SECURITY MANAGEMENT
AUGUST 2017
A PUBLICATION OF ASIS INTERNATIONAL

Issue & Beyond

Embassies
Governments struggle to protect embassy facilities.

Cybercrime Trends
Ransomware and cyber espionage top the list of threats.

14 HARASSMENT
42 PHYSICAL SECURITY
48 HOUSES OF WORSHIP

34 DRUG DIVERSION
Monarch Plus
Lock-In Key Control System

1. Each key electro-mechanically locked in place
2. Restrict access by user, key, date & time and cabinet, etc. (segregation of duties)
3. Digital image capture with every transaction
4. Email, SMS, audible and visual alerts and alarms
5. Networking, integration, API
6. The only lock-in system with emergency key release capability
7. Comprehensive reports and custom report builder is included
8. Highest key storage density (280 per cabinet) with industry leading expansion capacity (up to 15,000 keys)
9. Easy to use web browser based administration with full size 15” touch screen
10. US based 24-hour customer care

GS-07f-0771x

For product info #1 securitymgmt.hotims.com

KeuperSystems.com • KeuperStore.com
1-888-285-3361
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.

WinDSX

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

DSX Access Systems, Inc.

www.dsxinc.com

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


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

See us at ASIS Booth 3715

For product info #2 securitymgmt.hotims.com
SIMPLY SUPERIOR.

Our WEBS® Tower with IP Call Station is a platform of technology that outperforms the competition, and so do we.

+ Integrates with major technology partners
+ Mass notification software-compatible
+ Products installed in over 40 countries
+ Widest array of security and life safety products

TALKAPHONE.COM | 773-539-1100
“We take great pride in it, and we’ve actually become really good at reuniting lost property with its owner.”

Kenneth Dixon, director of safety and security at the Jacob K. Javits Convention Center in New York City, on the relationship between a good security posture and a spike in lost and found items. PAGE 46

Never allow staff or volunteers to work alone, ensure opening and closing procedures are in place, make sure all doors and windows have functioning locks, and maintain an inventory of expensive or easily stolen items.

A few of the 34 steps recommended by the ASIS International Houses of Worship Committee to improve security at little or no cost. PAGE 51

“The they are certainly not as helpful as people would want.”

Brian Lee, practice leader at CEB, on whether companies should depend on sexual harassment hotlines. PAGE 15

$80M
The fine paid by Walgreens for violating the U.S. Controlled Substances Act and unwittingly letting controlled drugs enter the black market. PAGE 38

50,500
The number of local employees working at U.S. embassies around the world, compared to 14,000 U.S. employees. PAGE 21

200%
The growth in the number of Certified Protection Professionals® in Kenya from 2015 to 2017. PAGE 56
It’s not just any security camera, #ItsAHikvision

www.hikvision.com

For product info #4 securitymgmt.hotims.com
34
THE DIRTY SECRET OF DRUG DIVERSION
Healthcare workers are stealing opiates from their workplaces, and it’s up to security professionals to identify, investigate, and keep track of offenders.
By Lilly Chapa

PHYSICAL SECURITY
JAVITS EMBRACES HIGH-TECH HOSPITALITY
The Jacob K. Javits Convention Center in New York City recently enhanced its approach to safety and security, decreasing crime and increasing customer service.
By Holly Gilbert Stowell

HOUSES OF WORSHIP
SECURING SACRED SPACES
Recent attacks at houses of worship around the globe challenge security professionals with protecting parishioners and facilities on a limited budget.
By Paula L. Ratliff

HOUSES OF WORSHIP
HOW TO PROTECT YOUR HOUSE OF WORSHIP
The ASIS International Cultural Properties Council created a guide that includes simple steps to help houses of worship bolster security.
By Megan Gates
FIBER SOLUTIONS

Altronix’s new NetWay Spectrum series takes fiber and power to a new level. Indoor and outdoor models include hardened Ethernet PoE switches and multi-port media converters with or without integral power. Units can be deployed with conventional single or multi-mode fiber...or composite cable which combines fiber with copper to simultaneously deliver power and data. Go further – with NetWay Spectrum from Altronix.

MADE IN THE U.S.A. & BACKED BY A LIFETIME WARRANTY

VISIT US AT ASIS - BOOTH #2823

altronix.com – info@altronix.com
New online this month: a study on security for houses of worship, a white paper on sexual harassment prevention, and reports on hate crimes.

Using data to find truth.

The challenges of embassy security.

A government contractor grapples with worker authentication.

Ransomware and other cyber trends.

The numbers behind the increase in U.S. terrorism arrests.
HARASSMENT
Sexual harassment should be considered a workplace violence issue, and those in the security industry should gain a greater awareness of the prevalence of this crime, the ASIS Crime and Loss Prevention Council states in the white paper Sexual Victimization.

HATE CRIMES
There were a reported 1,402 victims of religious hate crimes in 2015, and those crimes primarily targeted Jews, according to the FBI’s Uniform Crime Reports: Hate Crime Statistics 2016. Since early January 2017, more than 140 bomb threats have been phoned and emailed to 110 Jewish community institutions, according to the Anti-Defamation League.

EMBASSY SECURITY
A new approach to foreign embassy facility design aims to make the buildings more inviting and adaptable to unique geographic challenges, according to a new U.S. Government Accountability Office report.

BACKGROUND CHECKS
The U.S. Federal Trade Commission issued new advice for employers who conduct background checks on prospective employees.

INSIDER THREATS
A recent report finds that 45 percent of agencies were targets of an insider threat in the past year. Learn more about embedded threats in Inside Job: The Sequel.

GLOBAL RISK
Global risk has entered into a new era, according to The Global Risks Report 2017 issued by the World Economic Forum.

NEGLIGENCE
An employer can be sued for negligence by an employee who is injured on the job, even when the injuries are the result of a dispute that began outside the workplace, a Louisiana appellate court ruled.

To help houses of worship improve their security posture on a limited budget, the ASIS Cultural Properties Council created the Security Risk Analysis Guide specifically for religious institutions. The guide is designed to share a modified version of the Security Risk Analysis process so that house of worship leaders will be able to identify critical assets and assess threats and hazards. Council member Jim McGuffey, CPP, PCI, PSP, who was instrumental in the guide’s creation, sat down with Security Management to discuss how it can be used to protect houses of worship in a recent podcast.

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

Setting boundaries makes access in life smart and secure.

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

For product info #6 securitymgmt.hotims.com See us at ASIS Booth 2321

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

Set your boundaries.
n 1854, a cholera outbreak ravaged the SoHo district of London, killing more than 600 people. The city had weathered cholera epidemics in 1832 and 1849, but 1854 was different because of Dr. John Snow. The British doctor sought the source of the cholera through a radical experiment—the collection of data.

Snow documented every instance of the disease, literally mapping the outbreak and discovering that at the center of the illness was a single water pump. The finding paved the way for a theory that sickness was caused by germs rather than bad air.

Seth Stephens-Davidowitz cites Snow as a pioneer and his study as one of the earliest uses of Big Data. In his new book, Everybody Lies: Big Data, New Data, and What the Internet Reveals About Who We Really Are, Stephens-Davidowitz takes data analysis a step further and uses search results from Google and other Internet platforms to uncover the disparity between what people say and what people do.

Without Internet data, social scientists have traditionally relied on self-reported information. But, Stephens-Davidowitz notes, people lie about their innermost feelings. “Certain online sources get people to admit things they would not admit anywhere else. They serve as a digital truth serum,” he writes.

And that truth is not always pretty. Stephens-Davidowitz learned that a virulent, widespread racism exists in the midwestern United States; that the number of searches for “voting” in October can predict turnout for elections in November; and that child abuse reporting rates went down while actual abuse rose.

Our interaction with the Internet and with social media is also leading to new types of information that provides insight into society’s fears and anxieties. For example, Internet searches reveal that parents are excited about the intellectual prowess of their sons but concerned about the appearance of their daughters.

While these insights are revealing, Stephens-Davidowitz warns about putting too much stock in numbers alone. “A special sauce is often necessary to help Big Data work best: the judgment of humans and small surveys, what we might call small data.”

This small data manifests in human decisions based on expertise in a certain subject or simply on experience. Both types of data are critical in solving a problem explored in this month’s cover story. In “The Dirty Secret of Drug Diversion,” Assistant Editor Lilly Chapa talks to experts who crunch numbers to determine which medical facilities might be victims of diversion—instances when controlled substances are intercepted before they reach the patient. However, investigators are on hand to explore the human element as well, noting that drug diverters—who are often addicts—need help and are relieved to be caught.
It’s not just about protecting your business from disaster –

It’s about monitoring those side entries, keeping up with regulations and replacing that worn wiring by the break room.

When you partner with Red Hawk we don’t just provide the best solution – we provide the best solution for you. Our experienced team takes the time to understand your business and deliver the latest in technology with good-old-fashioned hands-on customer service. We won’t sell you anything you don’t need and will always be here when you need us. RedHawkUS.com | 888-991-0117

For product info #7 securitymgmt.hotims.com
Although their views may differ regarding the value of different prevention components, many security professionals seem united on a core issue: harassment is a serious workplace issue both in the United States and around the world, and it is one that deserves more attention and more prevention programs.

“One unfortunately, most people do not consider sexual harassment as a workplace violence issue, but this is a serious mistake,” the ASIS International Crime and Loss Prevention Council said in a white paper, Sexual Victimization, issued last year. “...It is imperative that we in the security industry each gain a greater awareness of the prevalence of this crime.”

One preventative measure that has attracted recent attention is the use of company phone hotlines for anonymously reporting incidents of harassment. The harassment hotline concept came into focus after intense media coverage of harassment allegations made against prominent Fox News broadcaster Bill O’Reilly by several female coworkers and program guests. The allegations eventually led Fox News to terminate O’Reilly’s contract in April 2017.

O’Reilly said that the allegations were spurious, and he maintained that no complaints against him had ever been reported on the company’s harassment hotline. But some experts say that a lack of hotline calls is never surprising and does not accurately reflect frequency of incidents.

Brian Lee, practice leader at CEB (now part of Gartner), a consultancy...
specializing in workplace incidents, says that, on the one hand, hotlines or “helplines” can be a valid component of an overall safe workplace programs. “But they are certainly not as helpful as people would want,” he adds. In part, this is because many companies employ a hotline for legal reasons, but do not publicize the actual phone number, which is sometimes embedded in a corporate policy handbook. “If you poll their employees, many have no idea what the number is, or how to get it,” Lee explains.

Another reason for low hotline use is that some employees suspect that the hotline isn’t truly anonymous, even if it is billed as such. Media reports of cases like the Wells Fargo fake account scandal of 2016, in which supposedly anonymous reports were still used for retaliation against whistleblowers, “have a chilling effect” on hotline use, Lee says.

In addition, the hotline can feel too impersonal, like taking a complaint and “dropping it in a box somewhere,” says Stephen Hollowell, CPP, vice chair of the ASIS International Crime and Loss Prevention Council and a member of the ASIS International Healthcare Council. Hollowell helped prepare the Sexual Victimization white paper.

A recent CEB global study on workplace misconduct seems to support Hollowell’s view. Only about 7 percent of respondents reported that they had used a hotline to file a complaint, compared with 68 percent who reported the incident to their direct managers. “The use of helplines tends to be much lower than people think,” Lee says. “It is far from the most popular way of reporting.”

But unlike hotlines, other components of workplace safety programs have been shown to be effective, says Hollowell, who is an advocate for treating harassment with the same seriousness as other incidents of workplace violence. One such component is harassment training for all employees, which starts with orientation but does not end there.

“You don’t just do it one time in orientation and then forget about it,” he says. Companies should provide periodic updates. Hollowell was involved in one organization that used the company’s weekly internal magazine to remind people that they should not hesitate to speak to their manager or call the firm’s helpline to report an incident.

Experts often say that there are two main reasons why many harassment incidents go unreported: fear of retaliation, and previous demonstrated inaction by the company. Given this, a rigorous prevention program should address both these concerns, Hollowell says.

To do this, managers should make clear that the company’s workplace is one free of harassment and violence, and that this ethos is reflected in the procedures for reporting complaints. Hollowell uses his own program as an example: if a complaint is reported to a supervisor and the supervisor does not take action, the employee is encouraged to take the complaint to the supervisor’s supervisor, or to another department like human resources or security. “We make it very clear,” he says. Additional action will take place immediately, if the complaint is valid, he adds.

Another point that should be made clear is that whistleblowers are protected. If an employee is penalized by a manager for filing a complaint in any way—such as by being assigned extra work or by having privileges taken away—“we make it very clear you need to come forward and make us aware of it,” Hollowell explains. “That could lead to [the manager’s] termination.”

However, it is also a workplace reality that, occasionally, false harassment allegations are made. This is one reason Hollowell does not like anonymous reporting—it makes it easier for disgruntled employees to target certain people, such as a coworker or supervisor they hold a grudge against, with false complaints.

**Most people do not consider sexual harassment as a workplace violence issue, but this is a serious mistake.**

---

While marijuana positivity within the general U.S. workforce increased between 2015 and 2016, the rate of increase in states that have legalized the recreational use of the drug was even higher.

<table>
<thead>
<tr>
<th>State</th>
<th>Urine Positivity Rates for Marijuana (%)</th>
<th>2015</th>
<th>2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>General U.S.</td>
<td></td>
<td></td>
<td>+4%</td>
</tr>
<tr>
<td>Washington</td>
<td></td>
<td></td>
<td>+19%</td>
</tr>
<tr>
<td>Colorado</td>
<td></td>
<td></td>
<td>+11%</td>
</tr>
</tbody>
</table>

**SOURCE:** Quest Diagnostics Drug Testing Index, Quest Diagnostics, May 2017
GLOBAL RISK

Given the possibility of false claims, impartial investigations are crucial, Hollowell says. Investigators take a “just the facts” approach, sticking to exactly what happened, and following wherever the facts lead. “If you start assuming, you’re not following the facts,” he says. Finally, keeping people informed of procedures and policies is crucial. “Transparency really is the watchword,” he adds.

For many years, harassment prevention programs would emphasize that company leaders needed to set a good example in their behavior, because the tone at the top was key. “But increasingly, that is just table stakes now,” Lee says. More firms are realizing that a coworker’s behavior is just as important as a manager’s behavior. “Employees are far more influenced by what they see around them than what they see at the top,” he adds.

Indeed, that philosophy is at the heart of a recommendation made recently by the U.S. Equal Employment Opportunity Commission (EEOC) Select Task Force on the Study of Harassment in the Workplace. In a report issued last year, the task force co-chairs recommended exploring an “It’s On Us” campaign for U.S. workplaces.

“It’s On Us” is a social movement first created in 2014 by the White House to prevent sexual assault on college campuses. The campaign urged everyone on campus to be an active part of the solution, not passive observers. Launching a similar campaign in workplaces across the country would be “an audacious goal,” and not easy, the EEOC task force concedes.

“But doing so would transform the problem of workplace harassment from being about target, harassers, and legal compliance,” the task force argues, “and make it one in which coworkers, supervisors, clients, and customers all have roles to play in stopping harassment.”

A SHIFT IN GLOBAL RISK

THE QUEST to better understand the sources of global risk, and the effect those sources of risk may have on security, is of continuing importance to many practitioners of enterprise security risk management (ESRM).

And now, global risk has entered into a new era, with people around the world facing more political instability, more economic challenges, and the prospect that more national policy decision making will be driven by emotion rather than reason, a new study finds.

The study, The Global Risks Report 2017, is the 12th edition of one of the flagship reports issued annually by the World Economic Forum. The report posits that the new era of risk began last year, a watershed time for instability when increasing economic populism and political polarization came to a head in unexpected election results and the disquieting rise of former fringe nationalist parties.

“The year 2016 saw profound shifts in the way we view global risks. Societal polarization, income inequality, and the inward orientation of countries are spilling over into real-world politics,” reads the study, which was conducted with the help of academic advisors from the University of Oxford,
EVERY CUSTOMER’S situation is unique. That’s why custom solutions are a big part of what we offer. We relish the opportunity to think outside the box. Whether you need guidance with a challenging installation, are inquiring about training or want help making a hardware decision, knowledgeable technicians, with nearly 50 years combined experience, are eager to help you think through your specific issues. Just call 800-729-3839.

Advantex line of exit devices & electrical functions
Super heavy duty low energy ADA operator
Automatically operated door easykits
Weatherized delayed egress easykits
Tailgate detection
the National University of Singapore, and the Wharton Risk Management and Decision Processes Center at the University of Pennsylvania.

The report argues that five “gravity centers” will shape global risks moving forward, and it sketches out the challenges that will result from each of them. First, continued slow economic growth, in tandem with high debt and demographic changes, will create an environment conducive to financial crises and growing inequality. Second, corruption and unequal distribution of the benefits of growth will convince a growing number of people that the current economic model is not working for them.

