against outside threats.

Preventing entry by anyone posing an immediate threat can be a serious challenge. If it’s your responsibility to protect students and staff from intruders, now you have a choice: rely on traditional manual locking for front doors—or install a Detex Lockdown system to instantly secure the main doors.

In these situations, timing is truly everything. With the Detex Lockdown system, a centrally located control switch secures panic hardware devices on the doors, saving precious time. There’s no searching for keys, no need for someone to run to the front doors and attempt to secure them while under pressure. Just one person pushing the Detex Lockdown button can control the threat.

*EasyKit*® Whether your campus buildings are decades old or only a blueprint, visit www.detex.com/lockdown and let us help you identify your ideal lockdown system.

800-729-3839

Where Trust is Built®
Life Safety and Security Door Hardware

For product info #3 securitymgmt.hotims.com
On May 10, 1869, Leland Stanford was poised to drive the last spike connecting the Union Pacific Railroad and the Central Pacific Railroad, creating a rail line that would span the entire United States for the first time. Stanford and his fellow executives felt that the entire country should share in this moment. Railroad employees connected the railroad spike to a telegraph so that when the final blow was struck, a signal would go out to the whole nation at one time.

Stanford missed the spike completely, but the telegraph operator manually pushed the transmit button, according to Michael O’Malley, author of *Keeping Watch: A History of Time in America*, who told the tale to the hosts of the Backstory podcast.

However, the signal that emanated that day would become a wakeup call. As newspapers reported the event, the official time was drastically different all over the country because there were no standard time zones.

As transit and communications technology marched forward, time zones began to coalesce around railroads because timetables had to be synchronized. Eventually, under pressure from the government, the railroads devised a system of five time zones.

The United States was not alone in these efforts. The entire world was in a frenzy to compete in a great age of technological innovation. Efficiency was paramount and depended on an effective measurement of time, according to Vanessa Ogle, professor of history at the University of Pennsylvania and author of *The Global Transformation of Time*.

“Fine-tuning schedules and timetables for trains and telegraphs became one of the major preoccupations of nation-states eager to move forward,” Ogle writes in “A Briefer History of Time,” in *Foreign Affairs*. “But for national times to be rational and efficient, they had to be integrated with other national times, initially those of neighboring states but increasingly of the whole world.”

As 2017 begins, it is difficult to imagine a world without instant communication, which completely removes time as a barrier. ASIS International is dedicating the new year to using communication to better serve members all over the world. Headquarters staff are fine tuning strategies, devising fresh approaches, and developing innovative content. We retired Dynamics, our member newsletter delivered in a PDF format, and will soon roll out a more robust and accessible member communications vehicle. (At this time, subscribers to *euroDynamics*, *Asia-Pacific Dynamics*, and *Middle East Dynamics* will continue to receive monthly e-newsletters.) ASIS will unveil a more user-friendly website and offer even more ways to engage through revitalized chapter and council structures.

Incoming ASIS President Thomas J. Langer, CPP, discusses his vision for the future in an interview on page 36. This vision emphasizes efficient outreach and communication with members in this new great age of innovation.
When you prepare, you prevent. Preparedness brings peace of mind. And G4S can help you stay ready, with everything from risk analysis and managed services to technology and security officers. To stay prepared, please visit g4s.us or call 855-622-5544.
WHEN ADMIRAL JAMIE BARNETT took over as chief of public safety and homeland security at the U.S. Federal Communications Commission (FCC) in 2009, he learned something interesting about the Emergency Alert System (EAS). “It had never been used, and it had never been tested,” he says.

The never-been-tested part was surprising, because by that time the EAS had been around since 1997, when it replaced the Emergency Broadcast System. And the importance of having a well-functioning system seemed undeniable. “If the president were concerned that North Korean missiles were headed our way, he would have the ability, in essence, to preempt all the programming in the United States, pick up a mic, and say ‘We are under attack,’” Barnett says.

So Barnett sent a memo to the chairman of the FCC, expressing concerns about the viability of a system that had never been tested on a nationwide basis, and in fact had never even been scheduled for such a test. In turn, the FCC chairman sent the message up the chain, and it eventually reached the White House. After input from leading agencies such as the National Association of Broadcasters, the U.S. Federal Emergency Management System, and the White House Military Office, the administration decided to conduct a national EAS test on November 9, 2011.

What these officials were testing was a system that is a great-grandchild of the Cold War. Up until 1950, the government had no real method for broadcasting warnings to the nation at large. In 1951, U.S. President Harry S. Truman established an early emergency broadcast system, CONELRAD (Control of Electromagnetic Radiation), that was primarily designed to alert the public in the event of a Soviet attack during the Cold War. When new defense technology reduced the likelihood of a Russian bomber attack, CONELRAD was replaced by the Emergency Broadcast System (EBS) in 1963. The EBS was tested on a weekly basis, with stations broadcasting a dis-
tinctive pattern of beeping sounds and a variation of the following announcement:

“This is a test. For the next 60 seconds, this station will conduct a test of the Emergency Broadcast System. This is only a test.” While the system was never used for a national emergency (save for a false alarm in 1971), it was activated thousands of times for regional emergency messages such as severe weather warnings. In 1997, the EBS was expanded to include cable stations, and it became the EAS. (More recently, the government created a Wireless Emergency Alert (WEA) system to disseminate emergency alerts on mobile devices; see Security Management’s December issue for more coverage of that system.)

In sum, the EAS sends audio signals—that distinctive pattern of beeps that the EBS testing formerly made familiar—to 77 primary entry point stations. When these primary stations hear the signals, they immediately transmit it to other stations, so that in a matter of seconds the whole country is covered. “That irritating noise that you hear—that’s actually what the stations are listening for,” Barnett says. In fact, the government prohibits anyone from replicating those irritating beeps in a movie or television program or song. “People have been fined. The FCC would contact you,” he adds.

Although the sending of audio signals may not be cutting edge in terms of technology, it is resilient. “The system is designed to work when nothing else does. If the power is cut, this system will work,” Barnett explains. Since the security technology around the system is continually updated, hacking incidents have been rare; one of the few occurred in Great Falls, Montana, in 2013, when the EAS system at a television station was hacked to broadcast a zombie apocalypse message: “Civil authorities in your area have reported that the bodies of the dead are rising from their graves and attacking the living.”

The 2011 national test, which went generally well, showed there was room for improvement. An assessment found that there were issues affecting 10 to 20 percent of the national system, such as local equipment problems.

For example, some stations experienced a feedback loop in which they started to broadcast the test, but then immediately shut down. One station malfunctioned and went silent during the test, and because dead air is against FCC broadcasting rules, an operator threw on a Lady Gaga CD. “So people heard ‘There is an emergency alert’ and then [the song] Born This Way,” says Barnett, laughing.

Despite these problems, the FCC did not run another test until five years later. That test occurred last September. In a response to an inquiry from Security Management, FCC officials said that early reports indicated that the test went well. “We have received over 24,000 initial reports from Emergency Alert System participants. The reports indicate that the vast majority of EAS participants successfully received and retransmitted the test alert,” Rear Admiral (ret.) David Simpson, chief of public safety and homeland security at the FCC, said in a statement. “After EAS participants file their more comprehensive reports, including information on any issues they encountered during the test, we will analyze the data and then work with the Federal Emergency Management Agency (FEMA) and other stakeholders to implement any needed improvements.”

However, given that such national testing is vital for maintaining a viable system, Barnett and others argue that it should be done more frequently.

“I think five years is too long,” Barnett says. “My thought originally was that it needed to become routine, so every two to three years would be about right.”

Nelson Daza, an incident communications expert with Everbridge, argues in favor of annual national testing, to ensure readiness and point out potential infrastructure problems. “FEMA reminds everyone to test local emergency plans and family emergency plans at least once per year, so why does the government not mandate an annual EAS test?” Daza asks. “If we let these systems lie dormant until we need them for an emergency, there’s a very real possibility that we may not be able to get these critical messages out.”

Daza also says he feels that some of the devices and protocols of the EAS need to be updated. He says that the hardware maintained by broadcasters is of limited functionality—it can only broadcast text information in ticker-tape style across the top or bottom of a television set. “Since the EAS system is vital to our national security and to our public safety, it should undoubtedly be a state-of-the-art system,” he explains.

But Daza does disagree with those who argue that the U.S. population’s general move away from broadcast televisions and radio, in favor of Internet-based programming and wireless communications, is making the EAS obsolete.

“WEA, television alerts, and radio alerts are just different channels for delivering a message. Tens of millions of people listen to the radio in their cars every day, and the average person in the U.S. still watches 5 hours of television every day,” he says. “With that many ears and eyes, it would be a mistake to think WEA, which distributes only mobile alerts, will replace emergency alerts broadcast via TV and radio.”

---

**Japanese Say Reliance on Military Force Does More Harm than Good in Fight Against Terrorism**

79% Relying too much on force creates hatred, more terrorism

14% Overwhelming force is the best way to defeat terrorism

7% Don’t know

Wildlife trafficking can contribute to instability and violence, and harm people as well as animals. According to reports, about 1,000 rangers were killed from 2004 to 2014,” says a recent study on the issue by the U.S. Government Accountability Office (GAO), Combating Wildlife Trafficking. Illegal trade in wildlife also fuels corruption, destabilizes local communities that depend on wildlife for ecotourism revenue, and undermines conservation efforts. This illegal practice is primarily driven by demand for exotic pets, culinary delicacies, and medicines. In some cases, it has pushed endangered animal species to the brink of extinction; unlawful capture and slaughter have devastated the populations of tigers, elephants, rhinos, turtles, exotic birds, and pangolins. The latter, a prehistoric mammal covered in scales that resembles an anteater clad in armor, is one of the most trafficked animals on earth, with 100,000 pangolins killed every year. Pangolin scales are sold by the bag in Asia, where some believe they can cure cancer, acne, and a host of other maladies.

Overall, wildlife trafficking results in revenue losses of anywhere from $7 billion to $23 billion, according to estimates from the United Nations Environment Program. In 2012, the price of rhino horn reached roughly $27,000 per pound, which was twice the value of gold at the time and more valuable on the black market than diamonds and cocaine, according to the World Wildlife Fund.

Although the United States is one of the world’s largest end markets for trafficked wildlife, much of the practice relies on an Africa-Asia nexus for supply and sales. For example, illicit elephant ivory is stolen in Africa, and most often comes out of Kenya and Tanzania. It is then shipped to China, Thailand, and Vietnam, with Malaysia and Singapore acting as transshipment hubs, according to a 2014 report, Out of Africa: Mapping the Global Trade in Illicit Elephant Ivory, issued by Born Free USA and C4ADS, two nongovernmental organizations.

Of all the bad actors involved in these practices, transnational organized crime networks are driving the trade. Wildlife trafficking is an increasingly popular area of specialization for international organized crime networks, according to the United Nation’s Office on Drugs and Crime 2016 World Wildlife Crime Report.

Last July, the U.S. State Department’s Transnational Organized Crime Rewards Program identified the Xaysavang Network as an international wildlife trafficking syndicate that facilitated the
Wildlife trafficking, enabled by corruption, contributes to instability and violence in many regions.

killing of elephants, rhinos, and other protected species. Vixay Keosavang, a Lao national, is believed to be the leader of the network, according to the U.S. State Department, which is offering a reward of up to $1 million for information leading to the dismantling of the Xaysavang Network.

Terrorist groups also seem to be involved in wildlife trafficking, but the extent of the involvement is still up for debate. The al-Shabaab militant group is either directly or indirectly (through taxation of illegal goods moving through areas they control) involved with illegal wildlife trade, the GAO report found. There are also some reports that al-Shabaab has been buying and selling ivory to fund military operations, although some argue that evidence of that is inconclusive, the report adds.

Finally, wildlife trafficking, enabled by corruption, contributes to instability and violence in many regions. According to a 2013 report from the U.S. Office of the Director of National Intelligence, systemic corruption enables illegal ivory and horn trade, and in turn the trade exacerbates corruption by making high-value illicit products available to influential officials along the supply chain, such as police, customs officers, and local security personnel.

The movements of armed poachers and traffickers also increases border insecurity; for example, gun battles at the South African border often occur between law enforcement and poachers from Mozambique who are trying to gain access to rhinos in Kruger National Park.

To beef up U.S. efforts to fight wildlife trafficking, President Barack Obama issued an executive order in 2013 that established an interagency task force, with 17 federal agencies as members, charged with developing a strategy to guide the government’s efforts. In 2015, the task force released an Implementation Plan for the National Strategy for Combating Wildlife Trafficking.

Task force agencies, following the implementation plan, are helping to fight wildlife trafficking through a variety of efforts, the GAO report found. But it also found that, “at the strategic level, the task force has not identified performance targets. Without such targets, it is unclear whether the task force’s accomplishments are meeting expectations, making it difficult to gauge progress.”

Given this, the GAO recommends that the secretary of state, the secretary of the interior, and the attorney general jointly work to develop performance targets for the task force. The agencies agreed with the GAO’s recommendation.

---

**BOOK REVIEW**

**THREAT ASSESSMENT**

**BY GREGORY ALLEN AND RACHEL DERR. BUTTERWORTH–HEINEMANN Elsevier.com; 156 pages; $59.95.**

**THREAT ASSESSMENT AND RISK analysis are best understood as a collaboration that commonly uses metrics to try to objectify a subjective process. A key step is to clearly define the threats, hazards, vulnerabilities, and risks and then determine how broad or focused the review should be. Threat assessment matrix metrics vary based on the type of risk analysis that is being conducted. A risk analysis of an individual who threatens to kill a coworker, for example, is different from that of a possible hurricane.**

**Threat Assessment and Risk Analysis: An Applied Approach provides a survey of sources and techniques used to successfully conduct these analyses. The authors examine assessment techniques used on a national level—for example, the U.S. Department of Homeland Security’s Risk Analysis and Management for Critical Asset Protection (RAMCAP)—as well as tools to be used by organizations to deal with local issues, such as enterprise risk management (ERM), a strategy designed to reduce the effects of risk on an organization.**

**The authors do not address issues involving imminent threats such as active shooters, but they do examine mitigation and preparation considerations. Crime prevention through environmental design (CPTED) methodologies are reviewed, as well as the development of emergency action plans. The emphasis here is for organizations to put the risk analysis findings into action beforehand to mitigate risk, to have preparations in place to address risk, and to be able to respond and recover operations quickly.**

**Blending writing styles and content can be a challenge, and there are some flaws in transitions and consistency. A glossary of terminology would have been helpful. The book is not comprehensive enough to be a how-to manual, but it provides a useful platform for discussing the range of metrics available to address the challenge of identifying and analyzing risks.**

**REVIEWER:** George Okaty, CPP, is a past member of the ASIS School Safety and Security Council. He is director of safety and security for the Tidewater Community College in Norfolk, Virginia, and is a past board member of the Virginia Association of Campus Law Enforcement Administrators.
It may be unsurprising that oppressive regimes are throttling Internet access. But national security leaders in many nations around the world are working with social media platforms to restrict content that encourages violent extremism, which privacy advocates say is no different from the Internet censorship taking place in North Africa and the Middle East.

ISIS and other extremist groups are using social media platforms excessively—and effectively—to recruit members, raise money, and spread their ideologies. In May, digital platforms, including Facebook, Twitter, YouTube, and Microsoft, signed a European Commission Code of Conduct agreeing to remove “illegal, online hate speech” from their sites. Since then, Twitter has stepped up its monitoring of users’ content, deleting hundreds of thousands of accounts linked to radical extremism. Facebook will remove any content celebrating terrorism. And Google redirects people searching for information about ISIS to anti-extremism websites.

