Issue & Beyond

- Global Risk
  Security symposium highlights travel safety.

- Cybersecurity
  LinkedIn networkers may be vulnerable.

- 24
  ACCESS CONTROL

- 42
  GUEST RELATIONS

- 46
  OPEN OFFICES

- 36
  SOFT SKILLS
IT’S OFFICIAL!

$800 MILLION RUN RATE

APPROX. 30,000 EMPLOYEES IN 320 OFFICES
IT’S OFFICIAL.

Last year, I asked you to keep a secret about a “deal” that would be a game-changer for us. Well, now it is official.

SecurAmerica has just acquired controlling interest in DGS, a national security and aviation services company owned by a major airline. The airline is retaining a minority stake; they have been and will continue to be a great partner since January 1980. They have helped me to go global before and will do so again.

DGS has a revenue of $450 million, has 20,000 employees, and services over 170 airports across the United States, including Alaska and Hawaii, Guam, and the Bahamas. Now we can compete with the Big Four (I mean, the Big Three).

After our deal with DGS, we now have over 30,000 employees with over 320 offices across the country. As a potential customer, why is this important? We now can compete on a national basis (and eventually, a global basis), but more importantly, we are in business for the long haul. We are not for sale. We must give you better service and for less money. Private equity is fairly predictable; they are focused on shareholders, not customers, and in general, they want to sell and reap as much profit as possible in 3 to 5 years. Our mindset is SERVICE, SERVICE, SERVICE. Their mindset is CUT, CUT, CUT and SELL. So who do you want to manage your security?

If you have questions, call me and let’s talk; my office line is 404-926-4202.
Reliability...When It Matters Most!

Two-way communications or one-way public address, GAI-TRONICS provides solutions to help you lead the way to a safer Campus.


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

For product info #2 securitymgmt.hotims.com

Connect with GAI-TRONICS!
“Being drunk, not only is it not a crime, it’s acceptable behavior at a casino and a nightclub—it’s what we market. Just because someone gets drunk doesn’t mean they are a bad person.”

Darrell Clifton, CPP, executive director of security for Eldorado Resorts, Inc., on dealing with intoxicated patrons. PAGE 44

$465,000
Amount paid by nursing and healthcare facility Absolut Facilities Management, LLC, to settle charges of pregnancy and disability discrimination. In the suit, the U.S. Equal Employment Opportunity Commission (EEOC) charged that the firm fired employees based on their pregnancy status. PAGE 58

“With you’re on LinkedIn, you want to know that you’re talking to real people, you feel safe, and you’re engaging with professionally relevant content.”

Madhu Gupta, director of product management, trust, and security for LinkedIn. PAGE 29

Year that then-U.S. Secretary of State George P. Shultz addressed members of ASIS and announced the formation of the U.S. Overseas Security Advisory Council (OSAC). PAGE 54
Visit us at BigBooth.com to find the options that meet your demanding security or site-specific requirements.

Quality Workmanship

“When I visited the B.I.G. facility, I saw that it was a very well run and lean ship. Quality workmanship was obvious from the moment I walked in. Everybody worked as a team to secure our nuclear power facility. We’re very pleased with B.I.G.’s performance—they made a big difference.”

Mission Critical Security Specialist

WWW.BIGBOOTH.COM
Ph. 626 448 1449 • Toll Free 1 800 669 1449

For product info #3 securitymgmt.hotims.com
GUARD FORCE
THE INTOXICATION ISSUE
Private parties regularly hire contract
security firms. But often, those
security officers have not received
training in how to interact with,
and manage, intoxicated guests.
By Megan Gates

OPEN OFFICES
OUT IN THE OPEN: THE
SECURITY CHALLENGES
OF NEW OFFICE SPACES
Open-concept office spaces are on
the rise. The safety and security
challenges they present are
significant.
By Holly Gilbert Stowell

THE HARD TRUTH ABOUT
SOFT SKILLS
We asked five security industry
recruiters about the importance
of soft skills. The short answer:
communication abilities and
emotional intelligence are crucial
for managers.
By Mark Tarallo

On the Cover: Illustration
by Steve McCracken

Cover Story
36
WHEN ONE DOOR CLOSES, ANOTHER OPENS.