Third, the transition towards a more multipolar world order will put a greater strain on global cooperation. Fourth, the fourth industrial revolution—Internet-connected technologies—will continue to transform societies, their economies, and their ways of doing business. Fifth, more people will seek to reassert identities that have been blurred by globalization, so decision making and election choices will be increasingly influenced by emotions rather than reason.

There is no one silver bullet solution to these challenges. But the report argues that the problems “create the opportunity to address global risks and the trends that drive them.” In that spirit, the study sets out several actions that leaders should take to push forward in creating a more secure and stable world.

The report argues that political leaders need a deeper commitment to fostering inclusive development and equitable growth, on both a national and global scale, instead of allowing increasing economic inequality to further destabilize societies. And while the report praises innovation, it also argues for better management of technological change, so the growth of new uses for technology causes less disruption and leaves fewer behind.

Finally, at a time when multinational institutions like the European Union and NATO are under unprecedented attack, the report calls on leaders to redouble efforts to protect and strengthen systems of global collaboration. Destabilizing international events—which range from migration flows created by the Syrian war to major weather events that impact several countries to a potential global water crisis—all warrant more cooperation between countries.

“It is ever clearer,” the report argues, “how important global cooperation is on the interconnections that shape the risk landscape.”
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.

**VERSATILE SOLUTIONS FOR ANY SIZE PROJECT**

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.

www.hikvision.com

For product info #10 securitymgmt.hotims.com

ASIS 17
BOOTH 
#3703

Stainless Steel
Bi-Spectrum Thermal PTZ
Ultra-Wide Panoramic
Multi-Sensor
Black Housing
That’s why Afghans were shocked by what occurred in Kabul’s Green Zone just before 8:30 a.m. on May 31, 2017, when a truck exploded in the center of the zone, killing at least 80 people and injuring upwards of 500. The bomb destroyed buildings and demolished cars in a several-block radius. Although the blast took place in a diplomatic area of the city, it was mostly Afghan civilians who were killed, including guards for several of the embassies in the zone.

The circumstances surrounding the massive blast in the Green Zone create a macabre juxtaposition. Officials have yet to figure out how a vehicle carrying enough explosives to create a 15-foot crater was able to enter the heavily-fortified area surrounded by 10-foot high blast walls. On the other hand, security measures were so heavy that security checkpoints snarled traffic, resulting in the high number of civilian casualties. Nobody has claimed responsibility for the attack, and investigators reportedly believe that the vehicle carrying the explosives was a waste collection truck, which is perhaps how it was allowed through checkpoints.

But the attack has left diplomatic officials trying to find the balance between fortress-like security measures and fostering a more open and transparent relationship with the host country, both physically and strategically.

The 1998 bombings of American embassies in Nairobi, Kenya, and Dar es Salaam, Tanzania, which killed more than 220 people, and the 2012 Benghazi, Libya, attack that...
Once a post is designated as high-threat, then other facets come into play in terms of additional funding, security preparedness, or staffing.

left four dead, all drastically shifted the way the U.S. Department of State approaches embassy security.

The United States has more than 300 embassies, consulates, and diplomatic missions around the world—the most of any country. After the 1998 attacks, the State Department determined that more than half of those embassies needed to be completely replaced to meet security requirements. The State Department then created a standard embassy layout that was used all around the world.

Since then, more than 30,000 diplomatic staff have been moved into hardened facilities that meet heightened physical security standards, including a 100-foot setback from the site’s perimeter, anticlimb walls and antiram barriers, hardened building exteriors, and controlled access to the compounds.

American embassies and consulates have different threat levels based on factors such as the overall security landscape and host country crime rates, explains Robert Baggett, CPP, PCI, PSP, a former Diplomatic Security Service (DSS) special agent for the State Department and current cochair of the ASIS International Academic and Training Programs Council.

Baggett led various Regional Security Office portfolios, such as local embassy guard forces and teams that identified security threats for U.S. missions in China, Iraq, and Vietnam. He tells Security Management that the risk ratings for individual embassies and consulates are assessed on a constant basis in light of any changes that may alter security posture.

“Once a post is designated as high-threat, then other facets come into play in terms of additional funding, security preparedness, or staffing,” Baggett notes.

Currently, 78 embassies are ranked as high-threat, high-risk posts, which means that all mission chiefs must receive Foreign Affairs Counter Threat (FACT) training that focuses on topics such as emergency response, first aid, offensive driving, and evacuations.

“FACT training provides familiarization on what can be expected while serving at these posts, thereby improving one’s situational awareness and empowering them to work more effectively and safely in this type of high-threat environment,” Baggett explains.

Approximately 14,000 American foreign service officers and specialists work at U.S. missions around the world. These Americans are bolstered by more than 50,500 locally employed staff, who are typically citizens of the host country where the U.S. mission is located.

Some high-threat posts, such as the U.S. Embassy in Baghdad, are also staffed by third-country national security forces—many of which hail from South America or Africa—that are employed under American-owned company security contracts. These guards often supplement the mission’s security force that comprises DSS special agents, special protective specialists, American Biosecurity: Institutional Biosafety

EDITED BY CAROLE BASKIN AND ALAN P. ZELICOFF. Academic Press; Elsevier.com; 270 pages; $79.95.

CAROLE BASKIN AND ALAN ZELICOFF of the Institute of Biosafety at St. Louis University bring together a distinguished list of contributors to deliver an outstanding overview of biosafety and biosecurity in Ensuring National Biosecurity: Institutional Biosafety Committees. Beginning with a historical perspective, it thoroughly examines the operational and regulatory challenges of biosafety and biosecurity within biomedical research.

Thirteen well-conceived chapters introduce the reader to the complexities of regulatory requirements imposed by the government, the institutional roles and responsibilities for biosafety and biosecurity, and best practices to ensure successful management of an institution’s biomedical research mission.

The content flows easily from the early beginnings of biosecurity to the present day and what lies ahead. Every contributor shares expertise and professional knowledge in an easily understandable manner. For example, Ryan Burnette and Nancy Connell characterize the importance of expanding the expertise of the Institutional Biosafety Committee to embrace biosecurity with the delivery of key bio and physical security training topics.

This book is recommended for everyone working in biosecurity and biosafety positions. It should be in bioresearch libraries, and managers should promote it as required reading. The book is that good.
civilian security force operators, and other personnel.

“In any embassy or consulate, you’re going to have to heavily rely on foreign service national staff to support operations, including political and economic sections, human resources, general services, and especially the local guard force,” Baggett notes.

“These individuals not only speak the native language, they are truly vital to the mission where they are familiar with host country laws, policies, and customs. They serve as an embassy or consulate’s foundation to conduct U.S. foreign policy overseas, have cultivated host country government contacts, and possess the historical knowledge of the mission, which is truly priceless since foreign service officers and specialists typically rotate assignments every one to three years.”

Maintaining effective communication between a U.S. mission and the host country’s government, regional offices, and local law enforcement is imperative for strengthening the embassy or consulate’s security, as well as the bilateral relationship with the host country, Baggett explains.

“We’d see plainclothes local law enforcement officers in front of our embassy and wonder why, and two hours later there’s a big protest.”

“Many times we would hear information through our foreign service national staff or established professional contacts, but we weren’t hearing it through official channels,” he says. “Other times we’d see plainclothes local law enforcement officers in front of our embassy and wonder why, and two hours later there’s a big protest that we didn’t know anything about. Being able to establish and develop professional local law enforcement relationships is paramount in receiving such potential threat information directly from the field rather than waiting on obtaining information from official channels.”

Strengthening the strategic relationship between embassy personnel and the host country goes beyond information sharing and includes the physical presence of the embassy.

Almost 15 years after the 1998 Africa bombings and subsequent implementation of standardized, high-security embassy construction, there was a push to allow more flexibility in embassy design while maintaining certain security standards. Dubbed the Excellence Approach, it gave the State Department’s Bureau of Overseas Building Operations (OBO) the ability to contract directly with individual design firms to “improve embassies’ appearance in representing the United States, functionality, quality, and operating costs,” according to a new U.S. Government Accountability Office (GAO) report.

“The whole idea of building these new embassies is to get our people into safer and more secure facilities,” says Michael Courts, director of international affairs and trade at GAO. “State Department officials believed they would have greater design control because they could customize the designs to the locations where they were being built.”

This is important because the previous standard design did not allow for embassy customization based on the region, space availability, or climate, lowering the flexibility and functionality when it came to building.
Quantum Secure’s SAFE software suite streamlines and automates secure identity management, compliance and operational analytics across multiple sites and systems in a single, fully interoperable platform—allowing you real time visibility into your entire security infrastructure. Already the leader in physical identity and access management software, we are now partnered with HID Global, meaning your investment in best-in-class technology can be made with confidence. Find out how to lower your risk profile and operational costs by visiting quantumsecure.com/know.
new embassies, Courts tells Security Management.

Instead, the Excellence Approach requires OBO and design firms to work together to make sure certain security standards are met at each unique facility while emphasizing location and design that will further the diplomatic mission.

The new policy emphasizes considering American values in promoting a sense of openness, accessibility, and transparency through location; proximity to other embassies and host country facilities; and a location that is connected to public transportation and infrastructure, according to the GAO report.

“How you implement those standards can change depending on what sort of site you’re building on, the density of the surrounding urban area—that is going to be somewhat challenging for the State Department because they are going to have to try to adapt to each context as they build their embassies,” Courts notes.

Keith Bobrosky, vice president of sales at Delta Scientific, agrees. “It’s subtle to an outsider, but from what we’ve seen it’s very important,” he explains. “For years they had standard embassies—all one design and arguably very militaristic and not very inviting. Now the embassy needs to mimic the surrounding environment aesthetically a lot more, so we still want to keep the utmost in vehicle barrier and perimeter security, but aesthetics play a far more important part when we’re a guest in some of these other countries.”

Bobrosky has been involved with the implementation of barrier protection at hundreds of overseas building operations for the State Department and the FBI. Despite the design changes, State has been relatively consistent in what it requires for perimeter security at its embassies, he says, but the technology itself is continuously changing to improve longevity and environmental impact.

For example, Bobrosky notes that embassies have always used hydraulic barrier systems—which rely on hydraulic fluids to operate their motion—but some newer builds have started turning to electromechanical barriers because they are more environmentally friendly.

“We’ve seen a paradigm shift from hydraulic to a more politically correct product—electromechanical—because there’s no fluid that could leak in these other countries where we’re really a guest,” Bobrosky says. “Some of them are very environmentally aware where they do not want to have any hydraulic fluid possibly hitting the soil.”

This fits in line with the shift Bobrosky has seen as OBO has implemented the Excellence Approach—placing emphasis on how the embassy can fit in to its surroundings while being respectful of the host country.

“Sometimes these fences are dozens of years old and the barriers we put in have to match,” he notes. “Or the cobblestone street in front of the embassy may be hundreds of years old, so when
It’s hard to have the best of both safety and security, because you have to take from one to get more of the other.

we install the bollards we have to meticulously move each cobblestone and replace it in the same manner.”

The customized embassy approach has been around for five years, but it’s unclear what effect the new, individualized designs have on security, the GAO report notes. OBO employees are divided on whether the Excellence Approach has improved the construction programs—37 percent agreed that it had, 34 percent disagreed, and the remainder were not sure, according to the GAO report. OBO has not defined performance measures to quantify the success of the new approach, the report explains.

“Without performance measures specific to Excellence and sufficient systems to collect and analyze relevant data, OBO will not be able to demonstrate whether the performance of Excellence projects over time justifies the increased emphasis on and investment in their designs,” according to the report.

Meanwhile, physical security providers such as Bobrosky continue to see small shifts in operations that make embassies more inviting. He notes that all barrier systems include in-ground vehicle detection, which prevents the accidental deployment of a barrier on an innocent party, such as a gate closing on a cleared vehicle.

“We’ve seen some changes in the last few years in this argument between safety and security,” Bobrosky explains.

Some embassies are requiring infrared sensors near their barriers, which are more accurate and would keep barriers or gates from being accidentally deployed on pedestrians.

“It’s a little less secure because there’s more of a chance for someone to keep the gate from operating as it should, but it’s a lot safer for pedestrians and vehicles alike,” he says. “It’s hard to have the best of both safety and security, because you have to take from one to get more of the other.”

To view the report mentioned in this article, visit SM Online.
“Our team performs this work all over the world; basically wherever the ships break, we go,” says Kirk Boettner, director of the technical flushing division at SBSBTC. This includes Japan, Bahrain, Spain, Diego Garcia, and parts of the United States and its territories, such as Florida, Guam, Hawaii, Virginia, and Puget Sound regions.

SBSBTC also has one of the largest tank-cleaning operations in San Diego, and provides non-skid surfaces for military vessels’ flight decks, cargo decks, and more.

As a U.S. government contractor, SBSBTC must comply with an array of requirements, including security vetting for personnel who need access to the multiple naval installations and vessels where the company does its work.

“To work on the naval bases, as well as the private shipyards, all of our people have to be drug tested and undergo background checks to make sure they don’t have any felonies, or things of that nature,” Boettner says. He adds that the U.S. government is continually increasing its security requirements for contractors, particularly in the realm of cybersecurity. Many of those requirements are mandated by the U.S. National Institute of Standards and Technology (NIST).

“The government in general has raised its bar for what their own people have to do to gain access to information and to gain access to computer networks,” he says, citing recent cyberattacks linked to nation-states like North Korea and China. He acknowledges that contractors are the weakest link in terms of letting hackers access government information.
To address this issue and to help keep hackers and cyberterrorists from accessing controlled unclassified information (CUI), the U.S. Department of Defense (DoD) requires all of its contractors to be compliant with the NIST 800-171 mandate by the end of December 2017.

One of the key provisions in that framework is the use of multifactor authentication—a PIN, biometric, or smartcard will be needed, in addition to a username and password, to log onto computer terminals and into certain government websites.

For SBSBTC, this meant the company had to develop a policy differentiating between who had access to CUI and who did not. Those with access would need the multifactor authentication. Separating the two types of employees can be a challenging task for a company like SBSBTC, where worker numbers widely vary.

“In our industry, with the workload spikes and turnover, we could be 400 employees in one month and 70 the next,” Boettner says. “So trying to maintain and manage that policy would be extremely difficult, and require lots of oversight to ensure that we stay in compliance with NIST.”

That’s the company’s relationship with SureID, an identity-solutions provider, came in. SBSBTC has been a SureID customer since 2011 when it adopted the RAPIDGate program to gain streamlined access to naval installations.

The RAPIDGate Program is SureID’s authentication solution, used by the DoD and other U.S. government agencies, that allows physical access to military bases and other facilities in a quick, efficient way.

At the gate to the Navy installations, armed DoD personnel check the RAPIDGate credential, which has the cardholder’s photo and a barcode. DoD employees use handheld scanners to read the barcode associated with the RAPIDGate Program credential.

The card also provides multifactor authentication for logging onto computer terminals because it complies with NIST’s Personal Identification Verification standard. That framework verifies the “identity of individuals seeking physical access to federally controlled government facilities and logical access to government information systems,” according to NIST’s website.

In the end, SBSBTC decided it would be more efficient to certify all of its employees under the new standard, and provide multifactor authentication for the non-RAPIDGate personnel through the SureID Certified PIV-I (Personal Identity Verification Interoperable credential).
“It was more beneficial to just have our overhead and general administrative staff on the same level as our RAPIDGate personnel, and just say the whole company has access to CUI,” Boettner explains.

The RAPIDGate card already meets all the protection levels and limits for the requirements in the NIST 800-171 program. “For people who already have RAPIDGate, which is most of the company, it serves both functions,” he says. “It gets them physically onto a location, as well as also covering the two-factor authentication; it’s a two-in-one card.”

For staff not requiring physical access, the SureID Certified PIV-I credential provides the same access except for admission to military locations and vessels. “A PIV-I credential is provisioned with digital certificates, photo, and fingerprint and among the most effective ways of addressing security vulnerabilities both online and on-premise,” a white paper from SureID explains. “A would-be hacker would have to infiltrate a given Public Key Infrastructure (PKI), and hack each individual card where the information is stored. Doing so would be practically impossible for a cyber espionage group physically located on the other side of the world.”

A SureID customer service representative came to SBSBTC in March 2017 to fingerprint and photograph the staff who didn’t have the RAPIDGate card to sign them up for the SureID PIV-I credential. “They set up a registration station at our facility here and we were able to process through all of our employees over two visits,” Boettner notes. SureID maintains the database for both the RAPIDGate and PIV-I cards.

When logging onto their computers, SBSBTC employees insert their SureID PIV-I or RAPIDGate card into a reader and enter their username and password. The cards are valid for a three-year period and can be renewed electronically.