However, privacy advocates note that there is no standing definition of illegal online hate speech, and that there is no way that censorship by social media platforms can be
objective. Indeed, Facebook is working with Israeli officials to remove pro-Palestinian posts that incite violence against Israel. In September, Israeli officials noted that Facebook, Google, and YouTube are complying with 95 percent of the government’s requests to delete content.

“What is extremist speech? The state doesn’t know,” says Shahid Buttar, director of grassroots advocacy at the Electronic Frontier Foundation, a nonprofit civil liberties defense organization. “And when it’s tried to define it, online or offline, it has always swept up constitutionally protected speech. It’s well documented that people silence themselves when they know they’re being watched.”

Buttar points to the recent removal of the famous Napalm Girl photo—depicting the aftermath of a napalm attack on a village during the Vietnam War—from Facebook, which does not permit its users to post content containing nudity. After worldwide backlash, Facebook reinstated the photo on its site. Buttar says sites like Facebook use algorithms to flag content that violates their terms of use, and that the context of the content—in this case, a series of iconic war images—is lost. “There’s a content-based discrimination implicit in the algorithmic approach that is obscured in the security conversation,” he notes.

Mark Wallace, the CEO of the Counter Extremism Project (CEP), helped develop one of those algorithms. Wallace explains that the nonprofit CEP “fills the gaps” when it comes to fighting extremists on a theater that has moved from sea, land, and air to online. Wallace worked with Hany Farid, who previously developed an algorithm to identify child pornography online, to find a way to report violent extremist images. The technology uses hashing, which identifies the unique digital signature of audio, video, or images and scans a database for matches—in this case, of violent beheading videos and other powerful extremist recruiting tools. The algorithm will automatically report the content to the host platform, which will ostensibly remove it.

“We have collected systematically thousands of video, audio, and photographic items that we think are extremist content,” Wallace tells Security Management. “We can take that database, and it immediately identifies that content wherever it resides on those platforms, including at the Internet Service Provider (ISP) level. The Internet has been a very welcoming place to the cyber jihadi. We hope our algorithm will be the mechanism to make the Internet and social media companies no longer a welcoming place for them.”

Wallace notes that researchers are responsible for initially identifying extremist content, but the same content tends to emerge repeatedly. He points to the messages of Anwar al-Awlaki, an al Qaeda recruiter and U.S. citizen who was killed in 2011 by a CIA drone strike.

“If you look at the domestic terror prosecutions here in the United States, a majority of those tried were radicalized by al-Awlaki’s videos from the grave,” Wallace says. “That’s content we know, and hopefully will be able to remove from social media platforms instantaneously.”

Free speech activists also identify al-Awlaki as a prime example of censorship, but for different reasons. There was a federal court proceeding at the time of al-Awlaki’s death in which his family sought due process for him, but he was killed before the courts could address the situation, experts say.

Wallace and the CEP are currently working with social media platforms and governments around the world to deploy their algorithm “in a manner that is effective and responsible,” he says.

“I think we can all agree that removing the worst of the worst content is a good starting place and should be uncontroversial,” Wallace says. “Maybe the next Jihadi John will realize that no longer is a video of a terrorist with his knife at the neck of some poor soul used as a tool to glorify a terrorist...
group, to propagandize, to call others to act, to fundraise, and to recruit.”

Meanwhile, the Middle East, North Africa, and Russia are still dealing with an increase in state-mandated Internet shutdowns. William Buchanan, a computing professor at Edinburgh Napier University, explains that Internet traffic goes through a countrywide firewall. In times of crisis, the country’s leaders can control the main firewall and drop service if necessary. He suggests that in the coming years, most countries will articulate plans for when and how they can take over the firewall.

“What happens in an emergency is people swamp the network with traffic, so I think many countries will have a plan to cut citizens off the network for a certain amount of time while they cope with something like a cyberattack,” Buchanan says. He says he thinks countries like Bangladesh are testing the network to see if they can take it over and make sure they have priority over the rest of the network.

Buchanan sees the use of firewall control during a major event as justified because it allows emergency and first responders to communicate in a timely manner, but he says in countries with high political tensions, blocking the Internet can be done maliciously. For example, when Bangladesh tested its network control, it blocked news outlets that reported on antigovernment organizations, he notes. And during the coup in Turkey last July, the government cut off access to YouTube, Facebook, and Twitter to quell any uprisings.

Many countries “play the terrorism card” to justify controlling the Internet or viewing private data, Buchanan says, which isn’t logical because terrorists know how to hide their tracks. “Operating systems that boot from USB sticks and leave no presence on devices, VPNs, and proxies...those are the types of tools that a terrorist or criminal will use, and invest a lot of time and energy to create.”

This kind of reasoning, as well as roundabout laws such as Saudi Arabia’s ban on all use of encrypted traffic, can be a slippery slope for privacy concerns and affects law-abiding citizens more than the troublemakers, Buchanan notes.

“The more that we use encryption panels, the less chance that law enforcement will have in actually tracing the real criminals,” Buchanan explains. “What they’ll end up doing is monitoring everyone else for the normal things, and then a data breach at an ISP could release information about the president or prime minister, and everyone else whose information was collected.”

Whether it’s a complete shutdown to Internet access or careful monitoring of potentially dangerous content, countries and companies around the world are taking advantage of the possibilities—and power—inherent in controlling what citizens see online. As criminals and extremists move their activities from land and sea to technology, governments must figure out how to counter digital warfare while simultaneously respecting and protecting citizens’ basic human right to Internet access.
When you prepare, you prevent. And when you choose a custom-designed solution from AMAG Technology, you’re prepared to take complete control of your company’s security. Our proven solutions are helping a wide range of customers around the world mitigate risk, reduce costs and comply with regulations. To learn more, please visit AMAG.com or call 800-889-9138.
Zions Bancorporation is one such institution that has taken steps to converge its physical and cybersecurity systems to protect its customers and assets, which total approximately $60 billion. One of its affiliates, Nevada State Bank, recently upgraded its access control system to provide enhanced security, as well as convenience, for its workers.

To workers at Nevada State Bank, the old system of physical keys and hard locks was both a security concern and a nuisance. For example, an employee was at the park playing with her child when someone broke into her car. Along with the employee’s purse, the robber got away with a physical key to the bank’s branch where she worked. She made a phone call to corporate security, and the entire building had to be rekeyed that weekend.

“To rekey all the locks and replace keys could cost $3,000—or it could be even more costly if it’s a master key that’s lost,” says Bob Shandle, regional security officer for Zions Bancorporation. He adds that when employees lose their keys, “it almost always happens over the weekend,” an inconvenience to the security staff.

Replacing physical keys with cards was one of the biggest advantages to upgrading access control at three Nevada State Bank branches, says Shandle, who introduced new security cameras and alarm systems as well. “Card access is just a small part of the big picture of what we’re trying to accomplish” in terms of security, he notes.

Zions worked with an integrator to find the best choice for an access control platform for the bank. In March 2015, it chose Sielox Pinnacle, the software that serves as the hub for
the overall access control system. Sielox 1700 Network Controllers are used to support card readers installed at door locations, including hardwired doors located in the branch’s vault.

At the majority of its entryways, the bank first chose Allegion AD-400 wireless locks that integrated with the Sielox system. Because the locks are large and require drilling holes for installation, the AD-400 locks were functional but not ideal. In March 2016, Shandle purchased Schlage NDE locks, which have a smaller form factor and are more affordable. Both Schlage and Allegion are owned by manufacturer Ingersoll Rand, so the microchips inside employee access cards did not change. The cards were simply updated through the Pinnacle software.

“The NDE lock requires no special modifications to the door. It goes right on top of where your old lock used to be,” Shandle explains. This is especially useful given the “bandit barriers,” or bulletproof glass walls, that run throughout the branch to protect tellers from potential shooters. With a wired system, “you’d basically have to disassemble the entire door area” for installation, Shandle says. “With the NDE lock I was able to get the mount right on top of that heavy-duty Plexiglas, and it worked really well.”

He adds that the locks resulted in a “huge cost savings,” and says the price of the wireless access control system was roughly one-third the cost of a hardwired one. Commissioning the lock to work with existing cards was also fairly seamless. Using a smartphone and tablet app from Allegion that integrates with the Sielox software, administrators create a username and password, and then link the wireless locks to Pinnacle. This enables the chips in the card to work with the control boards in the door readers. “Sielox is the only access controller provider in the market that seamlessly integrates the NDE locks from Allegion, so it really did work out well,” he adds.

In addition, someone at the bank is responsible for going through the card access database every day to ensure that it reflects employees who have been terminated, are on temporary leave, or have returned from leave. Changes can be managed within the Sielox Pinnacle online Web portal. Additionally, all actions are recorded and reported on every card, so security personnel can track activity and spot abnormalities in the log files.

Vendors who spend an extended period of time at a branch are assigned a bank employee who is responsible for their access card. “That supervisor or person from the bank would have to request the card in writing from us, and then we would issue it on a temporary basis,” he says. The assigned person from the bank is responsible for eventually getting the card back to security.

Currently three Nevada State Bank branches have card access throughout the building, as well as the central vault. Eventually Shandle says they hope to implement the system organization-wide. “We are trying to consolidate all of the branches under the Sielox Pinnacle card access system and eliminate the need for employees to carry keys altogether,” he notes.

The biggest concern with wireless access control readers is battery life, Shandle says, so Pinnacle has an application that tells security how long until the batteries on individual door readers are exhausted. And there is a small time-delay between putting the card up to the reader and when the door unlocks. “When it comes to presenting your credentials, the readers don’t always respond immediately like the hardwired ones do,” he notes.

However, these concerns are outweighed by the convenience of the overall system. A key can be disabled within minutes, no longer requiring an expensive and timely rekeying of the building. “It costs about $5, and I can have a key card removed from the system in a number of seconds,” Shandle says. “Even if you lose it on a Friday night, we can have that card disabled, so that the missing fob that grants access to our branch doesn’t work anymore.”

---

**For More Information:**
Karen Evans, karen.evans@sielox.com, www.sielox.com, 856.861.4568

---

**Stats**

**IT Industry Findings: Financial Services**

<table>
<thead>
<tr>
<th>Stat</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>41% Plan to increase spending on third-party partner security</td>
<td>47%</td>
</tr>
<tr>
<td>47% Of all IT services are delivered via cloud-service providers</td>
<td>61%</td>
</tr>
<tr>
<td>61% Require employees to complete privacy training</td>
<td>43%</td>
</tr>
<tr>
<td>43% Were victims of phishing attacks</td>
<td>38%</td>
</tr>
</tbody>
</table>

TREAT YOUR PASSWORDS LIKE YOUR UNDERWEAR: make them exotic, keep them to yourself, and change them from time to time. That’s the memorable approach that Cisco Chief Privacy Officer Michelle Dennedy takes to creating strong passwords.

But sadly, most people do not put that much effort into crafting passwords for their online accounts, and this can have dire consequences for corporations. In 2015, 63 percent of confirmed data breaches involved leveraging weak, default, or stolen passwords, according to the 2016 Verizon Data Breach Incident Report. “The capture and/or reuse of credentials is used in numerous incident classification patterns,” the report explained. “It is used in highly targeted attacks, as well as in opportunistic malware infections. It is in the standard toolkit of organized criminal groups and state-affiliated attackers alike.”

But just what should those stronger authentication mechanisms be? What approach should you take to make your passwords stronger in 2017?
Make them exotic. Creating an exotic password can mean something different, depending on who you’re talking to. For Dennedy, having an exotic password means creating a password with different characters that’s not a dictionary word. For instance, pick a favorite book and use the first letters of the first paragraphs of various chapters in that book to create a password.

“And have some special characters thrown in there,” Dennedy explains. “That’s a great formula, and you don’t have to remember anything more than the book.”

Or, exotic passwords can be developed from a pattern that is special to a various website. “So having something that reminds you of your shopping list site and then adding on your special paragraph pattern,” Dennedy says. “These are tricks that can make your password exotic enough that it’s not guessable, and yet memorable enough that you actually get use out of it, rather than having to change your password every time because you’ve forgotten it.”

Another option is to go for length, says Lance Cottrell, chief scientist for Ntrepid’s Passages. “It used to be that if you had an eight-character password, that would be enough, they are not going to be able to guess your password,” he explains. “But realistically these days, that’s not true. They are able to get through much longer passwords, particularly if you’re not using the full breadth of characters available to you.”

Instead, users should aim for at least 20 characters and use upper case and lower case letters, numbers, and emojis—if that’s an option.

“You just can’t beat length; the longer your password is, the better off you are,” he says. “Because it’s easy to guess your username; it’s probably your name or more often your email address. So if I steal your password on one website, I’m going to try that email address and password on every other website I know of. I’m going to hack it off of some website you don’t care about, and then try it on your bank and every bank out there just to see whether it will work.”

Instead of using a memory-based solution for his passwords, Cottrell uses a password management application to keep track of the passwords for his hundreds of online accounts created over the years. This application then syncs with his devices, such as his iPhone and iMac, so he doesn’t have to remember them.

“If there’s one practice that I could say, ‘Go do this thing and it will make your security better,’ it’s to start using a password manager application,” he says, adding that he uses the application 1Password to keep track of his. Like most password management applications, 1Password allows you to create a login and then save all of your passwords for your online accounts to the site. It then encrypts your data, securing it from potential hackers who might try to gain access to the site to steal your credentials.

“I have one really good password for that vault,” Cottrell says. “I have one really big, long passphrase that I have memorized that unlocks that, and then that gives me access to everything else.”

While you can add passwords you’ve created to the password management
application, you can also choose to have it automatically generate a password to your specifications—such as 20 characters in length—to give you completely random passwords for all of your online accounts.

One downside of password management applications, however, is that they can be inconvenient to use, which is one reason Dennedy adopted the practice and then gave it up. “I've tried the places she needs to be, especially when traveling.

“My job is weird; no two days are the same and I’m doing planes, trains, and automobiles, so if my login fails, that’s a real pain,” Dennedy explains.

Keep them to yourself. Many users have been there before. They have access to a corporate account, such as a Twitter account, and another employee needs access to it. So, they email the other employee the credential. While that might be an efficient way to share access, it is not a secure one and should be avoided if at all possible, Cottrell says.

Instead, if you’re sharing an account, make sure the password is strong—exotic, long, and possibly generated by a password management application. Also, make sure that you’re not sharing it through email.

“Even sending it through a text message is better than sending an email,” Cottrell says. “Send it in a path that avoids email and using the computer...as that makes it much more difficult for an attacker to make use of it. An actual physical note with the password on it, that’s shredded later, is going to be even better.”

Also, when it comes to passwords, make sure you’re not giving information away on social media sites that could be used to compromise your password hint questions, which are often a fixed set of questions with information that’s easily discoverable.

“Don’t put as your security question the name of your real dog,” Dennedy says. “It’s okay to lie there.” Instead, make up an answer such as using the name of a dog that you don’t own to answer your security question. And to keep track of these answers, you can set up a list in most password management applications to store them. This way, you don’t have to remember what your lie on your security question was, Cottrell says.

“So if the security question says ‘Where did you go to high school?’ Put in something like Richard Nixon High School or a Lord of the Rings reference,” he adds. “Anything you want can go in those slots, and then just add them to the notes section of your password management app.”

Change them. When it comes to changing your password, how often is too often? And does changing your password regularly make it less secure? The answer is complex. U.S. Federal Trade Commission (FTC) Chief Technologist Lorrie Cranor made headlines in 2016 when she suggested that companies rethink mandatory password changes for employees.

“There is a lot of evidence to suggest that users who are required to change
their passwords frequently select weaker passwords to begin with, and then change them in predictable ways that attackers can guess easily,” Cranor wrote in a blog post. “Unless there is a reason to believe a password has been compromised or shared, requiring regular password changes may actually do more harm than good.”