INSTALLED IN FACILITIES GLOBALLY, STRIKEIT INTEGRATES WITH HIGH IN-RUSH PANIC BARS, LOW CURRENT MLR EXIT DEVICES, ELECTRIC STRIKES AND MAG LOCKS. PROVEN POWER AND PRECISE FUNCTIONALITY COUPLED WITH AN UNPARALLELED WARRANTY, EQUALS RELIABLE ACCESS 24/7.

ALTRONIX SECURES YOUR MOST CRITICAL INS AND OUTS.

MADE IN THE U.S.A.  ALTRONIX.COM  LIFETIME WARRANTY
FEBRUARY 2019

NEWS & TRENDS
Security remains crucial for apartment renters, and old strategies like gated access are popular even as the newer app-based approaches gain traction.
By Mark Tarallo

10 CONTRIBUTING AUTHORS

12 SM DIGITAL

14 EDITOR’S NOTE
Communication.

20 NATIONAL SECURITY
The Overseas Security Advisory Council (OSAC) brings together U.S. security professionals to explore global risks.
By Michael Gips, CPP

24 CASE STUDY
The state of Michigan upgrades to a cutting edge, Bluetooth-enabled access control system.
By Holly Gilbert Stowell

28 CYBERSECURITY
LinkedIn can be an effective networking tool, but it can also be used to target employees and gain corporate secrets.
By Megan Gates

52 ASIS NEWS
ASIS Europe 2019 will examine smart cities of the future.

53 ASIS BOARD OF DIRECTORS

58 LEGAL REPORT
Security-related legislation considered by the 115th U.S. Congress.
By Megan Gates

62 INDUSTRY NEWS
By Flora Szatkowski

63 ADVERTISER INDEX

64 MARKETPLACE

66 GETTING TO KNOW
Gail Essen, CPP, PSP.
Pete Bernritter is senior regional manager, Americas Security and Safety at Dassault Systèmes, overseeing physical security, travel security, and crisis management operations in North and Latin America. He began his career as a U.S. Army military policeman, spending time as both a detector dog handler and a special agent in the protective services.

Since transitioning to the private sector, Bernritter has worked in pharmaceutical and technology multinational corporate security organizations. He is a member of the ASIS Investigations Council and serves on the ASIS Technical Committee for developing the Active Assailant Annex to the ASIS/SHRM Workplace Violence Prevention and Intervention Standard.

Book review  
PAGE 18

Glen Kitteringham, CPP, has worked in the security industry since 1990 as a loss prevention officer, internal investigator, security guard, supervisor, manager, and director. He is now president of Kitteringham Security Group in Alberta, Canada, where he provides security and management consulting services. Kitteringham also teaches security and emergency management courses at the University of Calgary and the Justice Institute of British Columbia.

Kitteringham obtained his doctorate in security risk management from the University of Portsmouth in 2017 and his Master of Science in Security and Crime Risk Management from the University of Leicester. He has been a member of ASIS since 1994.

Book review  
PAGE 22

Ben Rothke has more than 15 years of industry experience in information systems security and privacy. His areas of expertise include risk management and mitigation, security and privacy regulatory issues, design and implementation of systems security, encryption, and cryptography.

Rothke is the author of *Computer Security: 20 Things Every Employee Should Know*. He writes security and privacy book reviews for *Slashdot* and *Security Management*, and is a former columnist for *Information Security*, *Unix Review*, and *Solutions Integrator* magazines.

A frequent speaker at industry conferences, he is a member of the Society of Payment Security Professionals and InfraGard. He holds eight certifications in cybersecurity and IT subjects.

Book review  
PAGE 29

Poul Nielsen, PCI, is an intelligence analyst at the Copenhagen Police Department, where he is a subject matter expert on threat assessments, open source intelligence, and violent political extremism.