Boettner adds that there is much more to meeting the NIST 800-171 requirement than credentialing employees for multifactor authentication. “There’s a myriad of other changes we had to go through,” he says. “We had to get a whole new firewall, brand new hardware in our network closet, we had to switch servers; we had to do all these different things to be compliant.”

He notes that the SureID PIV-I credential, however, has made a huge difference moving toward meeting the deadline. “We’ve advanced very far down the requirement ladder because of them,” he says. “Probably more than a third of the work...we knocked out just by working with SureID.”

U.S. Federal Agencies and Insider Threats

In the last year...

- 45% of agencies have been a target of an insider threat
- 1 in 3 have lost data to an insider incident

Yet less than half of agencies use key prevention technologies:

- 48% Data Loss Prevention
- 46% Two-Factor Authentication
- 40% Endpoint Encryption

FOR MORE INFORMATION: Aaron Cohen, acohen@sureid.com, www.sureid.com, 503.924.5297

ASIS

Calling for TECHNICAL COMMITTEE PARTICIPATION for the ACTIVE ASSAILANT SUPPLEMENT STANDARD

Deadline for applications: AUGUST 25

asisonline.org/standards

With innovative wide-area imaging solutions for both IP and analog infrastructure, Dahua’s multi-sensor cameras include 6, 8 or 16MP options. IP models offer Starlight ultra-low-light technology, exceptional WDR, and Dahua’s exclusive Smart H.265+ compression, which saves up to 80% on bandwidth and storage over standard H.264.
DATA BREACH TRENDS

RANSOMWARE AND CYBER ESPIONAGE WERE RESPONSIBLE FOR MANY OF 2016’S DATA BREACHES. THESE EXPERTS SAY COMPANIES CAN DO MORE TO PREVENT THESE ATTACKS. BY MEGAN GATES

EARLY IN THE AFTERNOON on May 12, 2017, the United Kingdom’s National Health Service (NHS) confirmed that it had been hit by a massive ransomware attack that was spreading its way around the globe.

“This attack was not specifically targeted at the NHS and is affecting organizations from across a range of sectors,” the NHS said in a statement, confirming that at the time it was released, 16 of its organizations had been affected by WannaCry ransomware.

MalwareTech, a cybersecurity blogger and researcher, saw that NHS had been hit by the attack at approximately 2:30 p.m. That fact tipped him off “that this was something big,” MalwareTech wrote in a blog post.

To find out what was happening, he got a sample of the malware, ran an analysis, and registered an unregistered domain for $10.69 that the malware had queried.

“Now one thing that’s important to note is the actual registration of the domain was not on a whim,” MalwareTech explained. “My job is to look for ways we can track and potentially stop botnets (and other kinds of malware), so I’m always on the lookout to pick up unregistered malware control server domains.”

MalwareTech’s efforts, along with an emergency patch released by Microsoft for Windows XP (which hasn’t been supported since 2014), stopped WannaCry. But that doesn’t mean they will be so lucky in the future as ransomware and other types of crimeware become more prevalent.
In the recently released Verizon 2017 Data Breach Investigations Report, Verizon analyzed data from 65 organizations and found that 88 percent of breaches fell into nine patterns identified in 2014: crimeware, cyber espionage, denial of service, insider and privilege misuse, miscellaneous errors, payment card skimmers, point-of-sale intrusions, physical theft and loss, and Web application attacks.

These attacks are successful, in part, because most companies erroneously believe they won’t be targeted, wrongly think they have the basics of cybersecurity covered, are failing to set strong password requirements, and are relying on how they have always done things—as opposed to being innovative and proactive.

“While attackers are using new tactics and tricks, their overall strategies remain relatively unchanged,” the Verizon report explains.

“Understanding them is critical to knowing how to defend your organization from cyberattacks.”

The report also finds that it’s not just major companies being targeted. Instead, 61 percent of breaches in the report affected businesses with fewer than 1,000 employees.

Manufacturing, healthcare, and the financial services sectors were major targets for data breaches in 2016. But Verizon Global Head of Cybersecurity Strategy and Marketing John Loveland said that companies should not be distracted by that fact.

“I would say put a big emphasis on ‘industries most at risk,’ but that can be unhelpful because I think it may distract from the idea that every organization is a potential target,” Loveland said in a Verizon podcast interview.

Bryan Sartin, Verizon global security services executive director, echoed Loveland’s comments, and said that no organization should rest on its laurels.

Though they may be in denial, organizations are going to be targeted, Sartin explained on the podcast. “Whether it’s design plans, medical records, or good, old-fashioned payment card details—somebody, somewhere will see it as their meal ticket and as an opportunity to get a hold of that, exploit vulnerabilities, find that data, get it out, exfiltrate it, and try to convert it into cash. Most cybercriminals aren’t that fussy about who they steal from.”

Ransomware. One of the unchanged strategies that cybercriminals are using is ransomware, which was the twenty-second most common form of malware in 2014. It’s now moved up to the number five position. “For the attacker, holding files for ransom is fast, low risk, and easily monetizable—especially with Bitcoin to collect anonymous payment,” according to the Verizon report.

Due to the success of ransomware in the past several years, criminals have become more innovative about how they use it to turn a profit.

“Criminals introduced time limits after which files would be deleted, ransoms that increased over time, ransoms calculated based on the estimated sensitivity of filenames, and even options to decrypt files for free if the victims became attackers themselves and infected two or more other people,” the Verizon report says.

And while the hackers behind WannaCry didn’t make a great deal of money from the ransomware—CNBC estimated they made about $50,000 in Bitcoin in May—the way the malware spread was concerning for future attacks, says Jonathan Couch, senior vice president of strategy at ThreatQuotient, a threat intelligence platform.

This is because WannaCry spread through an initial infection, such as a malicious email that was opened, but from there operated like a peer-to-peer network, he explains.

“Clients would search for other clients on the network, spreading that
way, rather than having a user spread the ransomware,” Couch says, adding that this is one of the reasons that WannaCry spread so quickly—because it was able to do so on its own.

The ability of ransomware to target an organization, as opposed to an individual, was a major change to ransomware in 2016, and attackers combined this tactic with other strategies to make their efforts even more successful.

“Ransomware campaigns targeting organizations often have additional characteristics, such as credential theft to spread the attack throughout the organization, delayed encryption to infect as many machines as possible before detection, and code that targets corporate servers as well as user systems,” according to the report.

These tactics will likely make future versions of ransomware even more powerful than what has been seen so far, Couch says.

“People are going to improve the peer-to-peer to spread [ransomware] faster, and are going to use more encryption within their code to hinder analysis,” he adds.

Couch also predicts that future models will actually extract data from victims’ systems and encrypt it—rather than encrypting the data on the existing network.

“One of the ways to fight ransomware is to do a backup...so if I have a good backup, I just use that,” Couch says. “If you have taken all my files, now I run the risk of you exposing my information.”

While ransomware is not likely to go away anytime soon, the security industry is stepping up to the challenge to detect ransomware before infections become critical, protect organizations from criminal campaigns, and help rescue ransomed systems without paying cybercriminals.

The industry is doing this by improving endpoint protection and detection of ransomware, sharing threat information with law enforcement agencies and other organizations, and supporting the No More Ransom! Campaign.

Started in July 2016, the campaign now has 57 corporate, association, and public sector members that work to help victims recover their encrypted data without paying ransoms.

“To that end, nomoreransom.org currently hosts 27 decryption tools, which can recover files from a wide range of ransomware families,” according to the report. “No More Ransom! calculates that they have successfully diverted more than $3 million from criminals by offering free decryption tools to thousands of victims around the world.”

Cyber espionage. Another major pattern in 2016 identified by the Verizon report was the increase in the number of attacks linked to state-affiliated actors who may—or may not—have a motive of espionage.

Twenty-one percent of the breaches examined by Verizon in the 2017 report were related to espionage, and the manufacturing sector accounted for 86 percent of the breaches. And of those breaches, 73 percent of perpetrators used a combination of a social engineering attack—such as a phishing attack—to install malware.

“A malicious email is the cyber spy’s favored way in. But this is no smash and grab,” according to the report. “The initial email is typically followed by tactics aimed at blending in, giving the attacker time to collect the data that they need.”

Attackers want to infiltrate their target, find out where its secrets are kept, and then slowly collect them until they are detected—ideally, as long as possible.

“When state-affiliated actors are involved, their operations are targeted attacks, rather than opportunistic,” the report explains. “In other words, the criminals are coming directly for a

### FACT BOX

**WHO’S BEHIND 2016’S BREACHES?**

- **75%** perpetrated by outsiders
- **51%** involved organized criminal groups
- **25%** involved internal actors
- **18%** conducted by state-affiliated actors
- **3%** featured multiple parties
- **2%** involved partners

**SOURCE:** 2017 Verizon Data Breach Incident Report
particular organization with a specific purpose in mind.”

The cyberattacks on French President Emmanuel Macron’s campaign in spring 2017 is a prime example of this tactic.

After Russia’s efforts to influence the U.S. presidential election in 2016, Macron’s team knew it was likely to be targeted by similar efforts to help Russia-friendly candidate Marine Le Pen win. After winning a position in the final round of the election, Macron’s team began to receive sophisticated phishing emails.

Because Macron had limited staff resources, his team decided to create a disinformation campaign to confuse any potential hackers instead of focusing on keeping the hackers out altogether, said Macron’s digital director, Mounir Mahjoubi, in an interview with The New York Times following the election.

Mahjoubi said the team went on the counteroffensive, creating false accounts full of fake content that could be used to trap hackers. This way, once the hackers got into the accounts, they would have to spend precious time determining what content was fake and what was real.

While this was effective in slowing down the hackers and preventing the hack from being completely damaging, it’s not the best defensive approach to take, says Alex Vaystikh, cofounder and chief technology officer of SecBI, a threat detection provider.

“If we look at it from a defensive point of view, it’s a bad approach in terms of defense because the defense has come to the conclusion that there’s nothing it can do to prevent the hack,” Vaystikh explains. “The only way is to confuse the hacker with enough false information that when he gets in, he’ll have to go through certainly a lot of noise. Kind of a denial of service attack on the hackers with information.”

Several companies have taken this same approach to cybersecurity, which Vaystikh says is frustrating because it seems that they have resigned themselves to the fact that hackers are going to get in.

“It’s somewhat frustrating in the world of cybersecurity because it means that we’ve given up... and our only hope is that by the time [the hacker] gets the sensitive information and figures out what it is, it will no longer be that sensitive,” Vaystikh adds.

Instead, companies should be proactive about securing their systems and monitoring them, he argues, echoing suggestions from Verizon’s report.

For instance, Verizon recommends that companies separate their highly sensitive data to allow only those who need access to have access, provide phishing training to all employees, monitor internal networks, and implement data loss prevention controls “to identify and block improper transfers of data by employees.”

According to the Verizon report, “If a username and password is the only barrier to escalating privilege or compromising the next device, you have not done enough to stop these actors.”

Instead, companies should be proactive about securing their systems and monitoring them, he argues, echoing suggestions from Verizon’s report.

For instance, Verizon recommends that companies separate their highly sensitive data to allow only those who need access to have access, provide phishing training to all employees, monitor internal networks, and implement data loss prevention controls “to identify and block improper transfers of data by employees.”

According to the Verizon report, “If a username and password is the only barrier to escalating privilege or compromising the next device, you have not done enough to stop these actors.”
Healthcare workers are stealing opiates from their workplaces, and it’s up to security professionals to identify, investigate, and keep track of offenders.

Controlled substances were going missing at Hennepin County Medical Center (HCMC), and the hospital’s security investigator, William Leon, was determined to get to the bottom of it. So, at 11 p.m. on a Friday, Leon settled in for a night of observation at the Level I trauma center in Minneapolis, Minnesota. He kept a trained eye on one registered nurse who was suspected of stealing hydromorphone, an opioid pain medication, for her personal use.
HCMC has cameras set up in the medication room to monitor controlled substances, and Leon watched as the nurse began gathering prescribed medication for a patient in the emergency department. The process, called wasting, requires the healthcare worker to take a fresh vial or syringe full of medication and then dispose of the excess, leaving only the correct dosage—all with a witness present. Leon observed the nurse dispense a syringe of hydromorphone from the medicine cabinet, and, while a fellow nurse was signing off on the withdrawal, she placed the syringe in her pocket and pulled out an identical syringe, which Leon later learned contained saline. The nurse held up the saline syringe and wasted the required amount, tricking her fellow nurse, and left the room.

At this point, Leon knew exactly what was going on, and watched with increasing alarm as the nurse headed to a patient’s room in the orthopedic area of the hospital. “In that area, I knew immediately, this patient could have a broken bone—they were in intense pain and requiring this medication,” Leon says. “I see a lot of doctors standing around and I’m thinking ‘uh oh, this patient is going to get saline.’”

Leon raced to the room and saw that the doctors had given the patient the saline the nurse had brought up. “The patient was still screaming in pain and the doctor was frantically asking the nurse, ‘Are you sure you got the right dosage? Are you sure it was hydromorphone?’ and she was insisting she had,” Leon says. He called the doctor and the nurse into the hall and explained that the patient had just gotten saline and still needed the proper pain medication because the nurse had diverted the hydromorphone in the medication room. The doctor went to properly treat the patient and Leon called the nurse manager and the local sheriff’s detective in to begin an official investigation into the nurse’s actions.

Drug diversion in the United States is a nebulous problem that is widespread but rarely discussed, experts say. Whether in manufacturing plants, retail pharmacies, hospitals, or long-term care facilities, healthcare workers are stealing drugs—typically for their own personal use—and putting themselves, patients, and coworkers at risk.

“I hate to tell you, but if you have controlled substances and dispense narcotics, you’ve got diversion going on,” says Cherie Mitchell, president of drug diversion software company HelioMetrics. “It’s just a question of whether you know it or not.”

The scope and frequency of drug diversion is almost impossible to grasp, due in large part to how diversion cases are addressed. A facility that identifies a diversion problem might bring in any combination of players, from private investigators and local law enforcement to state accreditation boards or the U.S. Drug Enforcement Agency (DEA). There is no overarching agency or organization that records every instance of drug diversion in the United States.

Controlled substance management is dictated by a number of laws, including the U.S. Controlled Substances Act of 1971, which classifies substances based on how they are used and the potential for abuse. It also dictates how the substances are dispensed, and a facility may be fined if it does not comply.

The closest estimates of drug diversion rates come from people or organizations who dig up the numbers themselves. The Associated Press used government-obtained data in its investigations on drug diversion at U.S. Department of Veterans Affairs (VA) medical centers. Reported incidents of diversion at about 1,200 VA facilities jumped from 272 in 2009 to 2,926 in 2015, the data revealed, and the VA inspector general has opened more than 100 criminal investigations since last October. John Burke, president of the International Health Facility Diversion Association, extrapolated data he obtained from facilities in Ohio to estimate the presence of 37,000 diverters in healthcare facilities across the country each year.

Mitchell points out that any statistic derived from officially collected data still wouldn’t accurately reflect the extent of drug diversion in the United States. “There’s a lot of people investigators really suspected were diverters but had to be chaled up to sloppy practice due to a lack of concrete evidence, so any statistic is talking about known diverters who are fired for diversion,” she tells Security Management. “Even if you did have a statistic, it would be off because how do you incorporate those so-called sloppy practitioners, or diverters who thought they were about to get caught so they quit on you and left? No matter what number you come to, it’s probably bigger in reality.”

**ADDITION AND DIVERSION**

Although more people are paying attention to drug diversion due to recent high-profile cases and the current opioid epidemic in the United States, experts say they have been dealing with the same problems their entire careers.

“I can personally tell you that I dealt with the same issues 15 or 20 years ago...
that the healthcare arena is facing today, specifically in the drug abuse and diversion by their own hospital healthcare employees,” says Charlie Cichon, executive director of the National Association of Drug Diversion Investigators (NADDI) and a member of the ASIS International Pharmaceutical Security Council. “There are different drugs today, of course, than there were 20 years ago.”

Susan Hayes has been a private detective for healthcare facilities for more than a decade and says the opioid epidemic has magnified the drug diversion problem in recent years. “The opioid addiction in America has lit my practice on fire,” she says.

It’s no secret that opioid addiction has reached epidemic levels in the United States. In 2010, hydrocodone prescriptions were filled 131.2 million times at retail pharmacies alone, making it the most commonly prescribed medication, according to the Mayo Clinic. However, those are just the numbers that were legally prescribed—about 75 percent of people who take opioids recreationally get them from a friend or family member. According to the U.S. Centers for Disease Control and Prevention (CDC), approximately 52 people in the United States die every day from overdosing on prescription painkillers.

Healthcare workers are not immune to the draw of opioids. In fact, up to 15 percent of healthcare workers are addicted to drugs or alcohol, compared to 8 percent of the general population, according to the Mayo Clinic.