This is why all organizations should consider their risk profile and the security benefits and drawbacks of having employees frequently change their passwords, Cranor added in her post.

“Research suggests frequent mandatory expiration inconveniences and annoys users without as much security benefit as previously thought, and may even cause some users to behave less securely,” she explained. “Encouraging users to make the effort to create a strong password that they will be able to use for a long time may be a better approach for many organizations, especially combined with slow hash functions, well-chosen salt, limiting login attempts, and password length and complexity requirements.”
As concerns about workplace violence rise, companies should adopt protective intelligence strategies to prevent attackers from succeeding.

A LARGE, INTERNATIONAL FINANCE COMPANY was recently planning to fire one of its employees, but the company’s leadership was concerned. The employee, whom we’ll call John, had a history of being aggressive towards his supervisors.

Thankfully, the actual termination went smoothly and without incident, but that’s where the company’s good fortune ended. During the days that followed John’s termination, several employees received notes from him on social media instructing them to “consider not going to work” on a specified day.

As a precautionary measure, the company contracted for additional physical security at its main office building. However, when it became aware of the social media threats, the company reached out to the author’s international protection, investigations, and consulting firm for advice on how to handle this new challenge.

The firm immediately began conducting physical surveillance, following John’s movements. It also started analyzing his social media accounts and noticed that he had made
several posts about the company’s vice president of human resources.

Upon further observation, the firm discovered that John had recently driven to an intersection about one mile from the company’s building. This location was also on the route that the vice president took to get to work every day.

Using the intelligence gathered from social media and physical surveillance, the firm observed John’s behavior in real time and contacted law enforcement to prevent him from causing any harm to the vice president or to the company’s facility.

Not all workplace violence threats are so successfully mitigated. An average of 551 workers were killed each year between 2006 and 2010 as a result of work-related homicides, according to the most recent numbers from the U.S. Bureau of Labor Statistics (BLS). And as many as 2 million workers report having experienced workplace violence each year, according to the Census of Fatal Occupational Injuries.

Most alarmingly, shootings accounted for 78 percent of all workplace homicides—83 percent of which occurred within the private sector.

Unfortunately, the traditional corporate climate is reactive because most companies only respond after there’s been a highly publicized workplace violence incident. Furthermore, many do not enact changes at all once the dust settles and the incident is no longer in the media.

With concern growing over workplace violence from all sectors, there is a demand for protective intelligence, which can avert a crisis instead of reacting after it occurs. To put it simply, you cannot mitigate a risk that you have not anticipated.

The primary objective of protective intelligence is to collect information to help determine if an individual demonstrates the intent and capability to formulate and execute a violent plan of action.

To determine this, most use the intelligence cycle—an important process for investigators or anyone who collects information for assessment or analysis. Originally implemented by the U.S. Military Intelligence Division during World War I, this process is leveraged by many government entities and for a wide spectrum of tasks, such as by organizations like the Federation of American Scientists. This process is most notably used in the investigative processes within the FBI and within the U.S. Secret Service, namely the National Threat Assessment Center.

The FBI defines the intelligence cycle as “the process of developing unrefined data into polished intelligence for the use of policymakers.” Protective intelligence investigations differ from other kinds of investigations because the goal is to prevent violence or a loss, not simply secure the requested facts.

An individual, group, or organization must collect information that will develop the critical intelligence required to take preventative actions. The U.S. Secret Service defines this process as “gathering and assessing information about persons who may have the interest, motive, intention, and capability of mounting attacks against public officials and figures.”
The intelligence cycle has six steps. These steps are: identify requirements, plan and provide direction for intelligence that is to come, collect and gather information, analyze and convert that information to produce raw intelligence, and disseminate intelligence to those who will use it for tactical, operational, and strategic decision making.

**Identify requirements.** The first step is to identify the requirements the information is designed to satisfy. This step will help filter data into the most critical pieces of information and organize them by relevance.

For workplace violence investigations, investigators should focus on information that will help answer the fundamental question: Does this subject present a threat to protected individuals, groups, or organizations?

Some companies do designate internal employees as threat response personnel. Protective intelligence investigations are performed most effectively by those who have experience and training doing them and who are also unbiased, such as a third-party consultant.

**Plan and provide direction.** The second step in the cycle is to create a plan and provide direction for the intelligence that is to come.

**Collect and gather information.** Gathering of information is the third step and includes researching online databases, performing physical surveillance, and conducting interviews.

**Process and exploit.** After collecting relevant information, the fourth step of the intelligence cycle is to process and exploit that information. This means filtering the data into useable bits for the decision-making processes defined by the requirements in the first step; the bits can be referred to as the dots.

For example, when conducting an investigation of a subject who may be on the path to violence, social media or other tools may reveal his whereabouts during certain times that may be indicative of a hostile planning process. Critical decision points for likely pathways the subject would take to commit an act of violence could be established, and their correlation with the information that has been revealed would create the dots.

This can be a time-consuming burden, especially for investigators using social open-source intelligence (SOSINT). To be effective at this task, investigators should combine resources by directly researching on social media sites and by using search engines to do the task. With this methodology,
investigators can start to connect the dots, enabling analytical confidence—particularly when dealing with the concern of targeted violence.

**Analyze and convert.** The fifth step of the process is to analyze and convert these bits of data to produce raw intelligence.

In the event that a subject’s behavior reveals the impending manifestation of a perceived threat, these connected dots are used to make decisions that will effectively impede the process.

**Disseminate.** The final step of the cycle is disseminating the intelligence to those who will use it for tactical, operational, or strategic decision making.

---

**Sources**

Although most would believe that intelligence is gathered from secret or covert sources, the largest collection of information available to investigators is open-source intelligence (OSINT), or intelligence collected from publicly available resources.

Within the intelligence community, the term “open” refers to overt, publicly available sources drawn from public resources, such as the Internet, media coverage, photos, and geospatial information. However, it’s important to keep in mind that there is no authority ensuring the accuracy of any information available through OSINT. Because of this, employers who use this collection method have a responsibility to verify—or at least corroborate—its validity.

SOSINT, the collective term for information from sources such as Facebook, Twitter, blogs, and microblogging sites, is becoming more important within the intelligence community. SOSINT is a content-rich gold mine and a valuable investigative tool when seeking corroborative information about individuals or groups, such as behavioral changes, interests, emulations, gang activity, and general life circumstances.

Social media is particularly useful to investigators for several reasons. The first is the immediacy in which content is not only created, but disseminated. The Facebook news feed is the epitome of a media outlet for such content because there is no delay in publication and almost no restriction in its ability to spread virally. Social media provides a variety of ways for potential subjects to distribute thoughts or request tactical assistance, along with numerous ways for investigators to gather that information.

In 2014, LexisNexis published a survey, *Social Media Use in Law Enforcement*, of federal, state, and local law enforcement professionals in the United States who are users of social media on the job. The survey details how social media can enhance the assessment and threat management process.

The survey found that “respondents indicated several real-world examples in which they prevented or thwarted pending crime, including stopping an active shooter, mitigating threats toward school students, executing outstanding arrest warrants, and actively tracking gang behavior.”

For the private investigator seeking information on the behavioral circumstances of a subject, something as quick and easy as analyzing a subject’s status updates, check-ins, and posted photos may provide the information necessary to conclude if a legitimate threat exists.

---

**Surveillance**

Physical surveillance is one of the oldest and most common practices within investigative services, yet it remains the best option in cases when real-time information is required. To do this, employers must hire a licensed professional who can conduct surveillance legally.

Surveillance in the investigative field is used mostly as a tool for developing factual evidence to prove or disprove circumstance. However, surveillance can also provide information that is critical to the decision-making process for a much broader spectrum of investigations than most private detectives recognize.

In conducting protective intelligence investigations, surveillance is a viable option to gather the necessary information on a subject because not all attackers make direct threats. This increases the difficulty of validating or legitimizing the threat through other sources.

Using information from OSINT may reveal the threat, such as general ideas and interests, but it is typically not specific. Surveillance can be used to confirm a suspected threat or to find out more details.

Furthermore, the analytical confidence from deriving conclusions based on direct observations versus assessing the quality and quantity of third-party information is an important factor. This provides the investigator and analyst a more profound confidence in the facts at hand.

In one such instance, upon investigating a subject who was facing possible termination following a history of unsatisfactory performance and increasingly aggressive behavior, the author’s firm noted a hunting license in the subject’s background investigation.

Taken in isolation, this is not a threatening piece of information. However, during the day of a contentious announcement of the firing from...
the company’s CEO, it was decided by the author’s firm—hired to provide executive protection for the company—to restrict access to the facility.

Local law enforcement helped bar the subject from the property. The former employee had a hunting rifle in his vehicle even though no hunting seasons were in effect. There was no violence that day, but the potential mitigation was worth the effort.

Once the subject is identified and background information has been collected, the main factors investigators should concentrate on during surveillance are the current living characteristics of the subject and context of the subject’s daily routine.

Surveillance should focus on factors in the subject’s life and environment that might increase the probability of an outburst or attack, such as living arrangements; actions and behavior; and daily activities and social interactions, particularly compared to possible known historical circumstances and behavior of the subject. This focus on routine can provide valuable information that can help assess the subject’s stability.

For example, if the subject does not currently have the means to satisfy the basic needs of food, clothing, shelter, or social interaction, then he or she may be in desperate crisis with no option left but to act out.

Additionally, researching, planning, and coordinating the attack are critical to the attacker’s success. The steps required in developing a plan will reveal the person’s intentions, actions, and acquaintances.

For instance, this can be seen in the events that led up to the kidnapping of Sidney Reso, former president of Exxon Co. Reso was kidnapped by Irene Seale and her husband Arthur Seale from the end of Reso’s driveway in suburban New Jersey on April 29, 1992. Reso was shot in the arm during the kidnapping, and died a few days later. However, the Seales claimed that he was alive and demanded $18.5 million in ransom before finally being discovered and apprehended.

Prior to kidnapping Reso, the Seales watched his home from a van parked down the street for almost a month. These preparations were highly visible and could have been easily identified. The Seales could have potentially been intercepted with a counter surveillance effort as part of an executive protection program.

For violent attackers, the chances of success and escape are the predominant factors in determining the location to attack. Therefore, research and planning efforts on site selection...
and even tactical decisions pertaining to that site are particularly revealing during physical surveillance. The subject’s behavior and rituals during this process are also extremely revealing because the attacker’s intention may not include any escape plans at all, potentially indicating the worst case scenario of a suicide attack.

This type of behavior was demonstrated by Khalid al-Mihdhar and Nawaf al-Hazmi who flunked their flying lessons because they were disinterested in the landing process, administrative actions, or flying anything other than Boeing jets. The two individuals failed to obtain their pilot’s license, but ended up being two of the four “muscle men” on American Airlines Flight 77, which flew into the Pentagon on 9/11.

The potential attacker will want to gain familiarity with the location, how to get there, and—in most cases—how to escape. He or she may even take pictures of the location for reference later in the planning process, and may conduct rehearsals to discover what the security response might be during a crisis or how effective access control is.

In the investigation that followed the mass shooting in the Aurora, Colorado, movie theater, it was revealed that gunman James Holmes had purchased his ticket for that showing of The Dark Knight Rises more than a week in advance, carefully selecting the time and place for his attack.

Additionally, he had set explosive traps at his apartment, planning for them to be tripped prior to his attack to send resources to that incident instead of the movie theater.

Real-time information gathered via surveillance can lead to making preventative decisions sooner and more reliably than other methods of investigation.

Examples of behaviors that may indicate the coordination or planning of an attack could be visiting others who share the same ideas and interests, visiting websites linked to the company, obtaining supplies, or purchasing weapons. At this point, the investigator should avoid bias and assumption, concentrating only on facts.

For example, if a suspect who has no historical interest in firearms obtains weapons and ammunition over the course of an investigation and then proceeds to a target location, investigators conducting the surveillance may be able to involve the authorities immediately.

To be effective at surveillance, the investigators must anticipate the subject’s actions. Investigators must ask themselves where the subject would have to be and what materials would have to be obtained. To that end, investigators should develop a list of locations and activities that may be part of the subject’s target selection or planning processes.

For investigators, protectors, and those who conduct threat assessments and evaluations, protective intelligence programs are a critical aspect of proactively preventing workplace violence incidents before they occur. When it comes to reducing workplace violence as a whole, we all share the responsibility of identifying, assessing, and intervening as early as possible.
Together we can

Educate

Inspire

Heal

Nourish

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

Supporting Families Across America

For product info #15 securitymgmt.hotims.com
As Thomas J. Langer, CPP, takes the reins of ASIS International as its incoming president, he tells Security Management about his career in government security and the challenges the industry is likely to face in the future.

Thomas J. Langer, CPP, joined ASIS International in the early 1980s. He started in the Granite State Chapter in New Hampshire, eventually transferring to the National Capital Chapter as his employer of three decades morphed and merged. Langer served in several ASIS council leadership positions before being elected to the Board of Directors. This month, Langer begins his term as president of ASIS International. Security Management spoke to Langer about his security career and his insights on the industry. (For more on Langer’s ASIS experience and his plans for the Society’s future, see “ASIS News” on page 67.)

Q. How did your career aspirations lead you to the security industry?
A. I wanted to be in law enforcement from the time I was a child. I thought it would be a great profession, and the four years I spent as a police officer were probably the best work experience of my life.

After I completed my degree at Saint Anselm College in Manchester, New Hampshire, in 1977, I stayed and became a police officer. I left the force because I was married and had a child and needed a better salary. So, I joined Sanders Associates in New Hampshire as a facility security officer.... Sanders was acquired by Lockheed, which merged into Lockheed Martin. That was the crazy M&A period for businesses in the 1980s and 1990s. When the dust settled we were part of BAE Systems, Inc., but I’ve been with the same company for 36 years.

Q. How has your career trajectory helped you succeed?
A. I started as facility security officer with responsibility for one site. From there I became the head of information security, which at the time was physical document control—primarily classified material and classification management. I managed the security aspects of contracts between my employer and other companies and the government. From there, I went to a special programs assignment, and each of those roles increased the number of people who worked for me. And I went from a broad, does-everything role to much more specific and directed involvement in programs and a large staff of people I was managing.
In 1999, I was promoted to security director for that piece of the company. Two weeks afterward, Lockheed announced it was going to divest us, so any celebration was over. I went through the divestiture process, which professionally was one of the most interesting experiences I've had because we were auctioned. A number of companies were looking at us and we had to go through a lot of due diligence, and I took that opportunity to brief the different government agencies that had oversight because of the work we did. And so I went from agency to agency... and that allowed me to establish a relationship with a number of senior people in the government.

Q. What has been the most educational part of your job?
A. After my company was purchased by BAE Systems, a British company, the deal had to be reviewed by the Committee on Foreign Investment in the United States, under the auspices of the U.S. Treasury Department. We were given a special security agreement we had to live by. We have a special set of directors for the U.S. piece of the company, and fairly strict oversight by the U.S. Department of Defense.

The great thing was that it gave me an international exposure that I never had before. It’s a unique level of oversight and a unique level of responsibility professionally.

Our biggest challenges are helping customers understand the foreign ownership model and how that operates.... You find that you are also reeducating people on a regular basis because staff at various regulatory agencies and customers naturally change over time. To be successful in my role, I have to not only maintain the business relationships I have, but also spot their successors and build relationships with them.

Q. What does the security function need to focus on?
A. There’s a natural tendency to say “nothing’s happening, why don’t we cut the money we’re putting into security.” We have to find a way to express ourselves in business terms so that the leadership understands what’s happening. I have access to the president’s office if I need it. But I really do not like to exercise that option. I prefer to work with my peers.