Nielsen has been a member of ASIS International and the Denmark Chapter since 2011, and he earned his Professional Certified Investigator designation in 2013. He serves on the ASIS International Investigations Council. Nielsen is a certified security manager and is also studying for his master’s degree in intelligence and security studies.

Book review  
PAGE 56
In a recent survey of apartment renters, gated access was the most frequently cited amenity desired by respondents, and app-controlled door locks made the top 10.

WEAPON VULNERABILITY
Some U.S. weapons have a significant vulnerability—they are relatively easy to hack, according to a recent U.S. Government Accountability Office report.

SPY CONVICTION
A U.S. federal jury convicted Kevin Patrick Mallory, a former CIA case officer, on espionage charges for transmitting classified documents to an agent of the People’s Republic of China.

Following the U.S. midterm elections, most voters said it was very easy to vote, and confidence in election security increased.

High-performance employees tend to prefer quiet work spaces to open-office designs.

The Center for Employment Equity released a report on employers’ responses to sexual harassment.

By the end of 2018, almost 17,000 U.S. companies will have avoided a data breach.

Most Americans have heard of social media bots, but are concerned about how they operate.

“Pertinent subject!”
- Chris Stuart, vice president, Top Guard Security, commenting on Eugene Ferraro’s article “How to Investigate #MeToo.”

Go to SM Online for these and other links mentioned throughout this issue.
Every company faces risk that is unique to the complexities of their business. G4S can help you identify what those are through our Security Risk IQ Survey. Developed in conjunction with Georgia State University, the survey is a free online questionnaire that helps security professionals identify and quantify the risks they face. In just a few minutes, you can be better prepared for future threats.

Take a FREE Security Risk IQ survey. Visit SecurityRiskIQ.com

The one complete force in security. | 888-645-8645 | www.G4S.us

Get totally complete security under one roof. Yours.
linguistics expert Gretchen McCulloch had been hearing rumors. Parents were reporting that their toddlers, when given access to smartphones and texting apps, were composing texts entirely out of emoji.

McCulloch had questions. “I wanted to find out not only whether kids were texting emoji but which emoji, and why? How do they organize emoji into sequences and ideas, and how do these early ramblings shift as kids learn to read?” she wrote in an article for WIRED magazine, “Children Are Using Emoji for Digital-Age Language Learning.”

McCulloch enlisted those with young children to anonymize and send some examples of the kids’ electronic communications. The results showed that many preliterate children ages three to five send text messages comprising only emoji. These messages can be complex and sometimes follow a theme, according to McCulloch. For example, one five-year-old sent a long emoji string of “any animal that pinches.”

However, as the kids got older and learned how to read and write, their text messages grew more sophisticated. First, relevant words accompany the emoji and, eventually, children aged out of emoji strings altogether, using them only as line breaks or borders. “Several adults noted that their kids had simply stopped sending long emoji-filled messages once they learned how to read,” according to McCulloch.

What fascinated McCulloch is what these behaviors teach kids about written communication. Before the smartphone age, adults wouldn’t communicate directly in writing with preliterate children. “Why would my parents leave me a note before I could read it?” McCulloch noted. “But now that we all communicate in writing so much more often, kids also are reading text messages. For a kid to get a text message written directly for them, and read directly to them, which they can reply to in some fashion, it teaches them something powerful about the written word—that it can be used to connect with people you care about.”

Adopting new and powerful communication methods is also key to success in the workplace but embracing new ideas can be daunting. This month’s cover story, “The Hard Truth About Soft Skills,” makes it clear that communicating well and displaying emotional intelligence can mean the difference between a successful team and a failed venture.

ASIS International is investing in an ongoing effort to bring a sharp focus on important issues that advance the profession through a proactive approach to developing content on a variety of topics. Be on the lookout in the next few months for a new content series around management and leadership. Produced in collaboration with industry experts and volunteer leaders, the series will provide more information on the topic through a variety of channels, including webinars, videos, podcasts, and e-books.