“Healthcare providers are in very stressful jobs,” Hayes says. “They all have problems. Nurses have emotional attachments to patients that they see die. Even orderlies have very stressful physical jobs, they’re lifting patients. Pharmacists can make mistakes that mean life or death. You have people that are already in very stressful situations, and now you give them access to drugs…. I think the combination is almost deadly.”

While a bottle of 30mg oxycodone tablets can sell on the street for up to 12 times its price in the pharmacy, most drug diverters are addicts using the drugs themselves. Because of this, diversion shouldn’t be considered just a security concern but a patient safety concern, Cichon says. He references several high-profile diversion cases in which the diverters used the same syringe full of medicine on both themselves and their patients, spreading bacterial infections and hepatitis. In one especially egregious case, a traveling medical technician with hepatitis C would inject himself with his patients’ fentanyl and refill the same syringe with saline, ultimately spreading the virus to at least 30 people in two states.

Unfortunately, experts acknowledge...
that most diverters don’t get caught until they have been diverting for so long they start to get sloppy. “The people who are your real problem are the people who are hiding in the weeds, not doing enough to get caught, and those are the ones you want to find,” Mitchell says. “The people they are finding now are the people that have the needle in their arm or somebody has reported them. You want to try to find them before that.”

OUT OF THE LOOP

Hayes details the path of drugs through a hospital: a pharmacy technician orders the medication from a wholesaler, who will deliver them to the hospital pharmacy. The drugs are sorted and stocked in the pharmacy, where they will remain until they are brought up to the patient floors and stored in various types of locking medicine cabinets. When a patient needs medication, a nurse goes to the medicine cabinet and dispenses the drug for the patient.

Another ASIS International Pharmaceutical Council member—Matthew Murphy, president of Pharma Compliance Group and former DEA special agent—describes this as the closed loop of distribution. “Once a drug is outside of the closed loop, when it gets dispensed from a pharmacy or administered by a doctor, it’s no longer in the purview of DEA rules and regulations,” he explains. Drugs are most likely to be diverted during those times when they are in transit or exchanging hands, outside of the closed loop.

Wholesalers. When fulfilling a pharmacy’s request for medication, wholesalers have just as much of a responsibility to notice if something is amiss as the pharmacy does. Whether it’s a retail pharmacy or a hospital pharmacy, wholesalers are responsible for cutting them off if they start to request unusually high amounts of opioids.

In 2013, retail pharmacy chain Walgreens was charged $80 million—the largest fine in the history of the U.S. Controlled Substances Act—after committing record-keeping and dispensing violations that allowed millions of doses of controlled substances to enter the black market. Cardinal Health, Walgreens’ supplier, was charged $34 million for failing to report suspicious sales of painkillers. One pharmacy in Florida went from ordering 95,800 pills in 2009 to 2.2 million pills in 2011, according to the DEA.

Hayes says the fine against the wholesaler was a wake-up call, and now suppliers use algorithms to identify unusual spikes in orders of opiates. Wholesalers can even stop the flow of medication to pharmacies if they believe diversion is occurring—which can be disastrous to a trauma center, Hayes notes.
**Pharmacies.** To restock the shelves, pharmacy technicians compile lists of what medications they are low on to send to the wholesalers at the end of each day. Hayes notes that many pharmacies do not conduct a retroactive analysis on what is being purchased—which is why wholesalers must pay attention to any unusual changes in orders. She stresses the importance of constantly mixing up the personnel who order and stock medications.

“If you’re both ordering and putting away drugs, that’s a bad thing because you can order six bottles when you only need five and keep one for yourself,” Hayes notes.

Similarly, it is important to rotate who delivers the drugs up to the floors for the last 20 years,” Hayes says. “Well gee, did you ever notice that John drives a Mercedes and has two boats and a house on Long Island? He makes $40,000 a year, did you ever do any investigation into why?”

**On the floor.** Experts agree that the most egregious diversion occurs during the wasting and dispensing process in scenarios similar to the incident Leon witnessed at HCMC. Mitchell explains that all hospitals have different wasting procedures—some require nurses to waste the medication immediately, before they even leave the medication rooms, while others may have a 20-minute window. Other hospitals may prohibit nurses from carrying medication in their pockets to prevent theft or switching.

**INVESTIGATIONS**

Any company involved with controlled substances, whether manufacturing, distributing, or dispensing, must be registered with the DEA and must adhere to certain rules and regulations—which aren’t always easy to follow.

Murphy, who worked for the DEA for 25 years, now helps companies follow mandates he calls “vague and difficult to interpret.” For example, DEA requires anyone carrying controlled substances to report “the theft or significant loss of any controlled substance within one business day of discovery.”

“This hospital had 13 vials of morphine that ‘went missing’ and someone called me in to find out why,” Hayes says. “They asked me, ‘Are 13 vials substantial or not? Do I really need to fill out the form?’ I counsel them on what’s substantial because the language is very loose.”

Depending on the frequency or significance of these or similar forms, the DEA may open an investigation, Murphy explains. “DEA will look at these recordkeeping forms and determine if in fact everything has been filled out correctly, that they have been keeping good records,” he says. “If DEA determines that they are lax or have not been adhering to requirements, there could be anything from a fine to a letter of admonition requiring corrective actions.” In more serious cases, DEA could revoke the registration because the activity or behavior was so egregious that it was determined that the facility is not responsible enough, Murphy explains. If a facility loses its DEA registration, it cannot dispense controlled substances.

However, DEA does not get involved in every suspected case of diversion. “There are only so many DEA diversion investigators, so they have to prioritize what they get involved with,” Murphy says. “It has to be pretty egregious for them to get involved to seek a revocation or fine.”

That’s where people like Hayes come in. “They want me to come in instead of DEA or law enforcement,” she explains. “I’m a private citizen, I understand law enforcement procedures, and I can help them get at the root of the problem before they call in law enforcement.”

After an investigation into a diverter is opened, it is unclear what happens to the offender. Hayes says that she typically gathers evidence and gets a confession from diverters, at which point her client calls in law enforcement to arrest them. Leon, who was in charge of diversion investigations at HCMC for 20 years before becoming a consultant for HelioMetrics, was able to investigate but not interview suspected diverters. He tells Security Management that he would call in a sheriff’s detective to interview the suspect.

Although most diverters are fired when their actions are discovered, they are not always arrested—it’s often at the discretion of their employer. Depending on the diverter’s role, state accreditation boards—such as those that license nurses and pharmacists—would be notified and could potentially conduct their own investigations.

Cichon cautions that some hospitals hoping to avoid bad press and
DEA scrutiny may look for loopholes. “We found out through the course of investigations that if someone resigns and was not sanctioned it may not be a reportable action,” he says. “If we allow this person to resign rather than take action against him, then we don’t have to report it.”

Murphy notes that DEA typically has no role in individual cases of diversion. “If the diverter has a license from one of those state agencies, usually it’s required that they be reported, and then it’s up to the board how they proceed with the personal license of the individual,” he says. The DEA doesn’t regulate the personnel—that’s up to the state and the facility.

Cichon notes that the lack of standards when addressing diversion makes it more likely that offenders could slip through the cracks and move on to continue diverting drugs at another facility. “Unfortunately, there are different laws and statutes in every state that set up some sort of reporting requirements,” he says. “There are medical boards, nursing boards, pharmacy boards, and not every worker even falls under some sort of licensing board for that state.”

**STAYING AHEAD**

Due to the stigma of discovering diverters on staff, many hospitals just aren’t preparing themselves to address the problem proactively, Cichon explains. “This is something that is probably happening but we’re not finding it,” he says. “The statistics I’ve seen at hospitals that are being proactive and looking at this are finding at least one person a month who is diverting drugs in their facility. If a 300-bed hospital is finding one person a month, and Hospital B has the same amount of staff and beds and is finding nothing…”

NADDI has been providing training for hospitals to develop antidiversion policies. Cichon notes that many hospitals throughout the country have no plan in place to actively look for diverters. “As big as the issue is, many of them are still just not being that proactive in looking at the possibility that this is happening in their facility.”

Cichon encourages a team approach to diversion that acknowledges diversion as a real threat. “Not just security personnel should be involved with the diversion aspect,” he says. “Human resources, pharmacy personnel, security, everyone is being brought into this investigation, because the bigger picture is patient safety. The diverting healthcare worker typically isn’t one who’s going to be selling or diverting his or her drugs on the street, but they are abusing the drugs while they are working.”

Leon worked hard on diversion prevention at HCMC after discovering a surprising pattern: almost all of the diverters he investigated wanted to be caught. “What got me on this path of prevention was observing the nurses as they would admit to what they did,” he explains. “More often than not the nurses would say, ‘I wanted somebody to stop me. I needed help, didn’t know how to ask for it, and I was hoping somebody would stop me.’ That’s pretty powerful when you’re sitting there listening to this on a consistent basis.”

Leon implemented mandatory annual training for everyone in the hospital—from food service workers to surgeons—to recognize the warning signs of drug diversion. “If a nurse or anesthesiologist or physician is speaking with you and telling you they are having these issues, then you should say something,” Leon explains. “It’s not doing the wrong thing—you’re helping them, and that’s the message we sent out. Look, these individuals are not bad individuals. Something happened in their lives that led them down this path.”

Leon also had cameras installed throughout the hospital that allowed him to observe diversion but also kept his investigations accurate. “We had a nurse who was highly suspected of diverting,” he says. “With the cameras I was able to show that she wasn’t diverting, just being sloppy. The employees appreciated the cameras because it showed they weren’t diverting medication, they just made a mistake.”

Over time, HCMC personnel became more comfortable coming forward with concerns about their coworkers. Before the facility started the annual training, Leon caught at least one diverter a month. Before he retired, he says, that number had dropped to one or two a year.

“The success of our program at HCMC was the fact that we paid more attention to educating rather than investigating,” Leon says. “You have to keep those investigative skills up, but
Most diverters don’t get caught until they have been diverting for so long they start to get sloppy.

You have to spend equal amount of time on prevention and awareness.”

Mitchell points to algorithmic software that can identify a potential diverter long before their peers could. Taking data such as medicine cabinet access, shift hours, time to waste, and departmental access allows software to identify anomalies, such as a nurse whose time to waste is often high, or a doctor who accesses patients’ files after they have been discharged.

“Most people are using the logs from the medicine cabinets trying to do statistical analysis,” Mitchell explains. “You find out 60 days or six months later, or you don’t see that pattern emerge by just using one or two data sets. That doesn’t help. The goal is to identify these people as quickly as possible so they are no longer a risk to themselves or the patients or anyone they work with.”

Murphy encourages facilities to be in full DEA compliance to mitigate diversion. “If somebody wants to steal or becomes addicted, they are going to find a way to do it, and sooner or later they are going to get caught, but then there’s a problem because the hospital has to work backwards to determine how much was stolen and reconcile all that,” he says. He also notes the importance of following up internally on each diversion case and figuring out what went wrong, and adjusting procedures to address any lapses.

“Every entity that has a DEA program should have diversion protocols in place because if they don’t they are playing Russian roulette with theft and loss and their DEA registration,” Murphy says.

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

Most diverters don’t get caught until they have been diverting for so long they start to get sloppy.
With 3 million visitors crossing its threshold annually, the Jacob K. Javits Convention Center is a New York City landmark. It’s hard to miss the six-block long complex, which stretches from West 34th Street to West 40th Street in midtown Manhattan and features more than 840,000 square feet of exhibition space and 28,000 square feet of meeting rooms. Javits hosts an array of events annually, including the New York International Auto Show, the National Retail Federation’s annual convention, and New York Comic Con.

The Javits Center has undergone changes in recent years, including a $463 million renovation from 2009 to 2014. In addition to improvements to the mechanical and sustainability systems, the upgrade included adding 6,000 new glass panels to the outside.

Before the new patterned panels were installed, Javits had a mirror-like façade, making the facility among the top bird-killers in New York City. Birds would frequently fly into the glass walls, not recognizing that the building was there.
Now Javits is considered one of New York’s bird-friendliest facilities; besides upgrading the panels, Javits installed a green roof space spanning nearly 7 acres, which is home to 26 bird species. This rooftop also lowers the facility’s annual energy consumption by 26 percent by lowering heat-gain and water runoff.

But hospitality at Javits is not just for the birds. Providing excellent customer service while maintaining security is a top priority for the center. Security personnel are front and center when customers approach the immediate outside vicinity or enter the building. “We’re engaging the client, making eye contact with the people coming in—we want to be the first person you see when you come in the door,” says Kenneth Dixon, director of security and safety solutions at Javits. “Our focus is a balance between hospitality and security, and finding that right balance is a key to our success.”

**Challenges**

Being a busy convention center means constantly dealing with theft, lost property, and other larceny issues, Dixon explains. The type of theft that occurs varies, including exhibitors who steal from other exhibitors, attendees who steal from exhibitors, and employee theft.

The threat of terrorism also looms large over Javits, where anywhere from 60,000 to 70,000 attendees gather daily. In the spirit of being proactive, security decided to move heavy cement planters to a strategic location in front of the building “to give us a little more protection against vehicular attacks like the ones in London, Berlin, and Stockholm,” he says.

Unattended packages are also a cause for concern, Dixon says, citing the 2013 Boston Marathon bombings and other terror attacks caused by improvised explosive devices left behind.

To further address these security concerns, and to align with the new look and feel from the recent renovation at Javits, Dixon explains that there have been several changes to security procedures, technologies, and staffing at Javits.

“It was the first quarter of 2015 when we started implementing some new policies, and really started to monitor what happened at night, as well as address the legacy larceny complaints that we’ve had,” Dixon says.

With a new and improved security operations center, an increase in the security workforce, and a hospitality-centered approach, Dixon is confident Javits is now an even safer place for its customers, vendors, and staff. Here’s a look at some of the ways in which the Javits Center has accomplished that mission.

**Technology**

Upgrading the center’s security technology was a foundational step in beefing up security at Javits, and the center upgraded everything from cameras to its state-of-the-art command center. Dixon notes that Javits went from 150 legacy cameras to 860 4K-resolution IP cameras from Axis and Arecont Vision in the last year and a half.

**Cameras.** As of press time, the center anticipates having approximately 1,000 cameras at the end of this summer. They are situated throughout the facility, Dixon says, including in the exhibit space, at ingress and egress points, and on the loading docks.

Not only has Javits increased the number and quality of its cameras, but security decided to strategically place them at a visual level where they serve as a deterrent. In the past, cameras were placed above people’s heads and were painted the same color as the walls and columns to create a more visually appealing look.

Now, however, the cameras are placed lower and unpainted, so they may be clearly seen by everyone who comes to the center.

“The people who are looking for the cameras really see them, and know that they are being filmed,” says Dixon. “The chances of getting away with something here at the Javits Center are far less than what they used to be.”

Javits is also currently testing a video management system from Genetec to manage the wealth of footage collected by the cameras.

In addition, the cameras have facial recognition technology capability, so that video can be exported to law enforcement for identification if the need arises.

**Command center.** The command center at Javits is the heart and soul of the safety and security program, Dixon says, and is used for monitoring, dispatch, video review, and alarm monitoring.

Last spring, Javits put in an 18-monitor video wall from Orion that can be customized to view the cameras chosen by the operator. “That allows us to show 30, 40, 50, 60 cameras at a time—or just one at a time—on 18 monitors,” Dixon explains. “We can quickly change camera layouts on the video wall for whatever’s going on at any given time.”

One monitor is dedicated solely to door alarms. Security can also automatically lock large gates and doors with the click of a button. “We have 225 perimeter...
doors,” Dixon says, “each of the doors has a reader in the door that lets us know whether the door is opened or closed.”

If a door alarm is triggered, an audible alert, as well as video associated with the incident, automatically populates the monitor. This lets officers easily determine whether a response is warranted.

The remote open-and-close feature greatly improved convenience for guards working in the building on an overnight shift. “Years ago, we would have dispatched a security guard on the overnight [shift]...he’s maybe two or three city blocks away, and he would have to go open up the gate,” Dixon notes. “Now he can just do that remotely.”

Members of the safety team who patrol the show floor have smartphones to receive photographs and other media related to any dispatch calls. For example, if a child goes missing, a photo or description can be immediately disseminated.

**Analytics.** Frequently, crime at the Javits Center isn’t reported until the victim realizes his or her property is missing, which can be hours after it occurs. Or someone leaves a package unattended, with no trace of who the person was.

The security team wanted a video analytics solution to aid in the investigative process, so it turned to BriefCam software, which compresses hours of video into just a few minutes by speeding it up. “We use BriefCam to solve cases of property that may go missing for one reason or another...and for unattended packages,” Dixon says. “It’s been a real game changer for us.”

If someone leaves a package unattended, or stolen property is reported from a specific place, BriefCam can geofence the area where the item was left or stolen, and show the activity that occurred within a certain timeframe.

Other specific parameters can be set; for example, if security has information about the color of clothing the suspect was wearing, it can isolate the video to show only people wearing that color. “We’re able to see all the activity around the area of concern, and watch 13 or 14 hours of video in a short period of time,” Dixon says. “That has helped us close significantly more cases.”