As I have formed relationships with peers in other industries, I’ve found that we all share essentially the same problems—for example, making sure that company leaders understand security’s contribution to the business whole, how to motivate the security team, and how to get employees to accept that security is there to help them, not to delay their progress.

Q. What is your personal mission?
A. As I come up to my natural retirement time, I’ve been focused on developing those relationships for the next set of leaders in my company. I want them to extend to at least the next level down, if not further than that, because the people from regulatory and other oversight agencies must understand who we are, not just me, but our bigger organization.

Q. What are the future challenges for the security industry?
A. It’s a great industry for a lot of good reasons and sad reasons—we keep having a lot of challenges from nonnation-state actors from around the world. We are in a very different climate. I see continued growth and continued reliance on us. ASIS needs to raise the level of professionalism and create opportunities for our members. We want people in the industry to come into our membership because they see us as a real value to them and a real help to them. This isn’t about filling the coffers; we are a not for profit. ASIS is committed to creating an environment where people who are in the security industry or who want to be in the industry are going to benefit.

Another issue is the threat posed by emerging technologies—that are for the good of mankind but can be exploited by others. The Internet of Things is a good example. It’s really quite dangerous when someone can stop your car. Remotely. On the highway. Those types of challenges will be faced going forward. ASIS wants to help people see threats and counter them early, and they share that best practice. That is the model and the future of this organization—members helping members.
The world’s water supply faces issues of safety, security, and sustainability, while becoming a more tempting target for terrorists.

**World Water Woes**

**OUR MOST BASIC COMMON LINK IS THAT** we all inhabit this small planet. We all breathe the same air. We all cherish our children’s future. And we are all mortal.” U.S. President John F. Kennedy’s 1963 commencement speech, titled “A Strategy of Peace,” fore-shadowed the vulnerability of nonrenewable resources around the world today.

Human beings require approximately 50 liters (about 13 gallons) of fresh water per day. But in North America, the average citizen uses more than 300 liters (almost 80 gallons) of fresh water every day, more than twice the world average. At least 75 percent of the water consumed in North America has been acquired, transported, treated, and distributed through municipal or regional water treatment systems, at a significant cost.

Water treatment systems in North America are vital—and make tempting targets for
Between 1994 and 2014, 138 attacks targeting food and water supplies were recorded in the Global Terrorism Database maintained by the University of Maryland. As a vital asset and symbol of democratic societies, water is and will continue to be considered a high-value target for terrorists.

More evidence of threats to these critical systems can be found in the water conflict chronology list, compiled by the Pacific Institute in the United States. In 2014, three men in the U.S. state of Georgia were arrested for planning to attack water treatment plants, power grids, and other infrastructure. And, in 2011, a hacker targeted a water plant in Houston, Texas, following earlier news of an electronic attack on an Illinois water plant. The breach occurred after the attacker hacked into supervisory control and data acquisition software used by the utility.

The relative scarcity of water around the world may lead to global conflict. In 2012, the U.S. Office of the Director of National Intelligence (ODNI) issued *Global Water Security*, an assessment that concluded that the safety, security, and sustainability of Canada’s water supply may soon become a source of conflicts between nations.

“Several regions of the world will face major challenges coping with water problems,” according to the report. “Between now and 2040, fresh water availability will not keep up with demand, absent more effective management of water resources. These findings reinforce the view that water is not just a human health issue, not just an economic development or environmental issue, but a peace and security issue.”

Water rights may also impact the relations between countries, as exemplified by disputes that arose recently when municipalities in the United States began replenishing their aquifers by withdrawing water from the Great Lakes. Canada and the United States not only share the longest unprotected border in the world, but also the Great Lakes—the largest surface freshwater system on earth.

The United States and Canada have identified water and wastewater systems as critical infrastructure, and the protection of this infrastructure raises significant challenges, including a less-than-ideal governance model. There are no federal standards or...
agreed-upon practices within the water infrastructure sector to govern readiness, response to security incidents, or recovery in the United States or Canada. By providing the industry with an adequate governance framework, the governments could promote resilience along the entire water supply chain.

Given these governance issues, the aging water infrastructure, dwindling expertise, complex and open systems, and the lack of standards in protection, North America’s vulnerabilities to potential attacks may be considered high to very high.

“Although the frequency of warfare, particularly in developed countries, may be decreasing, advances in technology, including increased global mobility and communication, have heightened the threat posed by individuals and small groups, including decentralized terrorist organizations,” according to the 2014 book Drinking Water Security for Engineers, Planners, and Managers by Ravi Jain.

By assessing and revisiting the security risks associated to water and wastewater, the effectiveness of current layers of protection can be determined by using a standard equation where risk is calculated as the product of the likelihood, the consequences, and the vulnerabilities.

**Likelihood**

Many nations are engaged in a war of ideas and values with terrorist organizations that export their concepts to individual citizens. Recent events confirmed the fact that no one is immune to terrorist attacks and that these organizations will go to great lengths to carry out attacks on the most vulnerable contingents of society. Security professionals must learn from past events while building on this knowledge to identify how and where the next attack may occur.

Conflicts have begun to emerge between nations over water issues in Africa and the Middle East. These isolated events may increase in number as the world population continues to grow. Geopolitical, environmental, and economic factors will contribute to migrations, adding to the size of large metropolitan areas—by 2050, seven out of 10 people will live in cities.

These changes will spur new pressing demands for water services, which may affect public and national security as well. For example, while the likelihood of a terrorist attack in parts of Africa may currently be low, this level could be elevated rapidly based on intelligence gathered by national and international authorities.

**Consequences**

Attacks directed at water infrastructure can be categorized as rare events that occur with a low frequency. However, the consequences could be severe. Researchers have attempted to identify and even quantify just what those consequences could be.

“The potential economic fallout from accidental or deliberate contamination in a water system is significant,” Jain notes in his book. J.W. Porco with the American Water Works Association estimates that “the cost for radiological contamination in a water system serving a population of 10,000 could be as high as $26 billion; for a population of 100,000, the estimated economic impact could be $100 billion.”

Although biological, chemical, and radiological detection systems protecting water sources are becoming more sophisticated and effective, they can only protect against known forms of...
attacks and may not fare as well against zero-day vectors. Considering the severe impact that could be generated by similar scenarios, the consequences of such attacks can be estimated as very high.

**Vulnerabilities**

To identify a nation’s vulnerabilities, officials must start by assessing the governance model to determine how effectively the procedures and the equipment associated with the protection of water and wastewater systems are managed.

The U.S. governance model provides a significant level of coordination and oversight from the federal government under the leadership of the U.S. Environmental Protection Agency (EPA), supported by the U.S. Department of Homeland Security (DHS).

The objective of the EPA is to build resilience at drinking and wastewater utilities, notably by providing section-specific plans including security, which are found on the DHS website. It is unclear how the new U.S. administration will approach water infrastructure. In Canada, most of the investments and practical managing issues are delegated to municipal and regional authorities under distinct provincial and federal legislation. There is not as much coordination or oversight from the central government, which may explain the lack of national standards for water protection.

The newly-elected liberal government in Canada has pledged to provide provincial and municipal authorities in the country with infrastructure funding in the coming years. This may allow municipal and regional authorities to invest in water and wastewater infrastructure, which in many cases is old and fragile. The aging infrastructure is further compounded by a North American demographic trend where experienced workers are leaving the workforce in record numbers. It is unknown whether current succession planning and training efforts are sufficient to counter this trend.

**Managing the Threat**

Terrorist organizations are determined to exploit weaknesses, either physically...
or virtually, to create chaos and terror, usually accompanied by a significant impact on national economies. This is their raison d’être, and to remain relevant and to attract more followers, they will continue their attacks.

Simple and minimal resources on the part of the terrorists are inflicting major damages, whereas the means to prevent and protect against those attacks are both complex and costly, creating an asymmetric conflict. It is difficult to determine how much to spend on reducing the risk of attacks to critical infrastructure when measured against other forms of security risks, as well as whether the resources invested in the protection of this infrastructure are delivering the desired outcome.

As part of a diligent approach, the risk level associated with critical infrastructure must be regularly assessed to prevent accidents and incidents that could put North America’s respective populations at risk.

It may be beneficial for Canada and the United States to develop—in collaboration with provincial and state regulators—an all-hazards approach to water security based on existing models, such as the American Water Works Association Risk and Resilience Management of Water and Wastewater Systems. Although the countries’ regulations may differ, it may be beneficial to develop measures that could be mutually recognized and accredited by central, provincial, and state governments. To do otherwise may lead to duplication, confusion, and wasted resources.

Building resilience will also require an increased awareness of the issue on the part of the public. In this regard, Canada should copy and adapt the Water Sentinel project that was launched by the EPA in 2006.

Considering the cross-jurisdictional situation of watershed management, more regulatory clarity, increased oversight, and audits to build resilient water and wastewater systems are necessary to instill a higher level of accountability and readiness among the various stakeholders.

Collaboration

Demographic trends for the next 30 years show a significant growth in urban populations in the world, including North America. As the population grows so will the need for food and water, which are intimately intertwined. Along with the continent’s disturbing consuming habits and changing weather patterns, this will further stress fresh water supplies.

The scarcity of fresh water in the future will make this infrastructure even more critical and attractive for terrorist organizations. It will be imperative to effectively respond to unforeseen events, from using collaboration across national and organizational boundaries to resuming operations once the threat has been eliminated.

Collaboration fosters resilience, and actions such as providing stakeholders with standards, training, and common communication and information sharing platforms will help accomplish that.

YVES DUGUAY, ICD.D (INSTITUTE OF CORPORATE DIRECTORS, DIRECTOR), CSSP (CERTIFIED SPORT SECURITY PROFESSIONAL), IS THE PRESIDENT OF HCI WORLD.

To view the water scarcity report, visit SM Online.
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.
On a rainy early spring morning, a group of security professionals made their way along Great Russell Street in fashionable, bustling Bloomsbury, London. They passed vehicle-distancing bollards, entered through the gate of a black iron fence, and crossed a large courtyard to reach a neoclassical building that dates from the Georgian period.

After a security inspection, the visiting professionals traversed the Queen Elizabeth II Great Court with its soaring, tessellated blue glass roof. Once the open-air courtyard outside the Victorian reading room of the British Library, in 2000, the area was refashioned into an epic enclosure worthy of the treasure in the surrounding galleries.

“The British Museum is of the world, for the world,” David Bilson, CPP, head of security and

The British Museum is a world treasure house, as well as Britain’s largest tourist attraction—a distinction that requires special security.
visitor services, told the security professionals later, when they were congregated for a special program in the BP Lecture Theatre of the Clore Center for Education. It was the day before the opening of the ASIS International 15th European Security Conference and Exhibition, and Bilson was the host and first presenter.

“People sometimes think that the museum is about the history of Britain, but it’s not,” he explains. “It’s about the history of mankind.”

Just a few of humanity’s priceless objects that the British Museum cares for are the Rosetta Stone—a rock stele with the same inscription in three languages that helped crack the puzzle of Egyptian hieroglyphs; the Sutton Hoo Anglo-Saxon burial treasure; the classical Greek Parthenon sculptures; colossal granite heads from the Ramesseum temple in Thebes, Upper Egypt; the 12th-century Lewis chessmen; an Easter Island gigantic figure (Hoa Hakananai’a); and a pair of Assyrian human-headed, winged bulls from Khorsabad, Iraq, which date to about 710 BC. (In February 2015, ISIS extremists destroyed a similar pair from the ancient city of Ninevah.)

At the British Museum, said Bilson, “We present items that date from 2 million years ago to the present day, in a collection that we are still continuing to build.”

The 18th century physician and hot-chocolate entrepreneur Dr. Hans Sloane laid the foundation for the collection. When Sloane died in 1753, he left everything to King George II. A public lottery raised funds for the original building.

“We welcomed our first visitors here in 1759, so it is our 257th birthday,” Bilson added. Since then, the collection has grown to more than 8 million items.
“We are one of the nation’s treasure houses,” Bilson told his audience. “We now welcome 6.8 million visitors per year, which makes us the U.K.’s leading visitor attraction—and I say that not to be glib, but because it brings us major security and public safety issues. We are one of London’s ‘crowded spaces,’ so therefore we have security risks.”

Art thieves are also a threat. For example, Chinese art has skyrocketed in price at auction, allowing thieves to easily sell stolen items on the black market. In 2012, the Metropolitan Police New Scotland Yard intercepted a gang that planned to target objects in one of the museum’s public galleries. Working with law enforcement agencies is a key aspect of security operations at the museum.

In addition, Bilson said the museum “is a place that transforms at night. If you stand in the front hall of the museum at 5 to 6 o’clock, you’ll see all my security colleagues escorting visitors out and thanking them for coming. At 6 o’clock, all the contractors come in, and by five minutes till 7 p.m., the whole place may be transformed with tables for dinners or corporate events—which is another demand on the security services that we have here.”

Later that evening, the visiting security professionals would witness just such a transformation when the museum’s Egyptian Sculpture Gallery hosted an ASIS reception. The varied aspects of the museum’s security program were present and working, but even to the security practitioner guests, they were imperceptible.

Later, Bilson sat down with Security Management to discuss the security program at the museum and its myriad of security concerns.

The security context has changed tremendously for all museums, Bilson says, naming as examples the May 2014 attack on the Jewish Museum in Brussels, Belgium, the foiled 2014 attack on the Louvre in Paris, and the March 2015 attack on the Bardo National Museum in Tunis, Tunisia.

During the last four years, the British Museum has invested in various aspects of its security infrastructure. One part of that investment was completed in early April 2016 when security “switched to our new digital radio system with much better coverage across our locations,” Bilson says.

Also in place now are vehicle defenses. “I hope as you came through the front gate this morning, you admired our vehicle-standoff bollards, which are a substantial upgrade in our protective resilience,” he adds.

In 2013, the museum became a construction zone with the creation of the World Conservation and Exhibition Centre on the estate’s northwest corner. It comprises scientific laboratories, office facilities, and a major new public exhibition hall, “which gives us a bigger, more flexible space than we have ever had, and below ground, we have a secure collections storage area,” he says.

Security was involved in the design for the new facility, Bilson notes. “In fact, we upgraded security substantially because of the nature of that building. So that has become our benchmark for security across the rest of the estate. It integrates all the modern technology of cameras, alarms, access control, and now the new radio system.”

Guard force. Since the Great Court was built 16 years ago, the number of annual visitors to the museum has jumped by nearly 3 million.

“We are delighted to welcome more visitors but this of course impacts our operations; we want to ensure visitors have an enjoyable and safe visit,” Bilson says.

Guidance on the management of events in the United Kingdom has changed, too. This has led to an ongoing modernization of the guard force, which comprises 300 full-time, proprietary officers.

“We are looking to take up the best of that advice, as well as lifting the security standards for all of our officers here, to a high level of professionalism,” he adds. “They are all great people, and we want to lift them up still further into new ways of working.”

“In the U.K., there are two categories of security officers: you can either be proprietary if you are working in your organization on your site, but if you provide a security service...it has to be licensed,” he explains. “At the moment we are also using licensed support while we go through our improvements.”

There is a security central command center in the museum that is staffed around the clock.
As the preeminent organization for security management professionals, ASIS International offers a dynamic calendar of events to advance your professional development. From executive education to global exchanges, our events work together to help you reach new heights in your career.