Security professionals often feel that they are learning a new language while navigating the latest workplace trends. Use ASIS’s curated content to ensure that you are connecting powerfully—and successfully—with your teams.
DSX SECURITY AT YOUR COMMAND... AND IN YOUR HAND.

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

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

DSX STANDARD SYSTEMS FEATURES INCLUDE,

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

10731 ROCKWALL ROAD | DALLAS, TX 75238
888.419.8353 | DSXINC.COM

For product info #7 securitymgmt.hotims.com
AN AMENITY OF NECESSITY

A NEW SURVEY SHOWS THAT SECURITY REMAINS CRUCIAL FOR APARTMENT RENTERS—SOME OF THE OLD STRATEGIES (GATED ACCESS) REMAIN POPULAR EVEN AS THE NEW (MORE APPS) GAIN TRACTION.

BY MARK TARALLO

IS SECURITY TRENDY? It may seem an odd question. But consider the current residential apartment sector, where upscale rental buildings are competing for new tenants by offering increasingly luxurious amenities such as pet daycares, wine cellars, and movie screening rooms. A recent survey asked apartment renters which amenity they most desired, and amid all these intriguing choices the number one answer was...a security-based amenity.

“Gated access” was the most frequently cited amenity in the survey, chosen by 35 percent of respondents. It beat out such features as hardwood floors, rooftop terraces, and coffee shops. “App-controlled door locks” also made the top 10, chosen by 25 percent of respondents. The survey of 2,000 renters was conducted by RentPath and Egg Strategy in 2017 and 2018, and the results were released in October 2018.

Angie Amon, director of research at RentPath, says the survey reflects an unshakable reality in the apartment world: “It’s universal, the desire to feel safe and secure.” As evidence, she cites a renter focus group she attended, in which people were asked about factors involved in moving to a new apartment building. “Every single person talked about security and safety,” she says.

She adds that, in particular, the popularity of gated access is also being driven by more favorable economics. Currently, gated access communities “don’t necessarily have to be quote unquote luxury” developments—there’s a growing number of more moderately priced gated communities, which in some regions of the country are becoming popular. “They’re building them as fast as they can,” Amon says.

Apartment security expert Chris E. McGoey, CPP, says security has traditionally been one of the three most important factors when it comes to renting an apartment, along with location and price. McGoey, who conducts apartment security assessments as a consultant, has been a member of ASIS for nearly 40 years.

Moreover, gates in particular still have a powerful psychological effect for many, McGoey explains. Their prominence at the front of properties conveys a sense of safety to many residents. “If it can reduce the amount of traffic, it will filter out a percentage of people who would come in and take advantage of the property,” he says. And although an apartment community secured by a gate is “not Fort Knox,” McGoey adds that the gate still has the power to deter some potential criminals—if only as a psychological factor.

Another possible consideration driving the increased popularity of gated access apartment communities is demographic, says Mark Berger, president of the Securitech Group and a member of the ASIS Physical Security Council.

The gated access concept is an ancient one, Berger explains: “It all goes back to castles and moats and drawbridges.” But many of those now interested in renting are part of the Millennial generation and Generation X,
Young renters derive a certain comfort from restrictions on who can walk into their environment.

often raised in controlled, structured environments, compared with older generations more likely to run wild through the neighborhood as children. “The playdate generation has come of age,” he says, adding that many of these young renters derive a certain comfort from restrictions on who can walk into their environment.

Still, McGoey says that in one sense the growing popularity of gated communities is a double-edged sword. “The residents really like it. The developers like it, it gives the property more value. But what’s bad is the day-to-day maintenance,” he explains. In many situations, gates can be a “nightmare to maintain” because they are often hit or clipped by distracted and impatient drivers, and motorists who try to enter by tailgating, he says. Fixing damaged gates is not always easy or quick, so some communities may find them frequently disabled.