At the 2016 New York Comic Con show, for example, BriefCam analytics led to several arrests when property went missing from an exhibitor’s booth. Security isolated video to just around the booth and ran analytics to find the thieves.

“In the past, we didn’t have the ability to run analytics like we had in this case, and the person would have been long gone,” Dixon says. “The show would have been over, and we would have been chasing our tail trying to get all the information.”

**Floor plans.** The floor space at Javits is versatile, and conventions can choose the layout they want at their shows. Javits also has 28,000 square feet of flexible meeting room space, meaning that the walls can be easily converted to accommodate smaller or larger groups.

The center recently moved from traditional locks and keys on its meeting room doors to card readers to provide a greater level of security, and it can assign key cards to clients, which expire when their meeting or convention concludes.

But flexibility can come with challenges. In the event of an incident or emergency at the facility, pinpointing an exact location in the building for first responders can be difficult, because the Javits Center stretches for six city blocks, and every convention has a unique floor plan.

“We’ve been struggling over the last year and a half to replace outdated emergency evacuation plans, because we do 175 events every year—and

A recently declassified geospatial tool...allows Javits to pinpoint a more exact location.
Dixon says.

When police or fire departments respond to an emergency or incident, they often come to the facility’s main address on West 34th Street. “We have to say, ‘No guys, it’s actually on 39th Street in Hall C.’ Well, they don’t know where Hall C is—so it ends up causing a lot of confusion and a lot of wasted time,” he says.

A recently declassified geospatial tool from BAE Systems allows Javits to pinpoint a more exact location within the building. The solution works by laying customized show floor plans over the existing blueprint of the center and labeling a grid by numbers and letters. “Now we simply say, for example, ‘Go to H-33,’ and first responders know, within a certain amount of space, that’s exactly where the incident is,” Dixon explains.

The tool also works as an evacuation map, pointing out ingress and egress routes and the adjacent streets they spill out onto. It also shows first-aid office locations and where to find defibrillator machines. “For a building that’s six blocks long, it is extremely difficult to have one security evacuation plan that you can effectively articulate and communicate to everyone who is going to be involved,” Dixon explains.

The safety team has an app from BAE Systems on its smartphones that displays the grid for each show and evacuation routes. Javits eventually hopes to expand that app to first responders. “Right now, we are communicating with responders with a PDF, but they still find that extremely useful,” he notes.

**Customer Service**

“It’s one thing to have all these great procedures and great technology, but our most important asset is our people, and giving them the skills that they need to be successful,” Dixon says. “It’s the foundational aspect to everything we do.”

Because providing great customer service is a key business component, bolstering the security workforce has been crucial to the improvements at the Javits Center.

**Personnel.** A personnel increase has allowed Javits to provide a more robust security force on-site during exhibits and events. In the past, clients exhibiting at Javits would depend mostly on their own contract security force. Now they can work more closely with the increased staff provided by the center.

“There are 25 other companies that are approved to provide security services in the Javits Center, and we, for all intents and purposes, would be the 26th—but we’re here every day,” Dixon says. “We know all the players; we know all of the vendors, contractors, and business partners that are here on a regular basis.”

The safety team, a proprietary force, went from about 45 members to 80 in the last two years. Many of these full-time employees, called public safety officers, come from law enforcement, loss prevention, or corporate security backgrounds, Dixon explains.

The philosophy at Javits, he says, is to provide employees with the tools they need to be successful. “When it comes to training, we take it very seriously,” he says, noting that each safety team member receives 40 hours of hostile surveillance training from Israeli firm AS Solution. They also learn verbal de-escalation methods and undergo active shooter training.

Javits has even changed the appearance of the guard staff to create a more hospitable environment. “We’ve moved from uniformed supervisors and managers to suits and ties,” Dixon notes. “In a lot of ways, we’ve increased the credibility of our team by taking steps like that.”

Rather than large radios that hang off their uniforms and are loud enough for anyone nearby to hear, guards now sport a covert two-way radio earpiece.

**Lost and found.** With tens of thousands of people moving through its doors monthly, many who come to the Javits Center accidentally leave belongings behind or misplace them.

In 2015, the safety team implemented a new software tool to manage the wealth of lost and found items that are turned in—since then, the center has experienced a 28 percent increase in lost and found items reported.

“We follow New York state guidelines for lost property, and we have a chain of custody for every item,” says Dixon, explaining all lost items are logged into a database and put in tamper-proof evidence bags. Security has reunited owners with everything from misplaced iPads to wallets full of cash.

He adds that people are more likely to report that they have found a lost item when they feel deterred by their environment from stealing it. “There’s an interesting relationship between a good security posture within a facility...and a spike in lost and found,” Dixon says.

Not only are more items being turned in, but Javits has raised the level of lost items returned by 40 percent in the same time period. Because exhibitors and clients often come from other countries, security will ship items overseas to make sure they are returned to their rightful owners. “We’ve even returned a cell phone to Sydney, Australia,” Dixon says. “We will do everything within our means to get it back to that person.”

Dixon says an act as simple as reuniting a client with a lost item speaks volumes to the customer service provided by Javits. “It really means a lot to us,” he notes. “We take great pride in it, and we’ve actually become really good at reuniting lost property with its owner.”

Dixon has even personally delivered items to their owners, including an expensive tennis bracelet left at a jewelry exhibition. “The next day we were able to return the jewelry to the owner in New York’s Diamond District. He was thrilled,” Dixon says.

More improvements are on the horizon for the Javits Center. In early 2016, New York Governor Andrew Cuomo announced a $1 billion expansion for the facility, which will add 1.2 million square feet of additional space.
A major addition will be a new four-level truck garage to accommodate deliveries for events. This will reduce the need for tractor-trailers to circle around the city block again and again until a loading dock is available—they will be able to move in and out in a timelier manner.

“This expansion project will...really propel the convention center into the top tier of convention centers nationwide,” says Tony Sclafani, senior vice president and chief communications officer at the Javits Center. “With the new spaces such as new ballrooms, new meeting rooms, and a rooftop event space, we believe that we will attract many major trade shows and conventions that normally would not consider New York.”

Dixon adds that a huge proponent of the safety improvements was Javits Center CEO and President Alan Steel. “Through the board of directors, our CEO was able to obtain the necessary funding to help push all of this through,” Dixon says. “He’s been extremely supportive.”

Sclafani adds that security will only be further strengthened as Javits continues to serve its customer community. “It’s important to note that this security upgrade really is an extension of the renovation and changes—it wasn’t done in a vacuum.”

As Javits anticipates even more improvements, the reinvented approach to security has paid off in measurable ways. In the last two years, the center saw an 86 percent decrease in overnight theft, and a 74 percent decrease in total theft on a year-to-year basis.

“There are a lot of risks that are associated with being the busiest convention center in the country, and with being located in midtown Manhattan,” Dixon says. “We’ve tried to harden the Javits Center—to become more proactive and to do certain things that we think would deter anyone wishing to do us harm.”

CONTACT ASSOCIATE EDITOR HOLLY GILBERT STOWELL AT HOLLY.STOWELL@ASISONLINE.ORG. FOLLOW HER ON TWITTER: @HOLLYWGILBERT.
SECURING SACRED SPACES

RECENT ATTACKS AT HOUSES OF WORSHIP AROUND THE GLOBE CHALLENGE SECURITY PROFESSIONALS WITH PROTECTING OPEN FACILITIES ON A LIMITED BUDGET.
Christians were gathered in churches around the world to celebrate Palm Sunday on April 9, 2017, marking the beginning of Holy Week. During this time of year, many Christians share in a renewal of their faith as they remember the pilgrimage that Jesus took before his death and resurrection.

At Saint George Church in Tanta, Egypt, the church was full. Scriptures were read. Songs were sung. Somewhere between welcome and amen, a bomb exploded—killing at least 25 people and wounding dozens of parishioners and members of the clergy.

Investigators reportedly believe, according to CNN and other media reports, that someone had placed an explosive device under a seat in the prayer hall. Exactly how the bomb was detonated is still unknown.

As emergency personnel were working to secure the scene at Saint George, a second attack occurred just outside of St. Mark Coptic Orthodox Cathedral in Alexandria, Egypt.

The church service had just ended and people were leaving the building when a man arrived wearing a zipped-up jacket with one hand in his pocket. A security officer denied the visitor access to the cathedral and referred him to the metal detector outside the church’s entrance.

The man can be seen on video talking with the officer and then walking towards the metal detector. He walked a few steps past it, turned, entered the metal detector frame, and detonated a bomb, killing at least 11 people—including three police officers—and wounding 35 others. The actions of the security officer and the use of the metal detector saved numerous lives that day.

Between the two attacks, 43 people died and approximately 100 were injured. ISIS claimed responsibility for both attacks and warned that there would be more attacks in the future against Christians, police, and the military, according to CNN.
However, these attacks left many questions unanswered. Details such as how the bombers picked their targets, whether they were working together, and what advance preparations they had made all remained a mystery.

Did the bombers choose these congregations based on the size of the facilities? It appears that the attackers selected a day in which they knew more people would be present at the churches, possibly in an attempt to create more terror and politicize them as an assault on Christianity. A similar attack at a Christian church in Alexandria on New Year’s Day in 2011 killed 21 and injured 96, according to The Telegraph. Christians have been targeted in several attacks in Egypt, which explains the enhanced security precautions in place on Palm Sunday in 2017.

These bombings prompt several questions. What can be done to prevent an attack from occurring in our respective places of worship? Will it become customary to have a bomb-sniffing dog search the premises? Will metal detectors become a common feature outside religious and cultural properties?

“There is no commonly accepted or developed profile of a suicide bomber,” the Anti-Defamation League (ADL) wrote in Protecting Your Jewish Institution in 2015. “The only characteristic accepted by experts is that the overwhelming majority are prepared to die in the service of their cause.”

Security leaders are faced with the challenge of preventing an act that someone else is determined to achieve, even in the face of death.

We have known for years that the Islamic State wants to destroy Western culture, and that they plan to attack various locations, including houses of worship, bus stops, airports, hospitals, schools, shopping venues, concert halls, night clubs, parades, sporting events, and other places with large gatherings of people. Additionally, we are experiencing more attacks by individual terrorists with various affiliations, as seen in recent attacks using vehicles in Paris and London.

The ADL reported in January 2017 that bomb threats have increased. In addition, there is an increase in anti-Semitic assaults on college campuses. As a result, the league has updated some of its resources to assist synagogues with their security plans as they seek to secure places of worship, religious artifacts, and those attending services.

The Muslim community is not exempt from crime, and has reported increases in incidents of violence and vandalism, most of which are suspected to be committed by homegrown extremists in response to terror acts committed across the globe. In the Middle East, extremists often target more moderate Muslims as they seek to impose Sharia Law.

Houses of worship around the world are faced with various challenges as they try to secure their facilities, people, and programs with limited budgets and

---

**HOW TO PROTECT YOUR HOUSE OF WORSHIP**

*By Megan Gates*

**FIFTEEN YEARS AGO,** attackers threw grenades into a church in Islamabad, Pakistan, killing at least five people and injuring numerous others. No one claimed responsibility for the attack.

The attack garnered international response because it was in the diplomatic quarter of the city near the U.S. Embassy and was attended by diplomats and their families. Officials, according to CNN, said the church was only lightly guarded with a single officer responsible for overseeing access via its three entrances.

In 2015, Jim McGuffey, CPP, PSI, PSP, chair of the ASIS International Houses of Worship (HOW) Committee (a subgroup of the ASIS Cultural Properties Council) was in Pakistan and visited that church. He met the pastor and offered to do a security assessment for the church, which the pastor took him up on.

The interaction made him think about the increasing threats to houses of worship and how a limited security budget—or no security budget at all—could affect their security posture.

“These churches often can’t afford to have barriers, metal detectors, or bollards,” McGuffey says. “Most churches are not big money makers—most of them are smaller churches and not well-funded. When we approach them with security countermeasures, we have to think outside the box.”

This led to the creation of the Security Risk Analysis (SRA) Guide for houses of worship by the Cultural Properties Council that was released earlier this year.

It’s designed to share a “modified version of the SRA process, so that with guidance by a qualified security professional, house of worship leaders will be able to identify critical assets and assess threats and hazards,” according to a white paper on the guide. “This information will help determine levels of undesirable consequences.
resources. A congregation of 1,000 will have some of the same challenges as a congregation of 100, but it will have more resources. Smaller congregations may not face the same complexities as larger organizations but they may still encounter violence.

For example, when 21-year-old Dylann Roof entered the Emmanuel African Methodist Episcopal Church in Charleston, South Carolina, on June 17, 2015, only 12 parishioners were present. Every church throughout the world has the same goal: to provide a safe place to worship. We can implement interior and exterior controls and follow best practices to prevent many types of crimes. However, nothing can protect houses of worship from a bombing except denied access.

**BOMBINGS IN THE UNITED STATES**

The most notorious church bombing in the United States occurred in September 1963 in Birmingham, Alabama, at the Sixteenth Street Baptist Church. A bomb exploded in the building, killing four African-American girls during a service and injuring at least 14 others. Three former Ku Klux Klan members were eventually convicted of murder for the bombing. Between 1970 and 2007, there were 25 terrorist attacks against religious figures or institutions in the United States; nine of the 25 attacks involved explosives or bombings, according to the National Consortium for the Study of Terrorism and Responses to Terrorism (START). Nine of those attacks targeted Jewish institutions.

The FBI also tracks hate crimes against individuals and religious institutions, with a reported 1,402 victims of anti-religious hate crimes in 2015, according to the Uniform Crime Reports: Hate Crime Statistics 2016.

Those crimes primarily targeted Jews (52 percent), Muslims (22 percent), Catholics (4 percent), and individuals of...
HOUSES OF WORSHIP | BY PAULA L. RATLIFF

This was an increase from figures released in 2015, when the FBI reported that there were 1,140 victims of religious hate crimes in the United States. Hate crimes, as defined by the FBI, include traditional crimes—like murder, arson, or vandalism—that are motivated by bias.

For example, in January 2012 in Rutherford, New Jersey, several Molotov cocktails and incendiary devices were thrown at a synagogue, starting a fire in the second-floor bedroom of the rabbi’s residence. This was deemed the fourth bias incident in a month against a Jewish religious institution. Other incidents included a fire that was intentionally set and graffiti at two synagogues.

ACCESS CONTROL IS KEY TO A SECURE ENVIRONMENT.

BOMBINGS SUSPECTS

The profile of a bomber in the United States may be different from what security professionals expect. It could be a jilted spouse or lover who is seeking revenge at the end of their romantic involvement. It could be former business partners or employees looking for retribution when a business relationship goes south. It could also be the work of a terrorist—foreign or homegrown—trying to make a political statement toward a specific person or group.

As of this writing, most bombings in the United States are carried out by an individual working alone. Further investigations after the fact generally indicate that a spouse or family member had suspicions about the bomber’s behaviors, but did not seek help.

While security cannot anticipate the moves of a bomber, there are a few behavioral characteristics that could be considered suspicious.

• Nervousness, including sweating, tunnel vision, and repeated, inappropriate prayers or muttering, as well as repeated entrances and exits from the building.
• Inappropriate, oversized, and loose-fitting clothing.
• Concealed hands, such as in pockets, to hold a triggering device.
• Favoring one side or area of the body, as if wearing something unusual or uncomfortable.
• Projected angles under clothing,
such as those that would indicate the individual is carrying a firearm at the waist or ankle.

- Constantly adjusting clothing.
- Carrying packages or backpacks.

When this kind of behavior is observed, the “See Something, Say Something” principle is applicable. However, at religious institutions, if at all possible, congregants should be encouraged to leave the area.

Reports should be made to a law enforcement officer if possible. If law enforcement is not available at the location, individuals have the option to investigate on their own, report suspicions to church staff, or do nothing. In these instances, security professionals should trust their instincts.

PREVENTING A BOMBING

The attacker could use a mail bomb or a placed bomb. Placed bombs, like the one used in the Boston Marathon bombing, injure indiscriminately and can be concealed in boxes, backpacks, briefcases, and purses.

There is no certain way to prepare for a bombing. As witnessed with the Boston Marathon bombing, members of the public are vulnerable at events and in crowds. Someone can enter a facility with intent to do harm and there is little security can do to stop him or her.

But, just as Boston responded quickly with paramedics and doctors, houses of worship need to be prepared with security and safety measures.

Places of worship need video cameras for successful identification of attackers. Congregants must be diligent in their observations of attendees who might intend harm. They also need to be observant of behavior that is unusual, such as a person who attempts to enter a church after the service had ended, as the second Palm Sunday bomber did.

As a precautionary step, religious institutions’ office personnel should be trained about mail bombs and suspicious packages, such as the pipe bomb that was mailed to a Lakewood Church in Houston, Texas, in January 1990.