**ASIS Europe 2017**  
March 29-31 | MILAN, ITALY

**10th Annual CSO Summit**  
April 23-25 | WASHINGTON, DC USA

**ASIS NYC 27th Security Conference and Expo**  
June 7-8 | NEW YORK, NY USA

**IE Business School/ASIS Program: Effective Management for Security Professionals**  
June 5-8 | MADRID, SPAIN

**Latin American Congress of Mexico ASIS Security 2017**  
July 12-13 | MEXICO CITY, MEXICO

**ASIS Diamond Club Security Buyers Forum**  
July 25-27 | SCOTTSDALE, AZ

**63rd Annual Seminar and Exhibits**  
September 25-28 | DALLAS, TX USA

**Wharton/ASIS Program for Security Executives**  
October 15-20 | PHILADELPHIA, PA USA

**ASIS Middle East 2017**  
November 5-7 | BAHRAIN

For more information visit, [www.asisonline.org/profdev](http://www.asisonline.org/profdev).
“Not only are they doing a security watch, they are watching building systems and the condition of the building overnight, as well as the primary security function of protecting the collection,” Bilson points out.

Bag checks. While terrorism is a key threat to the museum, “The biggest challenge affecting us at the moment is the searching and screening of visitors,” Bilson says. “I’m not precious about it. We’re working hard to improve upon it, but it is a challenge on a day when 20,000 visitors come through who are not timed in their entry, so we get these peaks in demand. More than 50 percent have some sort of bag with them.”

Visitor bag searching has been stepped up at the museum, resulting in an increase in the discovery of weapons.

“The majority of our visitors are of course law-abiding and are here to enjoy the collection,” Bilson says. “But I have been surprised that a minority have brought in inappropriate items that could pose a risk.”

To ensure that the museum can secure its premises from weapons brought in bags through the entrances, new visitor search facilities were recently installed outside the building.

The museum’s executive leadership supports decisions such as these. “We have great support here. The trustees, the board that oversees museum operations, are in favor of more security, doing more, but keeping a
balance,” Bilson explains. “We want the visitors to know they are coming into a secure space, but to know that they are coming into a welcoming experience as well.”

**Perimeter security.** Bilson says that perimeter security depends upon the state of the museum at various times of day. For example, he explains that when the museum is on lockdown overnight, “we have clear definition of boundaries by way of walls and railings. They are guarded and protected by technology 24 hours per day. We use a range of technology measures, whether it is intrusion detection or surveillance or physical locks and access control.”

When the museum opens, the perimeter becomes porous, but with public boundaries, he says. “There are layers of defense within the site.” When the visitors leave, the perimeter hardens again.

“In explaining this to staff, I tell them we act in the same way as an airport—the secure air side and the public side,” he says. “So the status of areas within the museum changes, but broadly the back of house areas stay secure 24/7.”

Coordination between security and museum staff is “hugely important—that whole preplanning and coordination piece,” Bilson states. “We work very hard with facilities management and with events planning to think through levels of detail.”

**Collection protection.** Museum security protects its collection in much the same way that businesses protect their own assets. “Security technology helps, but we need people to intervene in situations as well,” Bilson says.

Like all large museums, temporary major exhibitions are staged at the museum, such as Life and Death: Pompeii and Herculaneum, which ran throughout most of 2013 attracting 400,000 visitors, and the newest, Sunken Cities: Egypt’s Lost Worlds, which closed in November and broke attendance records, according to Bilson.

The arrival and departure of special exhibitions is ongoing and security plays a large role. Before items are loaned to the museum, “we have to give an account to the lenders of how good our [security and environmental] processes are here,” Bilson says.

The museum also lends artifacts and even major collections to museums around the globe. “We apply all of our own security standards to the venue that the exhibition is going to,” Bilson explains. “Sometimes that is a learning experience for the people borrowing from us, and we try to help them get their security to such a standard that long-term they have a more resilient venue for themselves and can borrow more collections from around the globe.”

**Travel.** “The museum is constantly changing, always taking on new ideas and new things to do,” Bilson notes. “It is a busy organization that is studying and
researching and constantly evolving.”

Bilson says that the museum’s policies and procedures for staff working in other nations weren’t anywhere near as robust as they should have been.

An incident involving museum staff in another country caused the museum to rethink. “We asked ourselves, ‘Where are our people today? Do we know what countries they are in? Are they insured? Have we thought about their security and what measures have been taken?’” he explains.

Bilson discovered that there were free services tied to the museum’s insurance and travel services that had not been previously used, including “risk reports, country reports, access to services that we thought we might need one day…. Now we build emergency plans in case we need to bring teams home from overseas,” he says. “We put in place a good personal emergency plan for everybody, good support from London from the home department, and pre-travel risk assessments, advising staff before they go.”

Partnerships. The museum actively partners with police, “whether at the operational level or counterterrorism level, intelligence services, or security design advisors,” Bilson says. “We have strong links with specialists around art and antiques thefts and crime. We have a national museum security group, and most recently, we have established a European roundtable of CSOs so that we can link with our colleagues. After the terrorist events in Paris and Brussels, we supported our friends in that group, exchanging advice, and helping them with things that could be done in their museums.”

Security also works with the policing teams in the area around the museum estate. The museum interacts with its neighbors about emergency planning and special events that could affect them, such as when Night at the Museum was filmed on site or movies are shown outside on the lawn on summer evenings.

Bilson says that as a security case study, the British Museum is different because it houses a world collection that must be protected alongside large numbers of visitors and staff and a 200-year-old heritage building.

While the museum doesn’t discuss security systems in detail, visitors—he insists—want to know that security is in place.

“Peaceful, law-abiding visitors to the museum are looking for that kind of protection,” Bilson says. “When we check their bags, we get thanked for doing so and know that it gives them reassurance.”

ANN LONGMORE-ETHERIDGE IS A FORMER SENIOR EDITOR AT SECURITY MANAGEMENT.
WHEREVER YOU ARE

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

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

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

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

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

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

**E-MAIL**
Subscribe to the SM Daily and Weekly Newsletters.
Human resources directors don’t have reason to panic quite yet. The United Kingdom has just started the withdrawal process, and it has two years to negotiate the terms of the exit. During that time, the United Kingdom will still be a part of the European Union’s free trade agreement and be bound by all existing laws. Once the separation is complete, EU-driven employment legislation will remain in effect because the majority of it was passed domestically. It will be up to parliament to determine whether to repeal or change current employment legislation. However, if Britain does want to continue with the free trade agreement, the European Union may require that the United Kingdom comply with its employment law.

Attorneys with law firm Jones Day note that laws more likely to be repealed or amended after Britain’s exit include overly bureaucratic legislation—EU-enforced agency worker regulations and the required European Works Council, which won’t be relevant once the United Kingdom leaves the European Union. Other controversial legislation includes whether vacation leave is accrued while employees are sick, as well as how vacation pay is calculated.

However, U.K. employers may be facing more complaints of discrimination and workplace harassment soon. Britain currently abides by the European Union’s free trade and travel agreement, which allows EU nationals to freely live and work in any member country. But U.K. employers know that these rights are unlikely to extend after the withdrawal is complete, bringing up a hiring concern: why hire EU nationals if they may not be able to work in the United Kingdom in two years?

U.K. employers can refuse employment to anyone who does not have the right to work in the country, but refusing to
Brexit, Employment, and the Law

THE EUROPEAN UNION has historically been a driver for the advancement of nondiscrimination and equality employment legislation. The United Kingdom’s first-ever statutory prohibitions of discrimination based on sexual orientation, religion, and age were established in 2000 to comply with the EU Employment Equality Directive. But now that Britain doesn’t technically need to comply with EU employment requirements, what will happen to the current employment legislation?

hire someone because they may not be able to work in the United Kingdom in the future is almost certainly unlawful, according to CIPD, a U.K.-based HR professional body. Most employers know that this type of blanket hiring policy is likely to bring them trouble, CIPD’s website notes, and instead a more likely approach will be to require a potential employee to prove that he or she has indefinite rights to remain and work in the United Kingdom. However, this is grounds for an indirect discrimination lawsuit.

Instead, CIPD recommends that employers make employment contracts conditional on maintaining the right to work in the United Kingdom. This conditional agreement should be included in all employment contracts to avoid potential discrimination issues.

“Although this will not solve the problem of employees’ immigration status changing due to Brexit, it will help with terminating the employee’s employment if that proves necessary,” CIPD notes.

A more intractable problem facing U.K. employers is discrimination against Muslim women, according to a new report. While 69 percent of all working-age women are employed, just 35 percent of Muslim women have jobs, according to Employment Opportunities for Muslims in the UK, a report issued by the parliamentary Women and Equalities Committee in August.

Muslim women face a “triple penalty” when trying to find jobs: their race, their gender, and their religion, the report notes. A National Centre for Social Research for the Department for Work and Pensions study last year revealed that a job applicant who appeared on paper to be white would receive a call back after applying to nine jobs, while minority candidates with the same qualifications had to send 16 applications before receiving a response. To address the issue, former Prime Minister David Cameron passed legislation requiring that the government use
name-blind recruitment for all positions below a senior level. Several large private sector recruiters adopted the practice as well, but the practice needs to be countrywide, the report recommends.

“To be fully effective this should form part of a sustained initiative which profiles those employers which have successfully implemented the policy in order to incentivize others to follow suit,” the report notes “The government should monitor uptake and legislate if progress is not made within this parliament.”

Forty-one percent of Muslim women are unemployed and not seeking work, compared with 21.8 percent of the total population. However, this statistic should not discount the struggles Muslim women face when trying to find employment, says Maria Miller, the chairwoman of the committee that produced the report.

“The impact of Islamophobia on Muslim women should not be underestimated,” the report explains. “They are 71 percent more likely than white Christian women to be unemployed, even when they have the same educational level and language skills.”

The report lists a number of recommendations to help even out the path to employment, including more specific antidiscrimination legislation, professional mentoring programs within Muslim communities, and more generalized language and skills education. However, Miller notes that an unexpected find in the study was that the United Kingdom’s countering violent extremism (CVE) programs seemed to be contributing to discrimination against Muslim women.

Prevent, Britain’s original antiradicalization program, was implemented after 9/11. In 2015, new legislation was passed that requires public sector workers to report signs of extremism. The program has been decried by Muslim and civil rights groups for discriminating against religious minorities in Britain. It is widely known that Muslims are suspicious of the program, especially after a number of high-profile incidents in which children were interrogated by officials for alleged extremist views.

Furthering concerns of discrimination is a National Police Chiefs Council report, which found that last year, at least 90 percent of reports of alleged extremist behavior were made by non-Muslims.

“The government is making attempts to deal with the problems that Muslim people face in getting work, but our analysis would be that their attempts are being undermined by this clear link that Muslim people are making between government policy on employment and government policy on countextremism,” Miller told The Guardian.

CONTACT ASSISTANT EDITOR LILLY CHAPA AT LILLY.CHAPA@ASISONLINE.ORG. FOLLOW HER ON TWITTER: @LILLYCHAPA.
Hundreds of Security Product and Service Categories

Thousands of Security Products and Service Providers

One Resource for All Your Security Solutions

The Security Management Buyers Guide
www.securitymanagementbuyersguide.com

The place to find every company that exhibited at the ASIS International Seminar and Exhibits, and many more.
certify an event as an act of terrorism. Congress overrode President Barack Obama’s veto, allowing legislation to become law that gives terrorism victims and their families the ability to sue foreign states and officials for their role in an act of terrorism.

The veto override enacted the Justice Against Sponsors of Terrorism Act (P.L. 114-222), which removes sovereign immunity in U.S. courts from foreign governments that are not designated state sponsors of terrorism. It authorizes U.S. courts to hear cases involving claims against a foreign state for injuries, death, or damages that occur inside the United States as a result of a tort—including an act of terrorism—committed anywhere by a foreign state or official.

Legislation that would have created a U.S. Department of Homeland Security (DHS) Office for Countering Violent Extremism failed to advance in Congress.

The bill (H.R. 2899) would have authorized $10 million for the DHS secretary to establish the office through 2020 to coordinate DHS’s efforts to counter violent extremism by identifying risk factors and populations targeted by propaganda and recruiters. Managing DHS outreach and engagement efforts at-risk communities was also included.

House Homeland Security Committee Chair Michael McCaul (R-TX) introduced the bill, which did not advance in the House.

The House also failed to pass a bill that would have encouraged banks to tip off federal investigators about terrorism financing. H.R. 5606 would have enhanced Section 314 of the Patriot Act to allow financial institutions to report to the federal government if they suspected funds were being used for “terrorist acts, money laundering activities, or a specified unlawful activity.”

The bill also would have shielded financial institutions from civil litigation for filing these reports.

CYBERSECURITY. As part of an omnibus spending bill in 2015, Congress passed the Cybersecurity Information Sharing Act (P.L. 114-110).

The act allows private entities to share and receive cyberthreat indicators and defensive measures with other entities and with the federal government. Threat indicators are defined as information that is “necessary to describe or identify malicious reconnaissance.”

Companies, however, must remove personal identifying information not related to cybersecurity threats before sharing data under the act.

It also allows the director of national intelligence and the U.S. Departments of Homeland Security, Defense, and Justice to share cyberthreat indicators with private companies and state, tribal, or local governments.

Congress failed to advance legislation that would have directed the National Highway Traffic Safety Administration (NHTSA) and the Federal Trade Commission (FTC) to create federal standards to secure vehicles.

The bill (S. 1806) would have created vehicle performance standards that required all access points in vehicles to be equipped with reasonable measures to protect against hacking attacks, all collected information from the vehicle to be secured to prevent unwanted access, and all vehicles to be equipped with technology that can detect, report, and stop hacking attempts in real time.

AVIATION. Congress passed legislation (P.L. 114-50) that verifies that airports have working plans in place to respond
HIGH VALUE THEFT, REPUTATIONAL RISK, SUPPLY CHAIN DISRUPTION?

ALL OF THE ABOVE?

ASIS EUROPE 2017
FROM RISK TO RESILIENCE
MICO, MILAN ITALY 29–31 MARCH 2017

www.asiseurope.org
to security incidents inside their perimeters.

The law directs the assistant secretary of homeland security to verify at all U.S. airports that the Transportation Security Administration (TSA) performs or oversees implementation of security measures and that airports have working plans in place to respond to active shooters, acts of terrorism, and incidents that target passenger-screening checkpoints.

The assistant secretary must then report his or her findings to Congress to identify best practices and establish a mechanism to share those with other airport operators.

Congress failed, however, to pass a bill that would limit airport employees’ access to secure areas within airport facilities.

The bill (H.R. 3102) would have directed the TSA to create a risk-based, intelligence-driven model for screening airport employees based on the level of employment-related access to Secure Identification Display Areas, Airport Operations Areas, or secure areas at U.S. airports.

Additionally, it would have required TSA to create a program to allow airport badging offices to use E-Verify, create a process to transmit credential application data received by DHS to ensure that it’s complete and matches data submitted by airport operators.

The House passed the bill, which stalled in the Senate Commerce, Science, and Transportation Committee.

In a Federal Aviation Administration (FAA) extension act, Congress

LEGAL REPORT | BY MEGAN GATES

LEGAL HIGHLIGHTS

<table>
<thead>
<tr>
<th>ISSUE</th>
<th>Minimum Wage</th>
</tr>
</thead>
<tbody>
<tr>
<td>BILL</td>
<td>SB-3</td>
</tr>
<tr>
<td>VENUE</td>
<td>California</td>
</tr>
<tr>
<td>STATUS</td>
<td>Enacted</td>
</tr>
<tr>
<td>SIGNIFICANCE</td>
<td>Raises the minimum wage to $10.50 per hour for businesses that employ 26 or more people. Other employers will be required to raise their minimum wage to $10.50 in 2018.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ISSUE</th>
<th>Surveillance</th>
</tr>
</thead>
<tbody>
<tr>
<td>BILL</td>
<td>Investigatory Powers Bill</td>
</tr>
<tr>
<td>VENUE</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>STATUS</td>
<td>Enacted</td>
</tr>
<tr>
<td>SIGNIFICANCE</td>
<td>Enhances the government’s powers to spy on citizens and requires companies to decrypt data on request, limiting the use of end-to-end encryption.</td>
</tr>
</tbody>
</table>
The ASIS Foundation

Preparing tomorrow’s security leaders
by investing in research, leadership,
and community today.