Apartment security experts seem to agree that the use of the second most popular security amenity in the survey, app-controlled door locks, is very much on the rise, driven by demographics and new technologies. Many Millennials rely on their smartphones, so using their phones to open their doors appeals, both McGoey and Berger say. “These are the people who, if they could surgically remove their left hand and replace it with a cell phone, they would,” Berger says.

The growing popularity of app-controlled locks is accompanied by increased use of other “smart home” devices that have a security component, Amon says. These include devices and apps that allow remote control of garage doors, thermostats, and other home components, as well as alarm systems and other monitoring devices.

Amon also notices a shift toward a greater acceptance of cameras as a security device in apartment communities. She explains that, in discussions among renters she has been privy to, concerns that cameras in a residential environment represent an invasion of privacy never seem to come up. “I’ve never heard anyone say that, ever,” she says. In her view, this acceptance has been driven by
Concerns that cameras in a residential environment represent an invasion of privacy never seem to come up.

increasing use of cameras in everyday life, ranging from traffic and intersection monitors to the common use of smartphone video. “It seems we are now almost expecting that cameras are everywhere,” she says.

Another factor behind this acceptance may be the physical evolution of camera design, McGoeysays. Designers are making them smaller and less noticeable. “It’s like the paint on the wall or the trim on the door—residents don’t give them a second thought,” he explains.

What will the near future hold for apartment security? Security devices that use artificial intelligence (AI) seem to be getting more use but, based on early indications, Amon senses a “lack of complete faith in that technology.” Part of this seems to be the annoyance factor of being misheard by the AI receiver: “It doesn’t understand me, so I might as well type it in,” she explains. And discomfort persists about the possibility of being recorded all the time by the device, she adds.

Berger sees a general growth in apps and remote devices. “There’s a lot of space for electronics to grow in apartments,” he says. On top of that, he expects more use of facial recognition for security purposes. “It might be kind of Star Trekky,” he explains. And as with cameras, pushback on such futuristic technologies over privacy concerns should be minimal among younger renters.

“This is the generation willing to type in their birthdate five times a day on their phones. They don’t worry about personal information,” Berger says. “I think they’ll be fine.”

WEAPON WEAKNESSES

The U.S. Department of Defense (DOD) is planning to spend more than $1.5 trillion to develop its portfolio of major weapon systems. Although the investment may result in a state-of-the-art deterrence program in the future, the weapons currently have a glaring vulnerability—they are relatively easy to hack.

Officials from the U.S. Government Accountability Office (GAO), which was asked to review the state of DOD weapon systems cybersecurity, recently ran some tests to see if they could hack any of the Pentagon’s weapons.

They could, without much difficulty. “Using relatively simple tools and techniques, testers were able to take control of systems and largely operate undetected, due in part to basic issues such as poor password management and unencrypted communications,” the GAO explains in its report, Weapon Systems Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities.

It’s likely that the testing revealed only a small number of the actual existing weaknesses. “In addition, vulnerabilities that DOD is aware of likely represent a fraction of total vulnerabilities due to testing limitations. For example, not all programs have been tested and tests do not reflect the full range of threats,” the report says.

It’s a disconcerting finding, considering that adversaries of the United States are developing increasingly sophisticated cyberespionage and cyberattack capabilities to target DOD weapons. The GAO found several reasons for these vulnerabilities.

CORPORATE SECURITY

BY RICHARD J. CHASDI. Praeger; abc-clio.com; 248 pages; $48.

THE LANDSCAPE for corporate security practitioners is changing. Globalization and rapid technology advances are forcing industry leaders to understand and deal with convergence now more than ever. Corporate Security Crossroads: Responding to Terrorism, Cyberthreats, and Other Hazards in the Global Business Environment takes a scholarly approach to drawing a “then and now” correlation to modern day issues that multinational entities are facing. It presents a macro view on relevant geopolitical matters that will help key policy and decision makers better understand the complex risks that are present in less-developed parts of the world.

Setting this book apart from others, there are many ties to modern and recent issues. The book is incredibly well researched, and Richard J. Chasdi uses this data to support his own assertions. Reference source material represents a significant amount of the overall content—the “Notes” section comprises nearly 25 percent of the book.