The pastor’s daughter, director of ministries for the church, opened the package addressed to her father, suffering minor burns and bruises, according to The New York Times.

Access control is key to a secure environment, as the Tanta, Egypt, bombing shows. Someone was able to place a bomb inside the sanctuary, showing that someone had access to the facility prior to the start of the service.

Staff should also be advised to keep offices and desks locked when they are not in use to avoid creating hiding places for explosives. Staff should also ensure that utility janitorial closets, boiler rooms, mail rooms, computer offices, switchboards, and elevator control rooms are locked at all times.

Additionally, trash receptacles—especially dumpsters—should be locked and located far from the building. The area around the receptacles should also be free of debris. As demonstrated by the Oklahoma City bombing in 1995, cars and trucks should be required to maintain a safe setback from the facility.

A security plan should also include an evacuation plan for the facility with a designated meeting point to ensure that everyone is safe, should it be used. Places of worship should also be equipped with medically trained staff, first aid kits, and ambulatory services to quickly respond, should an attack take place.

There are no easy answers to this disturbing dilemma. There is no easy way to predict when or where a bombing may occur. There are even fewer ways to prevent it. As security leaders, we must be diligent in our observations of human behavior.


SECURITY JOBS AND CAREER CENTER

https://securityjobs.asisonline.org
While incidents of espionage, cyber-crime, terrorism, and violence continue to gain headlines, security professionals need to adapt. What worked just a few years ago is not enough for today’s volatile environment. Whether security practitioners are protecting a small organization or a global enterprise, it is critical for them to stay informed about innovations and learn best practices from experts in the industry. That’s the mission of ASIS 2017.

For more than six decades, the ASIS International Annual Seminar and Exhibits has stood as the premier educational and networking event for security professionals worldwide. ASIS 2017, taking place in Dallas, Texas, September 25-28, is the one event where security professionals across all disciplines and industry sectors gain insights from thought leaders and engage with product and service providers who can help translate expertise into solutions. This kind of networking and shared purpose builds community, which is the heart of the Seminar experience and what keeps attendees returning year after year.

“Now more than ever, harnessing the collective wisdom of a global community of peers by sharing ideas and best practices is critical,” says Peter J. O’Neil, CAE, CEO of ASIS International. “We have worked hard to make sure that our conference program meets this need. From breakout sessions, case studies, and lectures to panel discussions, demonstrations, and simulations—our learning program is designed to deepen connections, foster information sharing, and provide practical applications that can be used to advance each attendee’s educational needs.”

This year’s event offers the most comprehensive education program in Seminar history. The lineup includes more than 180 sessions aimed at helping attendees understand the latest developments in security.
ing security professionals keep pace with emerging threats, approaches, and best practices impacting the profession. Topics include Enterprise Security Risk Management (ESRM); drone/UAV reconnaissance and surveillance; active shooter, assailant, insider threat, and soft target attack response; radicalization and violence mitigation; big data, analytics, and the Internet of Things; cybersecurity and privacy; and workplace violence.

For example, the “Lone Offenders, Radicalization, and Violence Prevention” session on September 25 will teach attendees how to expand their organizations’ workplace violence prevention programs to identify and respond to behaviors that may be indicative of insider radicalization. “Defusing Hostile People” on September 25 will demonstrate how to use mental methods and tools to effectively respond to a hostile or potentially violent situation.

And those looking to learn how to apply ESRM principles will find an entire track of options. On September 26, presenters in “The Future of Cyber Security Risk? Wake up, You’re There” session will use ESRM concepts and theories to talk about cybersecurity risks as part of an overarching security risk management program. Later that day, “Enterprise Security Risk Management Requires a New Conversation Among the Executive Team” will examine how to become literate, not just in the language of security or business but in the language of technology and new external threats.

This is just a small sample of the expert-led sessions being presented at ASIS 2017. In addition, extensive education will be offered on the exhibits floor, including career development best practices, impact learning sessions, and product and service demos.

Terrorism and violence threaten our workplaces “in addition to the day-to-day issues we face that never make the news but impact us directly and immediately,” says Thomas J. Langer, CPP, 2017 president of ASIS International. “This year’s education program reflects this reality. From the global perspectives provided by the morning keynotes to innovative learning formats and learning lab experiences on the exhibits floor, our aim is to ensure attendees have the intelligence and professional connections to protect the people, property, and assets entrusted to their care.”

ASIS 2017 promises unprecedented educational value to attendees—addressing the full spectrum of security—through partnerships with leading organizations such as the Information Systems Security Association (ISSA) and InfraGard. To learn more about ASIS 2017, visit www.securityexpo.org.

SUPPORT THE FOUNDATION

In the past three months, full-tuition scholarships were awarded to eight security professionals from around the world to pursue undergraduate and graduate degrees at the University of Phoenix and Webster University. In addition, 10 active-duty military and law enforcement professionals are one step closer to achieving their board certifications—all thanks to ASIS Foundation awards and scholarships. These life-changing programs are funded solely through voluntary donations from individuals and companies who support the Foundation’s mission to provide valuable research and scholarship opportunities.

At ASIS 2017, there are many ways to help support this work—and have fun while doing so! Kick off Seminar week at the Golf Tournament, Sunday, September 24, at the Cowboys Golf Club in Grapevine, Texas. This is a great way to catch up with clients and colleagues at the world’s only football-themed golf club. Later that night, visit Gilley’s Dallas for the Opening Night Celebration. Thousands of peers will be on hand for a truly Texas experience featuring armadillo racing, live music, and the opportunity to donate to the Foundation by participating in the mechanical bull riding competition.

Need to update your professional photo? Head over to the Headshot Lounge located near the Career Center on the Expo Floor, which will be equipped with photographers and makeup artists. This
free service is sponsored by the Foundation. Donations are accepted and appreciated.

The Foundation will also sponsor several education sessions at ASIS 2017, including “Intelligent Building Vulnerabilities: Is There an Open Door into Your Facility?” on Monday, September 25; “Use Metrics Dashboards to Manage Enterprise Security Risks” on Tuesday; and “Archaeological Site Security: Clunia, Huerta De Rey, Spain” on Wednesday.

Stop by the ASIS Hub (#1613) on the exhibit floor to learn more about the Foundation’s work or visit www.asis-foundation.org.

PRE-SEMINAR PROGRAMS

Whether you want to cultivate a better understanding of IT security, security risks for financial institutions, or best practices for successful security consulting, the ASIS Pre-Seminar Program is designed to jump-start your education prior to ASIS 2017. The pre-show options also include ASIS certification reviews.

Understanding IT. Having a basic understanding of information security is essential to protecting physical security systems from cyberthreats, thereby improving the overall enterprise security position of an organization. Sunday, September 24, from 8:00 a.m. to 4:00 p.m., “IT Security for Physical Security Professionals—In Plain English,” sponsored by the ASIS ESRM Commission, will offer key resources and tools to use in navigating information security issues.

“Too often, physical security and cybersecurity professionals operate independently of one another, which prevents a holistic, enterprise risk-based approach,” says session leader Dave Tyson, CPP, CEO at CISO INSIGHTS and chair of the ASIS International ESRM Commission. “This session will use plain English to arm physical security professionals with the cybersecurity basics they need to communicate across that divide and begin working towards a more unified security posture. It will also serve as a valuable foundation for physical security professionals who are looking to extract even more value from the more technical cybersecurity sessions offered throughout the week ahead.”

Financial risk.

Practitioners in the financial sector will want to attend the “Security Risks and Mitigation Strategies for Financial Institutions” program, sponsored by the ASIS Banking and Financial Services Council on Sunday from 8:30 a.m. to 5:00 p.m. During this session, subject matter experts will address threats to global financial institutions, as well as mitigation strategies. Immediately following the program, a networking reception will afford an opportunity to connect with security leaders in the financial services industry.

Consulting.

The “Successful Security Consulting” program will provide insight on how to develop and market yourself as a security consultant while avoiding expensive mistakes. Sponsored by the International Association of Professional Security Consultants, the program is offered from 8:00 a.m. to 5:00 p.m. on Sunday.
Certification. Certification Review Programs provide a high-level review of the security concepts tested on the CPP, PCI, and PSP exams. Attendees will also take a sample test to gauge areas of strength and identify where to best focus their study efforts. Each class will take place from 8:00 a.m. to 5:00 p.m. on Saturday, September 23, and continue from 8:00 a.m. to 2:00 p.m. on Sunday.

Don’t miss the opportunity to begin your ASIS 2017 experience at the Pre-Seminar Programs. To register or learn more, please visit the Pre-Seminar Programs section of the ASIS 2017 website, located under the Conference tab.

40 YEARS OF BOARD CERTIFICATIONS AT ASIS 2017

This year marks the 40th anniversary of the ASIS International Board Certification Program, which began in 1977 with its first certification credential—the Certified Protection Professional® (CPP). ASIS was the first organization to offer a credential specifically for security managers, and it remains the global standard.

ASIS will recognize this milestone anniversary with special activities during ASIS 2017. Newly certified individuals as well as all certificants in attendance will be acknowledged during the networking luncheon on Monday, September 25.

In addition, the four individuals who have held the CPP certification for all 40 years will be celebrated at an awards presentation. Be sure to check out the Show Daily to read the interviews with these board-certified superstars.

- Dr. James D. Calder, CPP, Professor at University of Texas at San Antonio
- Don W. Walker, CPP, Chairman of Securitas Security Services USA, Inc.
- Dr. Kenneth G. Fauth, CPP, Senior Consultant at K. Fauth, Inc.
- James P. Carino, Jr., CPP, Senior Consultant at Executive Security Consultants

Stop by the ASIS Hub (Booth #1613) to get details on additional celebratory plans and for answers to your certification questions.

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

ASIS NYC HIGHLIGHTS

The ASIS 27th New York City Security Conference and Expo was packed with thought-provoking sessions, interactive panels, and engaging exhibitors. The event, held at the Jacob K. Javits Convention Center in early June, opened with a keynote by Paul Fitzgerald of the Boston Police Department, who was present during the 2013 Boston Marathon bombing. He gave attendees a captivating play-by-play of the events following the explosions. After an exhausting 72 hours—filled with managing social media speculation, a shootout, a carjacking, and a citywide shelter-in-place—Fitzgerald described the capture of the younger Tsaarnaev brother, which played on live television.

He discussed the changes made in the years since the bombing and said that partnerships between law enforcement and private entities are more imperative than ever. “The criminals are networking and that’s why it is so critical that we do as well,” Fitzgerald said.

Steve Crimando of Behavioral Science Applications followed the keynote with a discussion about how social media and fake news feed into terrorist operations. “Terrorism is not designed to cause the cracks,” Crimando explained. “It is by the continued use of ambient fear over time that those small tactical strikes deepen and widen those cracks.” Following a break, former Time Warner CSO Brian Allen, CPP, led an off-the-cuff discussion about how to shift security from a trade to a profession and better define the role of security managers.
“Industry folks are starting to talk about security management,” he noted. “It’s getting beyond tech issues and talking about legal liability, protests, and reputational issues. That’s where we should get to.”

An afternoon panel session on protecting America’s cities was led by Fitzgerald; Lori A. Hennon-Bell, CSO of Prudential Financial; John P. Cronan of the U.S. Attorney’s Office in the Southern District of New York; and James Waters, counterterrorism chief with the New York City Police Department (NYPD). They discussed public-private partnerships, combating violent extremism, the private sector’s role in mitigating risk, and challenges in prosecuting terrorism cases.

The following day, cybersecurity expert Iain Paterson led a discussion about organized crime as a cyber-threat. Brian Jantzen and Jared Van Driessche of AS Solution gave a joint presentation on how security professionals need to consider the Internet of Things (IoT) when making an executive protection plan.

The NYC Chapter Person of the Year Luncheon honored New York City Police Commissioner James P. O’Neill and other industry superstars. The Eugene J. Casey Award for Service was presented to Craig Schwab, CPP, former chair of the ASIS NYC chapter. Raymond L. Dean, CPP, was presented with the Joseph A. Spillane Lifetime Achievement Award. Chapter Chair Lynn Brown offered a touching tribute to the wife and son of NYPD Detective Steven McDonald, who passed away in January.

Accepting the Person of the Year Award, Commissioner O’Neill talked about a neighborhood policing model on the streets of New York that allows officers to take ownership of their beats and identify problems in the community. “Murders are down, shootings down...and to think that after all these years we can continue to push violence down is a testament to men and women of the NYPD,” O’Neill said to applause. “Partnership with everyone in this room is critical. I’m humbled—I started out as transit cop, and never in

Navigate Real-World Challenges in New Orleans

November
6-7: Security Force Management
6-8: Conducting Advanced Internal Investigations
6-8: Risk, Threat, and Vulnerability Assessment
9-10: Soft Target Awareness
9-10: Executive Protection

Early-bird savings end September 30. Book hotel by October 16.

LEARN MORE at asisonline.org/nola
my wildest dreams did I think I’d be up here.”

By Lily Chapa, assistant editor at Security Management. Contact her at lilly.chapa@asisonline.org. Follow her on Twitter @lillychapa.

MEMBER BOOK REVIEW

Corporate Executive Protection. By Christian West and Brian Jantzen. AS Solution; available from ASIS; 250 pages; $35 (ASIS members); $39 (nonmembers).

This is not a how-to book for individuals looking to enter the protection field as a bodyguard or executive protection specialist. It’s not about how to protect individuals as they exit a vehicle and enter a stadium where they are the main event. It’s not about what formation works best when moving a motorcade through an urban environment.

Instead, Corporate Executive Protection is a book about why the board of directors should consider an executive protection program, and it examines the benefits and potential issues of establishing a program. How will a proposed program affect the principal being protected? Does the program address the risks and threats faced by the principal? How does the program affect the principal’s family and private life? These and other questions are realistically addressed in this book.

Who will benefit from this publication? Just about anyone participating in the assessment, design, and review of an executive protection program for corporate principals and their families. This includes members of the board of directors, corporate staff supporting the executive protection effort, internal and contract executive protection managers, and others seeking to understand executive protection from a corporate point of view. It’s all about designing and justifying a solid program that will be valued by the corporation and the principal.

REVIEWER: William “Bill” Leap, CPP, is the vice president of security services for Chicago-based Titan Security Group. He is a member of the ASIS Security Services Council.

Throughout his 30-plus years in the industry, Jay (Chuck) McCormick, PSP, has pursued many facets of security integration and assumed many roles in security management. He says continuous learning, certification, and a great mentor were important factors in his upward career trajectory. McCormick credits his mentor, Bob Falconi, CPP, with advancing his career by at least 10 years in the six months they worked together. “His mentoring in program management has proven invaluable to this day,” he says.

In his current position as technical solutions engineer for ESCO Communications, McCormick’s tasks vary greatly from day to day. His ability to handle diverse assignments has been enhanced through his Physical Security Professional® (PSP) certification, which he attained in 2011. “That certification turned my career around,” he attests. “I have the credibility and skills that go beyond ‘that security guy,’” he adds. “I am able to speak with clients, present at conferences, and perform my functions with a high level of confidence.”

That confidence was put to the test when McCormick served as program manager on a four-person national accounts team. A large client summoned the team to discuss its displeasure with an underperforming branch. After hearing the complaints, three members of the accounts team acknowledged the concerns and left the meeting, leaving McCormick to discuss the resolution. Unexpectedly under the microscope, “I pulled from my experiences and molded a solution,” he recalls. By breaking the issues into manageable pieces, McCormick was able to show a flow chart from another project he was managing that hit every major point on the client’s list and commit to getting the work done. He credits his certification for helping him to understand the objectives for a physical protection system and to design risk treatments that provide a higher ROI for the client. “What was memorable,” McCormick says, “was that I was able to talk the talk and turn a hostile situation into a partnership.”

McCormick is studying to add the Certified Protection Professional® (CPP) to his resume. “Obtaining a certification is not an end, but a beginning to becoming more knowledgeable about your craft and career,” he says. Persons who meet the requirements should be willing to set aside a significant amount of time for study. “This is not something to be taken lightly,” McCormick advises.

ESCO encourages others to pursue ASIS certifications. The company supported McCormick in his position as chair of the ASIS Indianapolis Chapter. “ASIS has been branded as the preeminent security organization,” he says. “Being connected to ASIS can only benefit me as an individual as well as the company I keep.”

McCormick admits that safety and security are lifelong passions. He became a State Certified Fire Fighter at age 16 and moved into electronic security at age 20 before launching his security and life safety career. “Helping others to live productive, safe lives is what draws me to this career...and making a difference is what keeps me here.”

PROFILE BY MARY ALICE DAVIDSON, PRINCIPAL, DAVIDSON COMMUNICATIONS
JUDICIAL DECISIONS

NEGLIGENCE. An employer can be sued for negligence by an employee who is injured on the job when the injuries are the result of a dispute that began outside the workplace, a Louisiana appellate court ruled.