In 2016, the Foundation

- **invested** more than $500,000 in scholarships, communities, and educational awards
- **helped** more than 200 members and students take important steps forward in their professional growth
- **published** valuable research on security metrics and sports team travel security
- **provided** opportunities many would not get elsewhere

We could not have done it without you!

Donate today and help the ASIS Foundation continue to create strong communities, practical research, and education opportunities for security professionals across the globe.

www.asisfoundation.org/giveback
created a variety of new security measures to enhance aviation security. Under the law (P.L. 114-190), the number of government “viper teams” increased from 30 to 60. These teams stop and search suspicious passengers in public places outside the airport.

Another measure requires new passenger airlines to create secondary barriers to keep unauthorized individuals from gaining access when a pilot opens the cockpit door. It also requires the FAA to consider whether to implement additional screening for mental health conditions as part of a comprehensive medical certification process for pilots.

Additionally, the law requires TSA to use private companies to market and enroll more individuals in its PreCheck program. It also requires the FAA to authorize package deliveries by drones within two years of its passage.

DRONES. Congress failed to pass legislation that would address the security implications of drones. The bill (H.R. 1646) would have required DHS to assess the security risks associated with commercially available small and medium unmanned aerial systems (drones). The measure would also have required DHS to develop policies, guidance, and protocols to prevent or mitigate the risks if drones are used in an attack.

The House passed the legislation, which later stalled in the Senate.

PRIVACY. Congress extended some rights under the U.S. Privacy Act to European Union citizens and other designated allies. The Judicial Redress Act (P.L. 114-129) allows the U.S. Department of Justice—with the agreement of the U.S. Departments of State, Treasury, and Homeland Security—to designate countries or organizations whose citizens may pursue civil remedies if they have appropriate privacy protections for sharing information with the United States.

The law was enacted as part of an agreement between the United States and the European Union that allows the two to exchange more data during criminal and terrorism investigations.

HUMAN TRAFFICKING. Congress expanded the definition of child abuse under the Victims of Child Abuse Act of 1990 to include human trafficking and the production of child pornography. The law (P.L. 114-22) also expands prosecution to include individuals who patronize or solicit people for a commercial sex act, “making traffickers and buyers equally culpable for sex trafficking offenses.”

COMMUNICATIONS. A new law requires DHS to achieve and maintain interoperable communications. The law (P.L. 114-29) requires a DHS undersecretary to submit a strategy to Congress to achieve and maintain communications for daily operations, planned events, and emergencies.

The strategy must include an assessment of interoperability gaps in radio communications among DHS groups, information on DHS efforts to achieve and maintain interoperable communications, and information about the adequacy of mechanisms available to the undersecretary to enforce and compel compliance with interoperable communications policies and directives of DHS.

SCREENING. Congress did not advance a bill that would require the FBI to ensure that select individuals applying for U.S. refugee admission receive full background investigations before being admitted to the country.

DHS already conducts such screenings, but the bill (H.R. 4038) would have required the FBI to perform background investigations on nationals or residents from Iraq or Syria, individuals with no nationality whose last residence was in Iraq or Syria, and individuals present in Iraq and Syria at any time on or after March 1, 2011.

The House passed the bill, which stalled when it reached the Senate floor.

DISASTER RELIEF. Congress passed legislation that requires the Federal Emergency Management Agency (FEMA) to develop and implement a plan to control and reduce administrative costs for delivering assistance for major disasters. The measure would have expanded the definition of “disaster” under the Stafford Act (P.L. 114-132) to include Iraq or Syria, and individuals present in Iraq or Syria at any time on or after March 1, 2011. The law requires the FEMA to submit a strategy to Congress to achieve and maintain communications for daily operations, planned events, and emergencies.

The strategy must include an assessment of interoperability gaps in radio communications among DHS groups, information on DHS efforts to achieve and maintain interoperable communications, and information about the adequacy of mechanisms available to the undersecretary to enforce and compel compliance with interoperable communications policies and directives of DHS.

Congress did not advance a bill that would require the FBI to ensure that select individuals applying for U.S. refugee admission receive full background investigations before being admitted to the country.

DHS already conducts such screenings, but the bill (H.R. 4038) would have required the FBI to perform background investigations on nationals or residents from Iraq or Syria, individuals with no nationality whose last residence was in Iraq or Syria, and individuals present in Iraq and Syria at any time on or after March 1, 2011.

The House passed the bill, which stalled when it reached the Senate floor.

DISASTER RELIEF. Congress passed legislation that requires the Federal Emergency Management Agency (FEMA) to develop and implement a plan to control and reduce administrative costs for delivering assistance for major disasters. Under the law (P.L. 114-132), FEMA must compare the costs and benefits of tracking administrative cost data for major disasters by public assistance, individual assistance, hazard mitigation, and mission assignment programs.
FEMA must then submit to Congress by November 30 each year—until 2023—a report on the total amount spent on administrative costs.

**PRISONS.** Congress authorized legislation that requires the director of the Bureau of Prisons to issue oleoresin capsicum spray (pepper spray) to designated individuals.

The law (P.L. 114-133) requires the director to issue the spray to any bureau officer or prison employee who may respond to an emergency situation in the prison. The law also allows the director to distribute the spray to prison officers and employees as appropriate. Minimum and low-security prisons are excluded from the requirement.

Officers and employees designated to use the spray must first be trained on how to use it, and are required to undergo annual training on using the spray.

**EQUIPMENT.** The Senate failed to pass legislation that would have allowed DHS to give excess nonlethal equipment and supplies to foreign governments.

Under the bill (H.R. 4314), DHS would have provided these supplies to foreign governments if doing so furthered U.S. homeland security interests and enhanced the recipient government’s capacity to mitigate the threat of terrorism, infectious disease, or natural disaster; protect lawful trade and travel; or enforce intellectual property rights.

The House passed the bill, which stalled in the Senate Foreign Relations Committee.

**SEXUAL ASSAULT.** Congress established rights for sexual assault survivors that clarify what basic services sexual violence victims are entitled to.

Under the law (P.L. 114-236), victims may not be prevented from obtaining a medical forensic examination. They may not be charged for the examination. They have the right to have sexual assault evidence collection kits and their contents preserved—without charge—for the duration of the maximum statute of limitations or 20 years (whichever is shorter). They also have the right to be informed of any result of a collection kit if the disclosure would not impede or compromise an ongoing investigation.

Victims also have the right to be informed—in writing—of policies governing the collection and preservation of collection kits, and the right to receive written notification from officials no later than 60 days before their collection kit is to be destroyed or disposed of.

This column should not be construed as legal or legislative advice.
SECURITY AT ASIS 2016

ALLIED UNIVERSAL provided physical security at ASIS International’s 62nd Annual Seminar and Exhibits in Orlando, Florida. Allied Universal security officers and the company’s new robots patrolled the exhibit hall to help ensure a safe and secure environment.

Partnering with Allied Universal for security for the ASIS conference was Dan Taylor & Associates, LLC, a firm that specializes in trade show security. The companies have worked together for five years to provide security for the event.

Allied Universal is working with Knightscope to provide its new Machines as a Service program. The Knightscope K5 and K3 Autonomous Data Machines operate within a geofenced area and provide alerts generated by video cameras, thermal imaging, license plate recognition, audio recording, two-way intercom, and more. Shown here, Stacy Stephens of Knightscope (center) chats with two attendees.

Digi Security Systems partnered with March Networks to offer customers more electronic security products tailored specifically to the retail and banking markets.

DirectView Holdings, Inc., installed a comprehensive surveillance, alarm, and access control system for Primary at its flagship location in New York City.

New partnerships for exacqVision include integrations with Commend intercom systems and Hartmann Controls Protector.net Web-based access control systems.

Handheld mobile reader systems using Farpointe reader modules are now available from Cypress Integrated Solutions.

Galaxy Control Systems is introducing a hosted access control partnership program. The first partners are Bold Technologies, Dynamark, and Advanced Access Security.

GET Group North America is partnering with Speed Identity to offer biometric, live capture solutions for identity, credential, and access management to the North American market.

PARTNERSHIPS AND DEALS

Altronix appointed Thomasson Marketing Group to represent its power and transmission solutions in California, Hawaii, Nevada, and Arizona.

SMARTair wireless access control from ASSA ABLOY is in use at Córdoba, Spain’s new Red Cross building.

Axis Communications will market network video products from Canon Inc. in Europe, the Middle East, and Africa, plus North America.

BriefCam announced a technology integration partnership with Digifort, enabling users to extract data collected on their surveillance systems and achieve better security and operational management.

Computer Products Solutions, a division of Panasonic System Communications Europe, and FusionPipe Software Solutions Inc. formed a partnership for Panasonic to sell and support FusionPipe’s patented QuikID authentication solutions.
Hanwha Techwin America announced that its SRM-872 mobile NVR now integrates with the Genetec Security Center 5.5 SR1 security platform, allowing its use on trains, buses, and other modes of public transportation.

South Africa’s Western Province Blood Transfusion Service contracted installer Verivision to develop a hybrid security solution. Verivision chose products from Hikvision as the basis for the system.

Morphean is hosting its management platform for content analysis videos and incident detection in Interoute’s Virtual Data Centre.

March Networks integrated its Searchlight for Retail software with high-performance RFID technology from Zebra Technologies.

Netwrix Corporation announced that Bank of the South chose Netwrix Auditor to secure customer data and facilitate compliance with regulatory standards.

OffSite Vision Holdings, Inc., played an integral role in the 2016 Texas Night event hosted by the ASIS Houston Chapter at B.B. King’s Blues Club in Orlando. The EmergenZ People Pass System helped streamline the entry process for authorized attendees. It incorporated technologies from multiple security vendors including Orion Entrance Control, Inc.; Genetec; and Blue Line Technology.

The integration between OnSSI Ocularis 5 and Hitachi Visualization Suite software and Video Management Platform provides a public safety solution that supports safer communities through connected intelligence.

Regroup Mass Notification and Lexco Security Systems entered a partnership that will provide organizations with the technology and thought leadership necessary to improve on-premises security and employee safety. Regroup is also partnering with Singlewire Software for an integrated notification solution.

RiverSafe is a partner of the ThreatQuotient Threat Alliance Partner program, providing both technology and consulting services to protect data and IT systems.

Plastilam will purchase millions of Smartrac PRELAM inlays for contactless access cards over the next three years.

Quantum Corp. announced joint development initiatives with four video management system providers: Aimetis Corp., OnSSI, Qognify, and Verint Systems Inc. have joined the Quantum Advantage Program.

Securonix formed a partnership with ThetaPoint, Inc., to deliver security solutions that predict, prevent, and detect cyberthreats to enterprise security.

PSA Security Network and Sen-

<table>
<thead>
<tr>
<th>ASIS BOARD OF DIRECTORS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PRESIDENT</strong></td>
</tr>
<tr>
<td>Thomas J. Langer, CPP</td>
</tr>
<tr>
<td>BAE Systems Inc.</td>
</tr>
<tr>
<td>Arlington, Virginia</td>
</tr>
<tr>
<td><strong>PRESIDENT-ELECT</strong></td>
</tr>
<tr>
<td>Richard E. Chase, CPP, PCI, PSP</td>
</tr>
<tr>
<td>General Atomics</td>
</tr>
<tr>
<td>San Diego, California</td>
</tr>
<tr>
<td><strong>TREASURER</strong></td>
</tr>
<tr>
<td>Christina Duffey, CPP</td>
</tr>
<tr>
<td>Anderson Security Agency</td>
</tr>
<tr>
<td>Phoenix, Arizona</td>
</tr>
<tr>
<td><strong>SECRETARY</strong></td>
</tr>
<tr>
<td>Godfried Hendriks, CPP</td>
</tr>
<tr>
<td>GOING Consultancy B V</td>
</tr>
<tr>
<td>Alkmaar, The Netherlands</td>
</tr>
<tr>
<td><strong>CHAIRMAN OF THE BOARD</strong></td>
</tr>
<tr>
<td>David C. Davis, CPP</td>
</tr>
<tr>
<td>Apple Valley, California</td>
</tr>
<tr>
<td><strong>DIRECTORS</strong></td>
</tr>
<tr>
<td>Charles E. Andrews, CPP</td>
</tr>
<tr>
<td>Friends of Chuck</td>
</tr>
<tr>
<td>Houston, Texas</td>
</tr>
<tr>
<td>Howard J. Belfor, CPP</td>
</tr>
<tr>
<td>Belfor &amp; Associates</td>
</tr>
<tr>
<td>Black Mountain, North Carolina</td>
</tr>
<tr>
<td>Michael R. Bouchard, CPP</td>
</tr>
<tr>
<td>Janus Global Operations</td>
</tr>
<tr>
<td>Reston, Virginia</td>
</tr>
<tr>
<td>Darryl R. Branham, CPP</td>
</tr>
<tr>
<td>Avnet Inc.</td>
</tr>
<tr>
<td>Phoenix, Arizona</td>
</tr>
<tr>
<td>Gail Essen, CPP, PSP</td>
</tr>
<tr>
<td>Honeywell Building</td>
</tr>
<tr>
<td>Andover, Minnesota</td>
</tr>
<tr>
<td>Radek Havlis, CPP</td>
</tr>
<tr>
<td>Deutsche Telekom AG</td>
</tr>
<tr>
<td>Bonn, Germany</td>
</tr>
<tr>
<td>Jeffrey J. Lee, CPP</td>
</tr>
<tr>
<td>Saudi Aramco</td>
</tr>
<tr>
<td>Dhahran, Saudi Arabia</td>
</tr>
<tr>
<td>Richard F. Lisko, CPP</td>
</tr>
<tr>
<td>Dallas, Texas</td>
</tr>
<tr>
<td>Timothy M. McCreight, CPP</td>
</tr>
<tr>
<td>Above Security</td>
</tr>
<tr>
<td>North Vancouver, Canada</td>
</tr>
<tr>
<td>Jaime P. Owens, CPP</td>
</tr>
<tr>
<td>Panama Canal Authority</td>
</tr>
<tr>
<td>Panama City, Panama</td>
</tr>
<tr>
<td>John A. Petruzzi, Jr., CPP</td>
</tr>
<tr>
<td>Charter Communications</td>
</tr>
<tr>
<td>New York, NY</td>
</tr>
<tr>
<td>Malcolm C. Smith, CPP</td>
</tr>
<tr>
<td>Sasol Doha, Qatar</td>
</tr>
</tbody>
</table>
sera Systems formed a partnership to distribute Sensera’s solar/wireless/cloud site camera solutions.

Sensory Inc. and Samsung SDS announced a global partnership to provide customers with authentication services.

Sopra Steria announced a new partnership agreement with Sybenetix to enable investment firms to integrate behavioral management and compliance solutions.

Talkaphone added PLG Security as a manufacturer’s representative for Canada and Intelligent Marketing Inc. to represent the company in the eastern and southeastern United States.

ZKAccess welcomed Associated Engineering Systems, Inc., as an authorized partner.

GOVERNMENT CONTRACTS

BlackBerry’s secure tablet, integrated with government-grade MAM technology, was approved by the German Federal Office for Information Security at the “classified—for official use only” security level.

Buffalo Computer Graphics announced that its DisasterLAN Incident Management Software was recently used during the Vigilant Guard exercise administered by the Vermont National Guard and Vermont Division of Emergency Management and Homeland Security to test the state’s emergency response.

Working with Service Employees International Union—United Service Workers West, the Building Skills Partnership, passenger services contractor G2, and American Airlines, Los Angeles World Airports will develop a pilot training program for passenger service workers at Los Angeles International Airport in emergency response and situational awareness.

CNC Technologies was selected by the Bexar County Sheriff’s Office in Texas to deploy a mission-receive site to support the agency’s airborne policing and public safety operations. The system will enable personnel to receive encrypted data and video streams from department and partner agency aircraft.

COPsync, Inc., announced that the Bennington Oklahoma Police Department has joined the COPsync communication and information sharing network.

The Bergen County Sheriff’s Office in New Jersey selected Hanwha Techwin IP video surveillance cameras for security in its new parking structure and renovated police services building.

Hikvision USA Inc. provided Becker Public Schools in Minnesota with a security upgrade to protect students, staff, and facilities.

The International AntiCounterfeiting Coalition signed a memorandum of understanding with the City of London Police to formalize their solidarity in fighting for intellectual property rights.

Milestone Systems is helping the Topeka School District in Kansas with a video surveillance and inte-
SAVE THE DATES!

Mark your calendars for five important weeks of education and career development in 2017. Join us to earn CPEs and attend multiple programs in one trip!

**MARCH**
- BOSTON
  - REGISTRATION NOW OPEN
  - Save $100 with early bird rates through January 28
  - 6-7: CPP Review
  - 6-7: PSP Review
  - 6-9: ASIS Assets Protection Course™: Principles of Security (APC I)

**MAY**
- LAS VEGAS
  - 8-9: Active Shooter
  - 8-9: Executive Protection
  - 8-11: ASIS Assets Protection Course™: Practical Applications (APC II)
  - 10-11: Violence Assessment and Intervention
  - 10-12: Physical Security: Introductory Applications and Technology Workshop

**JULY**
- DENVER
  - 10-12: Facility Security Design
  - 10-13: Crisis Management: Program Planning and Crisis Plan Development
  - 10-13: ASIS Assets Protection Course™: Functional Management (APC III)

**SEPTEMBER**
- DALLAS
  - 23-24: CPP Review
  - 23-24: PCI Review
  - 23-24: PSP Review
  - Additional classroom programs to be announced soon.

**NOVEMBER**
- NEW ORLEANS
  - 6-7: Security Force Management
  - 6-8: Conducting Advanced Internal Investigations
  - 6-8: Risk, Threat, and Vulnerability Assessment
  - 9-10: Soft Targets
  - 9-10: Executive Protection

www.asisonline.org/profdev
Tyco Security Products announced that Wakefield Grammar School Foundation in Yorkshire, England, deployed an access control and video surveillance solution using multiple Tyco brands that will increase security across its five-school campus.

The Florida Fish and Wildlife Conservation Commission. Vigilant Solutions is providing fixed cameras to the La Verne Police Department in California to improve the safety of the community.

**AWARDS AND CERTIFICATIONS**

**Allied Universal** was awarded the Brandon Hall Gold award for the Best Launch of a Corporate Learning University.

**Geoswift** has obtained TRUSTe Enterprise Privacy Seals in both English and Simplified Chinese for the Geoswift website and PayTuitionNow portal.

**Global Technical Systems** gained status as a National Security Agency Trusted Integrator for Commercial Solutions for Classified Programs.

**Halton Regional Police Service** of Ontario, Canada, has been named a 2016 Computerworld Data + Editors’ Choice Award honoree for its use of Hexagon Safety & Infrastructure software in innovative Big Data initiatives.

The **Hikvision PanoVu Panoramic Camera** won a GIT SECURITY Award for its simple design, superior image quality, and easy installation.

At the CTIA conference, **Smartvue Corporation** won the IoT Emerging Company of the Year Award for the Consumer Market.

**SPHERE Technology Solutions** received national certification as a Women’s Business Enterprise by the Women Presidents Educational Organization.

**Veridos** announced that its ID smart card system was recognized with an Asia Pacific Smart Card Association Radiant Award for its smart technology.

**WHOA.com** announced that its data centers and cloud infrastructure have been validated for PCI DSS 3.1 compliance.

**Frost & Sullivan** presented Worldtech, a GE company, the 2016 North America Frost & Sullivan Award for Product Line Strategy Leadership.

**ANNOUNCEMENTS**

The Partnership for Priority Verified Alarm Response announced that ADT has joined the organization as a full industry member.

**Axon Public Safety Canada Inc.**, a subsidiary of TASER International, announced a partnership with the Canadian Centre of Public Safety Excellence to support the organization with access to technology including Axon body-worn cameras.

**Cambridge Pixel** is offering a free software tool to assist commercial security and defense integrators, installers, and developers to select the optimum location for a radar or other sensors.

**Canadian Pacific Railway** has introduced a new Web page that showcases its dangerous goods—response capabilities, training available to first responders, and other online resources.

**The Centers for Medicare & Medicaid Services** finalized a rule to establish consistent emergency preparedness requirements for healthcare providers participating in Medicare and Medicaid, increase patient safety during emergencies, and establish a more coordinated response to natural and man-made disasters.

**COPsync, Inc.** announced that Amber, Silver, and Blue alerts will be distributed via the COPsync Network to the thousands of officers using the system across the United States.

**Eyewitness Surveillance** secured an investment from LLR Partners to sup-
port the company’s expansion of its services and growth into new geographic and vertical markets.

**Galaxy Control Systems** offers an online video library on its website, including professional videos that provide answers to its eight most common tech support questions.

**Hoyos Labs** rebranded as **Veridium**, heralding a new corporate strategy and the launch of its end-to-end biometric authentication solution VeridiumID.

The **Imaging Source Europe GmbH** moved into new corporate headquarters in Bremen Überseestadt, Germany.

**IntellCorp** is making its services available in Portuguese-speaking nations around the world.

**March Networks** introduced a Security Audit tool to help systems integrators evaluate and improve the security of their video installation configurations and provide additional assurance to their customers.

**OpenSesame** is partnering with publisher **Ed4Online** to distribute a free Zika Virus Prevention Course worldwide.

**Parabon NanoLabs** is calling for participants in a research study, sponsored by the **U.S. Department of Defense**, in which DNA samples from distant relatives will be analyzed to improve familial matching. The research will assist in the identification of deceased service members.

**Raytec** launched a redesigned website dedicated to helping customers deliver the best lighting solutions for video surveillance.

To demystify pandemics, **Send Word Now** developed a new eBook: **Is Your Organization Ready for a Pandemic?**

**Vulsec, LLC**, unveiled a new YouTube video that details how companies can become vulnerable to cybersecurity attacks and what they can do to prevent and protect themselves from such attacks.

**Weir-Jones Engineering Ltd., and SGS Canada Inc.**, will bring affordable Earthquake Early Warning System technology, known as ShakeAlarm, to countries with high seismic risk that currently do not have systems in place to protect lives in the event of a major earthquake.

**Wombat Security Technologies** updated its platform to provide users with flexible training via the release of seven mobile-responsive modules.

**ZKAccess** was a sponsor of the first annual GreyStar Charity Golf Event to help raise funds for the **Post Traumatic Stress Disorder Foundation of America**.

**ASIS NEWS**

**LANGER TAKES THE HELM**

The incoming President of **ASIS International** Thomas J. Langer, CPP, will lead a Society in transition. The retirement of longtime CEO Michael Stack and the selection of incoming CEO Peter J. O’Neil, CAE, in 2016, set the stage for numerous changes in the years ahead. Langer spoke to **Security Management** about his experiences in ASIS and his plans for the Society’s future.

Langer says that he first became aware of ASIS through the Granite State Chapter in New Hampshire. “I worked for Joe Reynolds, who was the head of security at the time at Sanders Associates, and he had served on the ASIS Board of Directors and was a big proponent. So I joined the chapter and became more active through the council. The ASIS Defense and Intelligence Council was where I spent a lot of time starting in the early 1990s,” serving in every leadership position at least once.

When Langer first encountered ASIS he didn’t see the big picture. “I was so focused on government security that I didn’t have a real appreciation of the other aspects of the Society—of the other disciplines that are represented. With my involvement in the Board and at the council level—especially the Volunteer Leadership Conference each January—I got to see how much bigger the organization is and how many different industries it encompasses. I realized that there was so much I could learn from other members based on the experiences they had. I found it to be so helpful for me professionally,” Langer says.

However, Langer did immediately grasp the significance of his involvement with the Defense and Intelligence Council. “Through the council, ASIS was one of the first organizations in the defense and intelligence industry to bring in other cleared people from different countries. What I found by doing that—we had some support from the Canadians and the United Kingdom—is that we all had similar problems in bridging the
Once involved with ASIS, other volunteer leaders mentored Langer, encouraging him to get more involved. “I credit [former ASIS President] Cindy Conlon, CPP, with inspiring me to get more involved in ASIS. Cindy was the one who kept steering me right back to ASIS and what I was going to do in the future. She really pushed me.”

While Langer was active in other associations, such as the Aerospace Industries Association, at the time, Conlon kept reminding Langer that ASIS welcomed quality leaders. “Cindy kept steering me right back to ASIS International. In the late 2000s, a spot opened up on the Board and I asked to be considered. It’s been a great run,” says Langer.

According to Langer, the ASIS Board of Directors is unified in its vision for the Society as it seeks to deliver value to existing members, draw in additional members, and serve international constituencies.

**Value.** “I think the most important piece we need to deliver is the value proposition,” says Langer “We want a member to be able to look at ASIS International and conclude ‘I see the value in what this organization offers to my job,’ no matter where they are on the career spectrum from entry level to CSO.”

According to Langer, the value proposition can be showcased in many services ASIS offers from “delivering great educational opportunities and content to the members to helping them form the communities that will help them and to be responsive to their needs no matter where they are.”

Langer says that it’s critical for the Society to present tools and educational opportunities that help members reduce risk in their organizations. “We want their employers to also understand why this is an important membership,” he

**For John C. Villines, CPP, PCI, PSP,** the most rewarding aspect of practicing security management is making a difference for both his employees and his clients. “The employees benefit by developing the skills and knowledge that will enable them to pursue a viable career,” he says, and clients benefit “by having their assets protected and risks reduced or eliminated.”

Director of a consultancy that he founded in 1979, the same year he joined ASIS International, Villines oversees the operation of all federal government and private sector contracts and participates in the firm’s seminars and consulting assignments. While as many as seven independent contractors may report to him at any point, he strongly believes in collaboration. “This is a two-way street,” he says. “While the buck stops with me, I think it’s accurate to say that I report to each of them and to each of the clients we serve.”

Villines started his security career in 1973 as a security patrol officer and advanced through the ranks at an upscale shopping center in Atlanta, Georgia, leaving in 1985 as director of security operations. He moved on to become operations manager for a firm overseeing two shopping centers, with responsibility for both security and facilities management, before deciding to concentrate on his own contract security services and private investigations firm.

Along the way, Villines received undergraduate degrees and attended law school. While an undergraduate, he interned with the Georgia Police Academy and developed its first Crime Prevention Specialist training program for personnel in law enforcement agencies and private entities. In 2008 he completed a master’s degree in security management.

Villines serves on the six-person Georgia Board of Private Detective and Security Agencies, one of the two members from the security industry. Villines was appointed by two successive governors to this board, and he has chaired it for nearly half of the 13 years he has served on the board. This appointment moved him to pursue his first ASIS board certification.

“I believed it was important that the person at the helm of regulating the industry in Georgia should demonstrate competency in security management,” he says, and “the CPP designation is the most widely recognized and respected symbol of that competency.” He became a Certified Protection Professional® (CPP) in 2003, the year he was first appointed to the state board, and earned the Professional Certified Investigator® (PCI) and Physical Security Professional® PSP certifications in 2015.

Villines asserts that his ASIS membership has provided “tremendous resources” through the years in his efforts to keep pace with the ever-changing aspects of the security management field. His certifications “provide clients and potential clients with immediate assurance that I have demonstrated competency in the skills and knowledge relevant to meeting their needs,” he says.

While he recommends ASIS certifications to clients and in seminars as a way to enhance one’s professional career, he offers this advice: “Study, study, STUDY...and speak with your colleagues.”

Villines has put this advice to work in his own family. His son, Joshua Villines, is also an ASIS triple certificant, earning the three designations between 2013 and 2016. A security professional himself, Joshua Villines, CPP, PCI, PSP, will be profiled in the February 2017 issue of Security Management.
says, “why it’s important to professional development for them.”

Growth. The key to future growth, says Langer, is to leverage ASIS’s professionalism to garner new members. “We want new members, but for the right reason,” he says. “If we increase the value proposition, growth in the membership will follow that. People will see ASIS as the organization they want to belong to and as the best bang for the buck.”

Membership growth also follows the rising competence of the industry, according to Langer. “Part of what we need to do is to get people to understand that this is a profession. Something to aspire to,” he says. “You look at the Paris attacks—the security folks at the stadium were actually quite good at countering people who were trying to get in. There’s a lot of good that our profession does, and we need to get better at getting it out there so people see this as a true profession, as a calling—not just as a second career.”

Internationalism. The next step, according to Langer, is to address the needs of members worldwide. “From New York City to Nigeria to the Middle East and all the places in between...security professionals have different circumstances, a different set of challenges.”

To serve these members, Langer says the Society can form strong, professional communities that members can draw on to help counter their challenges and to progress their own careers. However, this challenge will be significant.

“We’ve got even more to do,” says Langer. “There are opportunities in many countries for the security profession. We want to get away from being an American-centric organization. The Board is focused on that.”

Langer says that convincing more international members to serve as volunteer leaders is a good place to start. “We want to have more international members on the Board. We want geographic, race, and gender diversity on the Board. We think that any organization with that kind of diversity, that actually looks like its membership, is going to be far more successful. And the ideas and experiences they share are going to benefit the entire organization.”

KANSAS CITY WINS SIMEONE AWARD
At ASIS 2016 in Orlando, Florida, the Law Enforcement Liaison Council and the ASIS Foundation awarded the 6th annual Matthew Simeone Award for Public-Private Partnership Excellence to the Kansas City Chapter for its partnership with the Overland Park, Kansas, Police Department. The award-winning Overland Park Residential Security Initiative brought law enforcement, private security, home builders, and educational institutions together to develop a program based on sound security principles, targeting criminals’ behavior and identifying products and companies that best serve the interest of the community.

Additional information on the award and this winning partnership can be found at https://foundation.asisonline.org/Simeone.

RENEW TODAY
If you haven’t renewed your ASIS International membership for 2017, time is running out. Visit www.asisonline.org/renewal to renew online.

LIFETIME CERTIFICATION GRANTED
The following security professionals have been awarded lifetime certification status.

- Michael A. Pepper, CPP, PSP
- Peter Stella, Jr., CPP
- William F. McCarthy, CPP
- John D. Twiggs, IV, CPP
- David A. Brondyk, CPP
- Kevin R. Sexton, CPP
- Robert A. Currier, CPP
- Terry L. Boone, CPP
- Fredrick G. Roll, CPP

STANDARDS AND GUIDELINES UPDATE
ANSI/ASIS PSC.1-2012, Periodic Maintenance/Evaluation
The ANSI/ASIS PSC.1-2012 Standard is approaching its fifth year as an American National Standard. Consistent with ANSI requirements, this project involves evaluating the standard to consider changes to applicable laws, regulation, and/or international agreements impacting the standard’s use, including industry good practices, lessons learned, and implementation feedback. The PSC.1 Standard establishes a mechanism for private security providers and their clients to provide demonstrable commitment, conformance and accountability to the principles outlined in the International Code of Conduct for Private Security Service Providers and the Montreux Document.