Towana Carr was injured at Sanderson Farms, Inc., when her coworker—Kevin Webb—struck her with a piece of equipment called a pallet jack. Webb, according to the lawsuit, allegedly used the pallet jack to knock Carr into a wall and struck her a second time after she said something to him.

Carr filed suit against Webb and Sanderson Farms, seeking recovery for her injuries. She alleged that before the incident, Webb threatened her with bodily harm when they were not at work.

Carr said she reported Webb’s threats to her supervisor, but was told nothing could be done because the threats were not made on Sanderson Farms’ property. In the lawsuit, Carr claimed that the “accident and the damages and injuries resulting [from

LEGAL LIGHTS

RETAILATION

The American Dental Association will pay $1.95 million to resolve retaliation discrimination based on an investigation by the U.S. Equal Employment Opportunity Commission (EEOC). The EEOC claimed that the association’s former chief legal counsel and director of human resources were fired in retaliation for complaining to board members about potential violations of federal anti-discrimination laws. The association denies that it engaged in unlawful conduct, and issued an apology to the two former employees.

CORRUPTION

The former minister of mines and geology for the Republic of Guinea was convicted for his role in a scheme to launder bribes paid to him by executives from China Sonangol International and China International Fund. Mahmoud Thiam, 50, of New York, was convicted of one count of transactions in criminally derived property and one count of money laundering for participating in a scheme where the two organizations paid him $8.5 million for mining rights in Guinea; he transferred roughly $5.9 million of that to the United States to pay for luxury goods and other expenses. “To conceal the bribe payments, Thiam falsely claimed to banks in Hong Kong and the United States that he was employed as a consultant and that the money was income from the sale of land which he earned before he was a minister,” according to the U.S. Department of Justice. (U.S. v. Thiam, U.S. District Court for the Southern District of New York, No. 1:17-cr-00047-DLC, 2017)

ISSUE: National Security
BILL: C-59
VENUE: Canada
STATUS: Introduced
SIGNIFICANCE: Would create a national security review body to provide oversight and security and intelligence activities in Canada.

ISSUE: Management
CASE: H.R. 2283
VENUE: U.S. House of Representatives
STATUS: Passed
SIGNIFICANCE: Would create a U.S. Department of Homeland Security employee engagement steering committee, and an annual employee awards program to improve morale.
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.
the incident] were caused solely by the negligence of Sanderson Farms” for “failing to heed the warning [Carr] gave about Webb’s threat” and for “failing to take any steps to prevent Webb from injuring” her.

Sanderson Farms, however, argued that Carr did not have a claim because it was prohibited under the Louisiana Workers’ Compensation Act, which prevents an employee who is injured by a negligent act at work from making a worker’s compensation claim and suing his or her employer.

The trial court agreed with Sanderson Farms and dismissed the case. Carr appealed the dismissal to the Louisiana Court of Appeal for the First Circuit, which sided with her and found that she could sue Sanderson Farms for negligence.

The appellate court said that “although negligence claims by an employee against her employer for injuries sustained on the job are typically barred by the exclusivity provision of the workers’ compensation act, the act does not cover injuries arising out of a ‘dispute with another person or employee over matters unrelated to the injured employee’s employment.’”

The appellate court also concluded that Carr had a cause of action to sue Sanderson Farms and that she had a valid cause for relief. “If an employer knows or should know of a dangerous condition or person on his premises, the employer is obligated to take reasonable steps to protect its employees,” the court wrote. (Carr v. Sanderson Farms, Inc., State of Louisiana Court of Appeal for the First Circuit, No. 2015-ca-0953, 2017)

**COMPENSATION.** Men can be paid more than women for the same work based on salary histories, a U.S. federal appeals court recently ruled.

“If prior salary alone is responsible for the disparity, requiring an employer to consider factors in addition to prior salary cannot resolve the problem that the [U.S. Equal Employment Opportunity Commission] and the plaintiff have identified,” wrote Judge Lynn S. Adelman in the opinion for the court.

The ruling stems from a case brought by Aileen Rizo, who was hired as a consultant for Fresno County California Schools in 2009 for an annual salary of $62,733—roughly $10,000 more per year than her previous job.

Three years later, Rizo learned that a man was hired for the same position but paid $79,000 per year, and that all other consultants in the same position—who were male—were paid more than she was. Rizo complained to the county about the disparity, but was told that all salaries were set under a standard operating procedure that took salary history into account.

Rizo then filed suit against the Fresno County superintendent under the U.S. Equal Pay Act. The county moved to have the case dismissed, claiming that while Rizo’s salary was less than her male colleagues’ it was based on a “factor other than sex,” according to court documents.

The district court, however, denied the county’s request and found that under the act, “prior salary alone can never qualify as a factor other than sex, reasoning that ‘a pay structure based exclusively on prior wages is so inherently fraught with risk that it will perpetuate a discriminatory wage disparity between men and women that it cannot stand, even if motivated by a legitimate non-discriminatory business purpose,’” the court said.

The district court referred the case to the U.S. Court of Appeals for the Ninth Circuit. Rizo—with support from the U.S. Equal Employment Opportunity Commission—argued that prior salary alone cannot be a factor other than sex.

This is because “when an employer sets pay by considering only its employees’ prior salaries, it perpetuates existing pay disparities and thus undermines the purpose of the Equal Pay Act,” according to court documents.

The appeals court, however, did not find this argument persuasive and reversed the lower court’s ruling. As an example, the court explained a situation where a male and female employee have the same education and years of experience, but the male employee was paid a higher prior salary than the female employee in his previ-
ous position. Their current employer sets salary by considering education, years of experience, and prior salary. “Using these factors, the employer gives both employees the same salary credit for their identical education and experience, but the employer pays the male employee a higher salary than the female employee because of his higher prior salary,” Adelman wrote. “In this example, it is prior salary alone that accounts for the pay differential, even though the employer pays the male employee a higher salary than the female employee because of his higher prior salary.”

While the appeals court reversed the lower court’s ruling, it also remanded the district court’s ruling to have it reconsider the business reasons the county offered for its standard operating procedures for setting employee salaries. (Rizo v. Yovino, U.S. Court of Appeals for the Ninth Circuit, No. 16-15372, 2017)

The guidance, published on the FTC’s blog, stresses keeping disclosures to prospective employees about background checks—which is required under U.S. law—simple by using easy to understand language.

The guidance recommends that employers avoid legal jargon, extra acknowledgements or waivers, certifications that all information in the job applications is accurate, using wording that purports to require the prospective employee to acknowledge that hiring decisions are based on legitimate nondiscriminatory reasons, and authorizations that permit the release of information that federal law doesn’t allow to be included in a background screening report, such as bankruptcies that are more than 10 years old.

This information “makes it harder for the prospective employee to understand the main purpose of the document,” and may be a violation of federal law, wrote David Lincicum, an FTC staff attorney.

**CYBERSECURITY.** U.S. President Donald Trump signed an executive order that aims to strengthen U.S. government networks and critical infrastructure.

The executive order is broken into three parts—securing U.S. government networks, enhancing critical infrastructure cybersecurity, and improving the nation’s cybersecurity.

A key element of the executive order is looking at the U.S. government’s cybersecurity as a whole—not as 190 separate agencies—and requiring all federal agencies and departments to implement the National Institute of Standards and Technology Cybersecurity Framework, explained Tom Bossert, White House homeland security advisor.

“We need to look at the federal government as an enterprise, so that we no longer look at the Office of Personnel Management (OPM) and think, ‘Well, you can defend your OPM network with the money commensurate for the OPM responsibility,’” Bossert said. “OPM, as you know, had the crown jewel, so to speak, of our information and all of our background and security clearances.”

**U.S. LEGISLATION**

**Texas**

**SANCTUARY CITIES.** Texas Governor Greg Abbott signed into law legislation that bans sanctuary cities, effectively making it a crime for police and sheriff departments to not cooperate with U.S. immigration enforcement.
Citizens expect law enforcement officers to enforce the law, and citizens deserve law breakers to face legal consequences,” Abbott said in a statement. “Texans expect us to keep them safe, and that is exactly what we are going to do.”

The law (formerly S.B. 4) requires cities, counties, and universities with their own law enforcement agencies to comply with federal immigration detainers, or face fines of up to $25,000 a day. It also allows the state to remove public officials from office who violate the law.

The law’s critics—including the Texas Major Cities Chiefs and the Texas Police Chiefs Association—claim, however, that it will adversely impact public safety and sow mistrust in immigrant communities.

**West Virginia**

**DRUG TESTING.** West Virginia enacted legislation that clarifies when employers can conduct workplace drug and alcohol testing.

To conduct testing under the West Virginia Safer Workplace Act, employers must distribute a written policy on testing to all employees. Employers may then conduct testing for employment-related reasons, including deterrence and detection of illegal drug use, alcohol abuse, or prescription drug abuse; impairment, accident, and misconduct investigations; and safety and productivity maintenance.

Testing also must take place during—or immediately before or after—work hours, and employees must be compensated for the time it takes to conduct the test. Employers also must cover the cost of testing and follow guidelines in the law for the testing process.

If an employee tests positive, employers can take disciplinary actions, including against “sensitive” employees—employees in a position where an accident could cause death, serious bodily injury, or property or environmental damage. 

This column should not be construed as legal or legislative advice.
Take Advantage of our
FREE Expo-Only Pass!

ASIS 2017 is where thousands of security professionals like you will go for best-in-class analyses and insights, the latest technology innovations, and unparalleled opportunities for collaboration and career advancement.

Your FREE Expo-Only Pass includes:

- Access to the Exhibit Hall on all three days
- Education sessions on the expo floor*
  Earn up to 8 CPEs for FREE on the expo floor
- ASIS Happy Hour on Tuesday
- Closing Keynote on Thursday morning

All-Access Passes, One-Day Passes, Guest Program Passes and event tickets also available

You won’t want to miss it!

Go to securityexpo.org/SMAug to see all registration options.
INTEGRATED SECURITY FOR ICELANDIC PRISON

HOLMSHEIDI PRISON is a high-security women’s prison located near Reykjavik, Iceland. The facility has 56 cells and occupies a 9-acre property. The prison required a security system that would provide conventional security, but also allow prison staff to proactively respond to potential incidents.

Milestone Systems joined forces with Security Center (Öryggismiðstöðin) and Verkis to provide an advanced security solution that combines Milestone XProtect Expert 2016 with CIAS fence and microwave detection systems. High availability is ensured by the failover technology and uninterrupted video recording capabilities in the video management system. The system is designed to reduce the overall cost of ownership and offers unlimited expandability, enabling the prison to control its surveillance investment now and in the future.

Icelandic project management and engineering firm Verkis is responsible for the project’s building management system and designed the electrical, lighting, and security systems. Security Center, a local security services company, provides the alarm and fence systems.

PARTNERSHIPS AND DEALS

CBES installed IP access control systems from ACT at Asda stores and distribution centers across the United Kingdom. Asda is the trading name of Walmart in the United Kingdom.

ASSA ABLOY announced the integration of its IP-enabled PoE and WiFi access control locks with Millennium Group’s Ultra browser-based access control platform.

BioCatch will integrate its behavioral biometric technology into the Experian fraud and identity platform, CrossCore.

BriefCam is delivering solutions powered by NVIDIA technology and deep learning to accelerate video processing performance and enable richer metadata extraction at a reduced cost.

CNL Software entered a nonexclusive technology collaboration with Sonardyne International Ltd., integrating their products for situational awareness of approaching underwater threats.

Dahua and DBAPP Security Ltd. signed a strategic agreement to establish a “safety eco-system” in the field of IoT security.

Genetec Inc. added STid, a French developer of RFID door controllers, to its access control partners.

Hanwha Techwin America and Camcloud are partnering to offer cameras that push video directly to the cloud.

Hikvision joined the HDBaseT Alliance as an Adopter member.

Lantronix, Inc., signed a distributor agreement with Connector Systems, a division of Ingram Micro Inc., in New Zealand.

Leidos will act as an expert service provider for the Fortinet Security Fabric portfolio of solutions.
Peoples Savings and Loan Company uses Netwrix Auditor to control access to sensitive data.

OnSSI is partnering with Jemez Technology to make perimeter video surveillance solutions employing AXIS cameras even more effective in protecting critical assets and infrastructure.

The prpl Foundation and EEMBC announced a formal partnership to advance the use of security-by-separation in Internet of Things edge devices.

PSA Security Network expanded its suite of cybersecurity products and service offerings designed for physical security systems integrators via new partnerships with IDmachines, Secure Global Solutions, and itSM Solutions.

Rajant announced that Sharp Electronics Corporation will use its Kinetic Mesh technology as the wireless communications infrastructure for the Sharp INTELLOS Automated Unmanned Ground Vehicle.

The Safariland Group, parent company of VIEVU, and Veritone will integrate their product offerings to apply artificial intelligence to process data from body-worn cameras.

Vanderbilt is partnering with Citel Spa to support Italy’s financial and industrial sector.

GOVERNMENT CONTRACTS

American Signal Corporation and United Telecom Ltd. designed a tsunami early warning system for the government of Tamil Nadu, India.

Kansas will be the first state to deploy AT&T ESInet, a 911 solution that provides IP-based call routing services to emergency response centers.

Decision Sciences International Corporation was awarded a contract by the Singapore Ministry of Home Affairs to deploy its passive detection system at the Immigration and Checkpoints Authority of Singapore.

Evolis was selected by the Shandong Social Security Department for the personalization and instant issuance of credentials that combine a debit card with a social security card.

HALO Maritime Defense Systems received an award from the U.S. Naval Sea Systems Command to provide an automated waterside security barrier at Naval Station Norfolk, Virginia.

Gwanak-Gu, South Korea, uses Infortrend storage to support its city surveillance operation.

Masergy Communications Inc. announced that Eurostar selected the company’s networking and security solutions to facilitate the high-speed railroad’s digital transformation initiatives.

SDI Presence LLC was selected to provide a turnkey digital upgrade of the public address system at O’Hare International Airport in Chicago.

Sterling High School in Somerdale, New Jersey, implemented Sielox Crisis Lockdown Alert Status System (CLASS).

Smiths Detection Inc. is partnering with Duke University in a project to advance airport checkpoint x-ray system screening capabilities in relation to a contract with the U.S. Transportation Security Administration.

The U.S. Marine Corps Warfighting Lab, in partnership with Defense Innovation Unit Experimental, awarded a contract to Sensofusion to further develop its AIRFENCE mobile capability.

AWARDS AND CERTIFICATIONS

EyeLock LLC announced two new U.S. patents: for acquiring iris images and for linking an iris image with a facial image.

Fireglass was awarded ISO 27001 certification, signaling that its information security practices meet the highest international standards.

Forensiq received Certified Against Piracy and Certified Against Fraud seals from the Trustworthy Accountability Group.

General Dynamics obtained full operating capability status from the U.S. Department of Homeland Security’s Customs and Border Protection for a remote video surveillance platform.

For the 11th year in a row, Genetec was named one of the top employers in Montreal by the editors of Mediacorp Canada Inc.

Hikvision Optical Character Recognition Technology won first prize in the International Conference on Document Analysis and Recognition 2016 Robust Reading Competition.

Passport Systems, Inc., announced that its SmartShield Networked Radiation Detection System completed formal lab evaluation by the National Center for Spectator Sports Safety and Security.

The Security Industry Association honored products from its New Product Showcase at the ISC West trade show. Chosen as the best new product was the CrucialTrak BioMetric Access Control System. The Judges’ Choice Award went to Hydra for its Thermal Imaging Radar. The judges presented awards in more than 20 product and service categories. See the complete list of winners at http://www.iscwest.com/SIANPS/Award-Winners.

University of Maryland, Baltimore County defeated nine other finalist teams to win the 2017 National Collegiate Cyber Defense Competition. The University of Warwick was recognized as an Academic Centre of Excellence in Cyber Security Research by the United Kingdom’s National Cyber Security Centre and the Engineering and Physical Sciences Research Council.

ANNOUNCEMENTS

Anixter, Tri-Ed, and CLARK are continuing Tri-Ed’s Stadium Tour training and networking events in U.S. cities during the 2017 baseball season. The daylong events feature technical trainings, dinner, and a ballgame.

ASSA ABLOY Openings Studio is a plugin to building information management software that helps users design door security solutions.

BICS will acquire TeleSign Corporation and create an end-to-end Communication Platform as a Service.

Camden Door Controls expanded its support of Western U.S. and Canadian customers with faster shipping and extended technical support hours.

The government of Canada implemented a dedicated telephone tip line and online form to accept anonymous tips about fraud, collusion, or corruption in government contracts.