If you are interested in serving on this committee, contact standards@asisonline.org. Applications are being accepted in the User/Manager and General Interest categories.

For additional information on ASIS’s Standards & Guidelines project, visit: https://www.asisonline.org/Standards-Guidelines/Pages/default.aspx.
**VIDEO MANAGEMENT**

**INDIGOVISION** of Edinburgh, Scotland, launched Video Management Software with control Center v14.0 to improve the way the software is delivered. It can be purchased at three levels: IndigoLite, IndigoPro, and IndigoUltra. The tiered offerings enable customers to buy only what they need. Easier licensing results in straightforward setup and maintenance, saving time and money. Features include real-time monitoring, map-based tracking, video wall compatibility, incident management, NVR switching, and more. 101

**EMERGENCY CALLS**

New emergency call system kits and components from **CAMDEN DOOR CONTROLS** of Mississauga, Ontario, Canada, support the use of momentary emergency assistance activation devices. The new CX-WEC12 Emergency Call System Kit is designed for universal restrooms with pushbutton reset, and the CX-WEC13 Emergency Call System Kit works for universal restrooms with key switch reset. They support the use of momentary “press for emergency assistance” activation devices, such as tape switches. Using momentary switches also requires a reset device to deactivate the alarm. The units offer the option for a CM-8000/13 reset push button or CM-1100/14 reset key switch. 103

**DIAGRAMMING SOFTWARE**

**FARO** of Lake Mary, Florida, released FARO Zone 2D diagramming software that is optimized for law enforcement, fire service, and insurance professionals. It allows professionals to quickly create accurate diagrams without the complexity of traditional CAD programs. A new intuitive command interface uses Work-Flow Ribbons to allow users to quickly create diagrams for crashes, crime scenes, pre-incident plans, and fire-protection plans. Diagrams can be saved to several standard image formats for integration into reports. 104

**VIDEO SURVEILLANCE**

Performance, equIP, and HDZ series cameras from **HONEYWELL** of Northford, Connecticut, combine with the XOa 3.2.33-enabled ADPRO FastTrace 2E video recording and alarm transmission solution and the iFT Series remotely programmable operating system from Xtralis to help security professionals design connected building systems. They are easy to use, easy to install, and provide higher-quality video. New in XOa 3.2.33 are improved automatic focusing support with an ONVIF Profile S driver, improved cybersecurity level on remote access, and enhanced camera timestamp synchronization. 105
**DRONE RESPONSE**

The ReDrone system from **ELBIT SYSTEMS** of Haifa, Israel, provides protection for closed air spaces, national infrastructures, and other critical areas against hostile drones. Designed to detect, identify, track, and neutralize different types of drones, it can also separate a drone’s signals from its operator’s remote control signals. After detecting a target, the ReDrone system disrupts the drone’s communication with its operator, blocks its radio and video signals and GPS positioning data, and sends it off track. The infrastructure is designed for easy installation in various terrains, and it operates in all weather conditions. The digital control unit, based on Android technology, features an intuitive user interface.

**VIRTUAL REALITY TRAINER**

**ELBIT SYSTEMS** of Haifa, Israel, introduced its Emergency Scenarios Virtual Reality Trainer, a simulation trainer that provides a realistic three-dimensional virtual environment for training emergency response teams to deal with a variety of emergency situations. Scenarios that can be simulated include ballistic missiles falling in an urban area, earthquakes, search-and-rescue operations, and more. The virtual reality goggles allow users to experience these scenarios as if they were part of a response team. Use of the trainer can help reduce operation and maintenance costs, minimize flight and ground training time, and ensure operators’ safety.

**METAL DETECTORS**

**ZKACCESS** of Fairfield, New Jersey, introduced three new metal detectors. The HMD100 handheld metal detector is equipped with programmable alarm settings, so the user can choose from either a sound and light alarm, or vibration and light alarm. The WMD118 walk-through metal detector features six overlapping detection zones with multiple alarms. Sensitivity for each zone is adjustable. Sound and LED alarms located on both sides indicate precisely where metal is detected. The WMD218 walk-through metal detector features 18 overlapping detection zones with multiple alarms. It features a 3.7-inch LCD screen, and sound and LED alarms. Like the WMD118, it automatically counts people and alarms, and only authorized personnel can access the control panel.

**EXPLOSIONPROOF CAMERAS**

Explosionproof security cameras from **LARSON ELECTRONICS** of Kemp, Texas, include analog cameras, compact rechargeable action cameras, and IP cameras. The company also offers NVR systems, DVR systems, security networking equipment and solutions, cabling, and complete turnkey solutions to a variety of security applications within hazardous environments where they can also be used for vessel, tank, and reactor monitoring; remote observation of external facilities; and more. Operators can purchase everything they need from Larson, or they can supplement existing recording systems with explosionproof security cameras and explosionproof cabling.

**NETWORK VIDEO RECORDER**

**TYCO SECURITY PRODUCTS** of Westford, Massachusetts, introduced the new exacqVision M-Series, a cost-effective network video recorder that is easy to install and use. It includes integrated power over Ethernet camera ports and exacqVision START video management software, which can easily be upgraded to the Professional or Enterprise software. Users can connect up to eight IP cameras per recorder and can view and administer live and recorded video directly from the recorder using the included exacqVision client or remotely using a Web browser or exacqVision client on a separate computer. The free Exacq Mobile app allows users to view live and recorded video on iOS or Android mobile devices.
**DRONE RESPONSE**

The ReDrone system from **Elbit Systems** of Haifa, Israel, provides protection for closed air spaces, national infrastructures, and other critical areas against hostile drones. Designed to detect, identify, track, and neutralize different types of drones, it can also separate a drone’s signals from its operator’s remote control signals. After detecting a target, the ReDrone system disrupts the drone’s communication with its operator, blocks its radio and video signals and GPS positioning data, and sends it off track. The infrastructure is designed for easy installation in various terrains, and it operates in all weather conditions. The digital control unit, based on Android technology, features an intuitive user interface. 107

**VIRTUAL REALITY TRAINER**

Elbit Systems of Haifa, Israel, introduced its Emergency Scenarios Virtual Reality Trainer, a simulation trainer that provides a realistic three-dimensional virtual environment for training emergency response teams to deal with a variety of emergency situations. Scenarios that can be simulated include ballistic missiles falling in an urban area, earthquakes, search-and-rescue operations, and more. The virtual reality goggles allow users to experience these scenarios as if they were part of a response team. Use of the trainer can help reduce operation and maintenance costs, minimize flight and ground training time, and ensure operators’ safety. 108

**METAL DETECTORS**

ZKAccess of Fairfield, New Jersey, introduced three new metal detectors. The HMD100 handheld metal detector is equipped with programmable alarm settings, so the user can choose from either a sound and light alarm, or vibration and light alarm. The WMD118 walk-through metal detector features six overlapping detection zones with multiple alarms. Sensitivity for each zone is adjustable. Sound and LED alarms located on both sides indicate precisely where metal is detected. The WMD218 walk-through metal detector features 18 overlapping detection zones with multiple alarms. It features a 3.7-inch LCD screen, and sound and LED alarms. Like the WMD118, it automatically counts people and alarms, and only authorized personnel can access the control panel. 106

**EXPLOSIONPROOF CAMERAS**

Explosionproof security cameras from Larson Electronics of Kemp, Texas, include analog cameras, compact rechargeable action cameras, and IP cameras. The company also offers NVR systems, DVR systems, security networking equipment and solutions, cabling, and complete turnkey solutions to a variety of security applications within hazardous environments where they can also be used for vessel, tank, and reactor monitoring; remote observation of external facilities; and more. Operators can purchase everything they need from Larson, or they can supplement existing recording systems with explosionproof security cameras and explosionproof cabling. 109

**NETWORK VIDEO RECORDER**

Tyco Security Products of Westford, Massachusetts, introduced the new exacqVision M-Series, a cost-effective network video recorder that is easy to install and use. It includes integrated power over Ethernet camera ports and exacqVision START video management software, which can easily be upgraded to the Professional or Enterprise software. Users can connect up to eight IP cameras per recorder and can view and administer live and recorded video directly from the recorder using the included exacqVision client or remotely using a Web browser or exacqVision client on a separate computer. The free Exacq Mobile app allows users to view live and recorded video on iOS or Android mobile devices. 110
**MARKETPLACE**

**POE SWITCH**

To eliminate the need for additional bulky power supplies, **VIDEGENIX** of Brookline, Massachusetts, introduced uSwitch PoE. Simple to use, with no programming required, and with just one input power source, the switch automatically senses and negotiates voltages from 48 volts down while providing 15.4 watts of power per port. For non-PoE devices, uSwitch PoE provides a 12-VDC output. It also has an IP relay that automatically reboots or controls non-PoE devices. The switch automatically builds a control Web page, is password protected, and can operate as a standalone device or be controlled via the Internet or a local intranet. Users can control any device over the Web, including modems, lights, sirens, doors, gates, and cameras. 111

**ATM LOBBY ACCESS**

**PARABIT** of Roosevelt, New York, introduced the Multi-Media Reader (MMR), which works with mobile NFC devices, wearable technology, and magnetic stripe cards. It is also integrated with the ACS-1E ATM Lobby Access Control/Remote Facility Management System, which detects skimming devices installed on or around the MMR Reader. Patented SkimGard technology detects overlay skimmers plus RFID listeners. The reader supports iPhone 6 and newer, Android phones, and wearable tech with NFC. It allows customers to use their smartphones or cards to enter the ATM lobby. 112

**LED BEACONS**

**E2S** of West London, England, developed beacons with output-enhancing, field-replaceable color lenses and LED light sources. These latest features are now available on the LM6 alloy BEx family of beacons. The lenses, molded in UV-stable polycarbonate for long life and toughness and integral prismatic structure for enhanced light output, are available in a choice of colors. The LED version beacon has a high output Cree array, oriented to optimize visibility in any direction. It is user-configurable as a steady light or one of five flashing modes. The combination provides a practical low-power, high-output option suitable for many applications. 113

**DOOR CONTROL**

The CICP2100 uniVerse Single Door Controller from Continental Access, a division of **NAPCO SECURITY TECHNOLOGIES** of Amityville, New York, supports two readers on one door using power over Ethernet. Used in a CA3000 or CA4K access control security management software environment, the tamper-supervised controller features a 54 MHz RISC Processor. The compact unit fits in a standard double-gang electrical box and can be networked with Continental’s Accelaterm or Supertwo Controllers or integrated Trilogy Networx Wireless PIN/Prox Access Control Locks. It includes a paintable metal faceplate cover with LED indicator status window. 114

**ELECTRONIC MEDIA DESTROYER**

The SEM Model SSD1-HS from **SECURITY ENGINEERED MACHINERY** of Westboro, Massachusetts, reduces solid state devices to waste particles of 0.5 millimeters or smaller. Absolute destruction through repetitive high-speed cutting of memory media ensures that all data is properly sanitized. Storage items that can be destroyed include solid state boards, RAM, smartphone and cell phone components, SIM cards, USB flash drives, compact flash, and optical discs. Safety interlocks prevent operation when any safety guard or panel is not in place. An air filtration system is also included. 115

FIND OUT MORE about items featured in Marketplace. Go to http://securitymgmt.hotims.com and search by company, category, or reader service number.
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.

CIRCLE # | PAGE #
--- | ---
08 | Abloy Security, Inc. ......................... 20
09 | AMAG ........................................... 21
29 | ASSA ABLOY .................. 75
03 | Axis Communications ................. 06
26 | Commport Technologies ............. 61
05 | Detex Corporation ..................... 11
18 | DSI (Designed Security Inc.) .......... 48
30 | DSX Access Systems, Inc. .................. 76

CIRCLE # | PAGE #
--- | ---
06 | G4S ................................................. 13
20 | GAI-Tronics Corporation .......... 50
13 | Garrett Metal Detectors ............ 33
02 | Hikvision USA .................. 04
04 | Mercury Security .................. 08
15 | Mission 500 ................... 35
01 | SecurAmerica .................. 2-3
12 | Special Response Corporation .......... 31

ADVERTISERS ONLINE

Abloy Security, Inc.
www.abloyusa.com

AMAG
www.amag.com

ASSA ABLOY
www.intelligentopenings.com/in100

Axis Communications
www.axis.com/support

Commport Technologies
www.comm-port.com

Detex Corporation
www.detex.com/lockdown

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

DSX Access Systems, Inc.
www.dsxinc.com

G4S
www.g4s.us

GAI-Tronics Corporation
www.gai-tronics.com

Garrett Metal Detectors
www.garrett.com

Hikvision USA
www.hikvision.com

Mercury Security
www.mercury-security.com

Mission 500
www.mission500.org

SecurAmerica
www.securamericallc.com

Special Response Corporation
www.specialresponse.com
THE ROLE OF SCHOOL RESOURCE OFFICERS

Mo Canady, Executive Director of the National Association of School Resource Officers (NASRO), Discusses the Security Implications of an SRO’s Role in Today’s Educational Environment.

Q. What are School Resource Officers (SROs) and what are some of their job functions?
A. SROs are sworn law enforcement officers assigned by their employing law enforcement agency to work with schools. They go into the classroom with a diverse curriculum in legal education. They aid in teaching students about the legal system and helping to promote an awareness of rules, authority, and justice. Outside of the classroom, SROs are mentoring students and engaging with them in a variety of positive ways.

Q. What are some of the standards and best practices your organization teaches?
A. There are three important things that need to happen for an SRO program to be successful. Number one, the officers must be properly selected. Number two, they have to be properly trained. And thirdly, it has to be a collaborative effort between the law enforcement agency and the school district. This can’t just be a haphazard approach of, “We have a drug problem; let’s put some police officers in there and try to combat it.” It needs to be a community-based policing approach.

Q. Some SROs have come under fire for being too aggressive in the classroom. What’s your take?
A. There have been a handful of incidents that have played out in the media. But, it is up to the investigating agency to determine right and wrong. I’ve been very happy with the fact that the majority of those officers involved in these incidents have not been trained by us.

Q. How does NASRO train officers to deal with potential threats?
A. In our training, we certainly talk about lockdown procedures and possible responses to active shooter situations, but we don’t get too detailed. It’s really up to each agency to make those kinds of decisions. In the case of an active shooter, I don’t believe most SROs are going to wait for additional backup to get there. Most of them are so bought into their schools and their relationships with their students, that if they hear gunfire, they’re going to go try to stop whatever is happening.

Q. Do SROs consider themselves security officers?
A. We’re engaged in security and it’s a big part of what we do—but it’s just one piece of what we do. Sometimes when people think about physical security, the idea of relationship building doesn’t necessarily come in there, and yet it’s the lead thing for us. We know that through those relationships, if we’re building them the right way, we may get extremely valuable information from students, parents, faculty, and staff. It’s what leads to SROs in many cases being able to head off bad situations before they happen.
The BEST of BOTH WORLDS

Need the convenience of wireless, and the real-time communication of online access control?

Then the new IN100 Aperio® wireless lock is for you.

- Remote lock/unlock in less than 10 seconds
- Streamlined design with your choice of black or white reader, 50+ levers and 14 finishes
- Simultaneous support for HID Mobile Access® and multiple credential types, including smart cards and Prox
- Seamless integration with a broad range of access control platforms

Available from ASSA ABLOY Group brands:
CORBIN RUSSWIN | SARGENT

IntelligentOpenings.com/IN100
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


For product info #30 securitymgmt.hotims.com