Carnegie Mellon University (CMU) and Tata Consultancy Services are breaking ground on a new facility to be built on the CMU campus in Pittsburgh, Pennsylvania. The building will include research and academic spaces, an innovation courtyard, rain garden, and a robot yard.

Cities of Service launched the Prepared Together impact volunteering grant program, which is supported by the Walmart Foundation. Selected cities will engage citizen volunteers in initiatives that prepare the city for disasters.

Galaxy Control Systems published a new white paper titled Understanding Cloud Services for Access Control.

Hanwha Techwin is constructing a manufacturing facility in Vietnam’s Bac Ninh province.

The Heinz College of Information Systems and Public Policy and the CERT Division of the Software Engineering Institute at Carnegie Mellon University launched a Chief Risk Officer Certificate program.

Mission500 raised more than $125,000 at its eighth annual Security 5K/2K Run/Walk and related sponsorships at this year’s ISC West.

NTT Security formed the Global Threat Intelligence Center to replace the former Security Engineering and Research Team.

Observables is a new security solutions company that created a connected service platform that unifies access control, automation, surveillance, and security.


Point Blank Enterprises and First Tactical merged and will build an integrated clothing and body armor system.


Security vision products from Siqura are now branded TKH Security Solutions.

Sword & Shield Enterprise Security launched a new federal division, Sword & Shield Federal, and opened an office in Washington, D.C.

TASER International is changing its name to Axon.

Western Governors University is now offering a bachelor of science degree in Cybersecurity and Information Assurance.

STRATEGIC MOVES IN THE NEWS

<table>
<thead>
<tr>
<th>WHO</th>
<th>WHAT</th>
<th>OF/WITH</th>
<th>RESULT</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASSA ABLOY</td>
<td>ACQUISITION</td>
<td>JERITH ALUMINUM FENCE</td>
<td>The move strengthens ASSA ABLOY’s position in North America and helps the company provide a complete range of door opening solutions.</td>
</tr>
<tr>
<td>HANWHA TECHWIN</td>
<td>GLOBAL PARTNERSHIP</td>
<td>NVIDIA</td>
<td>The two companies will develop surveillance solutions with embedded artificial intelligence.</td>
</tr>
<tr>
<td>OROLIA</td>
<td>ACQUISITION</td>
<td>NETWAVE SYSTEMS B.V.</td>
<td>Netwave and McMurdo, another Orolia brand, will work together to enhance and integrate maritime safety equipment.</td>
</tr>
<tr>
<td>PIVOT3</td>
<td>STRATEGIC OEM RELATIONSHIP</td>
<td>INTELLIGENT SECURITY SYSTEMS</td>
<td>ISS will integrate the Pivot3 hyperconverged infrastructure platform with its video management software for robust security intelligence and video storage options.</td>
</tr>
</tbody>
</table>
Let’s Talk Security

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

Available on iTunes

Apple and the Apple logo are trademarks of Apple Inc., registered in the U.S. and other countries. iTunes Music Store is a service mark of Apple Inc.
Together we can

Educate  Heal

Inspire  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
RETAIL ANALYTICS

Bosch Security Systems of Fairport, New York, introduced In-store Analytics, a solution to provide retailers with valuable insights on store traffic for improving operations, customer engagement, and sales. This cloud-based service uses position data generated by intelligent cameras to provide detailed information on how shoppers move throughout a store and interact with the displays. Bosch IP panoramic cameras with on-board Intelligent Video Analytics create position data of shoppers’ movements. The solution easily scales to cover even the largest retail stores and large multistore chains.

INTEGRATED SECURITY

An integrated video and access control software platform from 3XLOGIC, INC., of Westminster, Colorado, enables total remote system administration from a mobile device. No wires are needed to connect access control to the video system; that is done via software. An automated cloud-based programming tool allows users to install the software by scanning a QR code using a smartphone. The system offers push notifications and the ability to use a cell phone as a credential. It is designed to be affordable for small and medium-sized businesses.

MOBILE WEATHER ALERTS

IBM and Atlanta-based The Weather Company, an IBM Business, introduced Mesh Network Alerts technology that provides a mobile method of communicating with underserved populations in developing countries. The technology can notify residents about potential severe weather events or disasters, even in areas with limited Internet connection and disrupted cellular networks. The mesh technology will be available via the Weather Channel app in emerging markets. The app uses peer-to-peer connections within the mesh network to send alerts via smartphone, and it links other nearby phones to extend the signal.

BODY SCANNER

The SOTER RS low-dosage full-body scanner from ODSECURITY of Leeuwarden, The Netherlands, combines ultra-low radiation with maximum visibility for use at airports and prisons. Within seconds, the unit reveals metallic and nonmetallic objects such as weapons, narcotics, and gemstones. Even ingested or camouflaged items can be detected, because the scanner distinguishes between human tissue and other materials.
HIPERWALL, INC., of Irvine, California, unveiled next-generation Hiperwall Premium Suite video wall management software designed with fault tolerance, limitless resolution, and overlapping display boundaries. Because no proprietary hardware is required, it is cost effective and budget friendly. The solution features software with a simple user interface designed for nontechnical users and requires no specialized servers or switches. The software features an ultra-high resolution display capability with scalable size that can support a combination of objects, including still images up to 16B resolution, HD and UHD videos, and streaming content and PC applications. Hiperwall Core Suite is an entry-level system that provides the basic Hiperwall capabilities. 805

CAMDEN DOOR CONTROLS of Mississauga, Ontario, Canada, enhanced its line of CM-AF500 illuminated annunciators with superior visibility and clearer text. When illuminated, text and graphics are highly visible, even in bright daylight; when not illuminated, the text is invisible. Weatherproof and vandal resistant, they are available with almost any text and graphics. They feature heavy-gauge stainless steel face plates and are backed by a three-year warranty. Adjustable volume control makes them suitable for confined spaces such as small restrooms. 806

AMBERALLA, INC., of Santa Clara, California, introduced the S5L family of 4K System on Chips (SoCs) with advanced analytics and low power use to enable the next generation of IP cameras. The S5L is designed for professional IP cameras and includes 4K high dynamic range processing, multi-streaming, on-chip lens distortion correction, and dual video inputs. The S5LM targets the home monitoring market, including battery-powered cameras and doorbell cameras. Both chip families feature advanced analytics and support the company’s SmartHEVC (H.265) and SmartAVC (H.264) algorithms to deliver video with low bitrates and excellent quality. Analytics include object and person detection. 807

The modular AXIS FA Series from AXIS COMMUNICATIONS of Lund, Sweden, consists of units that are sold separately. The AXIS FA54 Main Unit, the AXIS FA1105 Sensor Unit with standard lens, the AXIS FA1125 Sensor Unit with pinhole lens, and the AXIS FA4115 Dome Sensor Unit with varifocal lens offer cost-effective, discreet indoor surveillance. The Main Unit can stream HDTV 1080p videos from four connected sensor units simultaneously using one IP address. Forensic wide dynamic range is optimized for low light. It can support advanced video analytics and can be connected to monitors. Sensor units are small enough to be built into surfaces, and can be installed at eye-level without drawing attention. 808

TYCO SECURITY PRODUCTS of Westford, Massachusetts, announced that its EntraPass Go Pass now supports the Apple Watch mobile credential that allows cardholders to use the watch for quick passage through access points without an access card. It extends the power of the EntraPass Go Pass mobile phone application to the Apple Watch environment. All user activities are recorded on the EntraPass server. Cardholders download the app to a mobile phone and then accept a credential invitation from the system administrator. Once accepted, end users can gain access to a door by pressing the appropriate icon of the door in the app on the phone or the Apple Watch. 809
MARKETPLACE

EAS TAGS

CHECKPOINT SYSTEMS of Thorofare, New Jersey, created its smallest Electronic Article Surveillance (EAS) tag with organized retail crime leave-behind protection. Designed for high-theft retail categories, the 2928 S Swat Micro Tag optimizes protection without obscuring branding and product information. The clear RF EAS label includes visible circuitry and messaging for visual deterrence against theft. It offers the added protection of an indelible graphic that’s left behind on product packaging if the tag’s EAS circuitry layer is forcibly peeled away; this makes stolen goods more difficult to fence. The tag is easily deactivated at point of sale for an improved customer experience. Custom printing options enhance targeted protection and store branding. 810

COMPLIANCE SOFTWARE

London-based CITICUS LIMITED updated its risk and compliance management software with the ability to conduct privacy impact assessments as required by the European Union’s General Data Protection Regulation. The software provides a triage assessment of information systems or initiatives that involve the collection and processing of personal data. Risk factors to personal data can be identified objectively and evaluated to determine the overall level of risk. The software can then identify and manage actions to mitigate the risk and track compliance. 811

ACCESS SYSTEMS

A new line of physical access systems from DORMAKABA of Reamstown, Pennsylvania, includes security revolving doors, personal interlocks, full-height turnstiles, sensor barriers, and tripod and waist-height turnstiles to control access to building entrances, perimeters, and restricted areas. Security Revolving Doors provide a practical and secure solution for any interior access point. An optical separation system accurately detects more than one person in a revolving door and allows or denies passage as appropriate. Full-height turnstiles are recommended for securing perimeters, and modular versions enable individual combinations of multiple units to accommodate bicycle doors, integrated doors, and emergency egress. 813

ETHERNET OVER COAX

ALTRONIX of Brooklyn, New York, is expanding its line of eBridge Ethernet over Coax solutions with the introduction of the new eBridge 800E Managed 8-Port EoC Receiver with Integral PoE Switch. This device is an all-in-one multiport media converter with a built in PoE switch and network communications. It is an ideal head-end solution to integrate coax infrastructure with IP devices such as cameras and accessories. The compact unit features two 1-gigabit uplinks, eight ports providing up to 30 watts of full power per port, and a media converter. The receiver is compatible with eBridge100TM and eBridge100ST hardened transceivers. 814
REQUEST DETAILED PRODUCT INFORMATION THROUGH OUR MONTHLY E-RESPONSE. VISIT HTTP://SECURITYMGMT.HOTIMS.COM, OR USE YOUR SMART PHONE TO ACCESS THE QR CODE ON THIS PAGE.

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

<table>
<thead>
<tr>
<th>CIRCLE #</th>
<th>PAGE #</th>
<th>CIRCLE #</th>
<th>PAGE #</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>22</td>
<td>10</td>
<td>19</td>
</tr>
<tr>
<td>29</td>
<td>75</td>
<td>01</td>
<td>02</td>
</tr>
<tr>
<td>--</td>
<td>08</td>
<td>30</td>
<td>76</td>
</tr>
<tr>
<td>21</td>
<td>41</td>
<td>28</td>
<td>69</td>
</tr>
<tr>
<td>15</td>
<td>27</td>
<td>12</td>
<td>23</td>
</tr>
<tr>
<td>--</td>
<td>29</td>
<td>07</td>
<td>13</td>
</tr>
<tr>
<td>08</td>
<td>17</td>
<td>17</td>
<td>33</td>
</tr>
<tr>
<td>06</td>
<td>11</td>
<td>13</td>
<td>24</td>
</tr>
<tr>
<td>22</td>
<td>47</td>
<td>14</td>
<td>25</td>
</tr>
<tr>
<td>02</td>
<td>03</td>
<td>03</td>
<td>04</td>
</tr>
<tr>
<td>04</td>
<td>06</td>
<td>18</td>
<td>37</td>
</tr>
</tbody>
</table>

ADVERTISERS ONLINE

<table>
<thead>
<tr>
<th>Abloy Security, Inc.</th>
<th><a href="http://www.abloyusa.com">www.abloyusa.com</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>AlarmLock</td>
<td><a href="http://www.alarmlock.com">www.alarmlock.com</a></td>
</tr>
<tr>
<td>Altronix Corp.</td>
<td><a href="http://www.altronix.com">www.altronix.com</a></td>
</tr>
<tr>
<td>Ameristar Security Products</td>
<td><a href="http://www.ameristarsecurity.com">www.ameristarsecurity.com</a></td>
</tr>
<tr>
<td>Commpoor Technologies</td>
<td><a href="http://www.comm-port.com">www.comm-port.com</a></td>
</tr>
<tr>
<td>Dahua</td>
<td><a href="http://www.dahuasecurity.com">www.dahuasecurity.com</a></td>
</tr>
<tr>
<td>Detex Corporation</td>
<td><a href="http://www.detex.com">www.detex.com</a></td>
</tr>
<tr>
<td>dormakaba</td>
<td><a href="http://www.dormakaba.com">www.dormakaba.com</a></td>
</tr>
<tr>
<td>DSI (Designed Security Inc.)</td>
<td><a href="http://www.dsigo.com">www.dsigo.com</a></td>
</tr>
<tr>
<td>DSX Access Systems, Inc.</td>
<td><a href="http://www.dsxinc.com">www.dsxinc.com</a></td>
</tr>
<tr>
<td>Hikvision USA</td>
<td><a href="http://www.hikvision.com">www.hikvision.com</a></td>
</tr>
<tr>
<td>Keyper Systems</td>
<td><a href="http://www.keypersystems.com">www.keypersystems.com</a></td>
</tr>
<tr>
<td>Mercury Security</td>
<td><a href="http://www.mercury-security.com">www.mercury-security.com</a></td>
</tr>
<tr>
<td>Mission 500</td>
<td><a href="http://www.mission500.org">www.mission500.org</a></td>
</tr>
<tr>
<td>Quantum Secure</td>
<td><a href="http://www.quantumsecure.com">www.quantumsecure.com</a></td>
</tr>
<tr>
<td>Red Hawk Fire &amp; Security</td>
<td><a href="http://www.redhawkus.com">www.redhawkus.com</a></td>
</tr>
<tr>
<td>Research Electronics, Int’l</td>
<td><a href="http://www.reiusa.net">www.reiusa.net</a></td>
</tr>
<tr>
<td>Safety Technology International, Inc.</td>
<td><a href="http://www.sti-usa.com">www.sti-usa.com</a></td>
</tr>
<tr>
<td>Special Response Corporation</td>
<td><a href="http://www.specialresponse.com">www.specialresponse.com</a></td>
</tr>
<tr>
<td>Talkaphone</td>
<td><a href="http://www.talkaphone.com">www.talkaphone.com</a></td>
</tr>
<tr>
<td>WM Security Services, Inc. (WMSSI)</td>
<td>wmssi.wm.com</td>
</tr>
</tbody>
</table>
COUNTERTERRORISM OR COERCION?

The U.S. government has prosecuted more than 800 people on terrorism-related charges since 9/11. However, a “majority had no direct connection to terrorist organizations,” according to a recent review of U.S. Department of Justice data by *The Intercept*. “Many were caught up in FBI stings, in which an informant or undercover agent posed as a member of a terrorist organization.”

25
Percentage of defendants charged with terrorism-related offenses who were prosecuted in New York

<table>
<thead>
<tr>
<th>Alleged Affiliation of Defendants</th>
<th>Prosecuted in New York</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unaffiliated</td>
<td>41.1%</td>
</tr>
<tr>
<td>Al Qaeda</td>
<td>24.8%</td>
</tr>
<tr>
<td>ISIS</td>
<td>17.5%</td>
</tr>
<tr>
<td>Taliban</td>
<td>8.4%</td>
</tr>
<tr>
<td>Al Shabaab</td>
<td>8.2%</td>
</tr>
</tbody>
</table>

Terrorism Defendants Caught Up in FBI Stings

- Involving Informants: 33%
- Not Involving Informants: 4%

Plea and Conviction Results of Defendants

- Plead Guilty: 52%
- Found Guilty at Trial: 4%
- Acquitted, Charges Dropped, or Dismissed: 44%
Networx Wi Fi Access System: 
*Installs in place of a lock,* on any door, in under an hour. (Free Security Management Software, too.)

Networx. It’s just easier to install, afford, network, manage & use. Simple. WiFi. No wires to run from gateways to locks. Runs right on customer’s network or Ethernet. Proven performance, and providing many years of battery life, it’s very low maintenance. Free Windows-based software, or enterprise platform integration options, with leading brands:

**ALARM LOCK**

Ask for Alarm Lock Networx & 
Visit us at ASIS, Napco Booth 3120
or call us 1.800.ALA.LOCK or www.alarmlock.com

*Trilogy, Networx, ArchiTech & Lock and **Continental CardAccess or CA4K™ CardAccess are trademarks of Alarm Lock, a division of Napco. **Lenel Open Alliance Program Partners is a trademark of United Technologies Corporation.*

For product info #29 securitymgmt.hotims.com
Solid. For 25 years, security-conscious organizations have built their systems on the most solid access control platform in the business. Utilizing best practices in access control and cyber security, Mercury’s high-performance, rock-solid hardware is the most trusted in the industry. Strong, reliable and scalable, it’s the ultimate defensive line for facilities. Ask about Mercury. At the heart of a robust system, it sets the standard for serious security. Learn more at www.mercury-security.com

Your favorite football team has a defensive line.

Your security system has Mercury.