Case studies paint a clear picture for readers but do not represent a true global perspective. The inclusion and analysis of Western-focused incidents, along with the others, would have better supported the author’s attempt to present wide-reaching global business hazards.

Corporate Security Crossroads is an advanced text and an ideal publication for research and academic environments, as well as for companies and other organizations that focus largely on geopolitical matters. It is less relevant to CISOs and CISOs operating outside of a governmental or foreign affairs role.

REVIEWER: Pete Bernnitter is senior regional manager, Americas Security and Safety, at Dassault Systèmes. He is a member of the ASIS Investigations Council and serves on the technical committee for developing the Active Assailant Annex to the ASIS/SHRM Workplace Violence Prevention and Intervention Standard.
One is that the Pentagon’s weapons systems are increasingly dependent on IT. The amount of software in today’s weapons systems is growing exponentially and is embedded in numerous subsystems. But this dependence on software increases the weapons’ attack surface.

Similarly, DOD weapons systems are more networked and interconnected than ever before, and they are also connected to some external systems, such as GPS. These factors further increase vulnerability.

In addition, DOD has only recently made weapon systems cybersecurity a priority. Instead, for many years, DOD focused its cybersecurity efforts on protecting traditional networks, such as accounting systems. “Until around 2014, there was a general lack of emphasis on cybersecurity throughout the weapon systems acquisition process,” the report says.

This late-to-the-game approach will have long-term consequences, the GAO found. “Numerous officials we met with said that this failure to address weapon systems cybersecurity sooner will have long-lasting effects on the department,” the report explains. “Due to this lack of focus on weapon systems cybersecurity, DOD likely has an entire generation of systems that were designed and built without adequately considering cybersecurity.”

In the last few years, however, DOD has made progress on some new weapon cybersecurity initiatives and policies. Given this, GAO urged the DOD to press forward with these efforts. “To improve the state of weapon systems cybersecurity, it is essential that DOD sustain its momentum in developing and implementing key initiatives,” the report says. Finally, GAO pledged to continue to evaluate the issue.

To read the apartment survey and the GAO report, see SM Online.

SEXUAL HARASSMENT

Of those who reported that they experienced sexual harassment in the workplace, an overwhelming majority never filed formal charges.

Percentage of respondents who never filed formal charges:

99.8%

SOURCE: Employer’s Responses to Sexual Harassment, Center for Employment Equity, December 2018

What is Your Company or Agency Doing to Protect Your Communications & Information?

- EXPERTS - CORPORATE & GOVERNMENT COUNTERESPIONAGE
- TRUSTED - ACCREDITED GLOBAL TSCM PROVIDER
- EXPERIENCE & TRAINING – 25+ YEARS
- TECHNOLOGY – CUTTING-EDGE EQUIPMENT & PROCESSES

SCHEDULE YOUR TECHNICAL & PHYSICAL TSCM SWEEP NOW

TSCM America
Protecting America’s Privacy™

Nationwide Services 866.448.3138 | www.tscmamerica.com
info@tscmamerica.com

For product info #9 securitymgmt.hotims.com
TOP ANGST: CYBER AND TRAVEL

THE OVERSEAS SECURITY ADVISORY COUNCIL (OSAC) BRINGS TOGETHER THOUSANDS OF SECURITY PROFESSIONALS FROM U.S. ORGANIZATIONS TO EXPLORE GLOBAL SECURITY ISSUES. THE TWO HOTTEST TOPICS TODAY? CYBERWARFARE AND TRAVEL RISK.

BY MICHAEL GIPS, CPP

NOW IN ITS 33RD YEAR, OSAC brought together thousands of security professionals from U.S. organizations to explore global security issues and challenges, hear from corporate and government thought leaders, and receive regional briefings from OSAC analysts in November 2018. Topics ranged from social media disinformation in India and emerging autonomous threats to creating a contemporary operations center and building a 21st century security program. But two topics stood out: cyberwarfare and travel risk management.

Cyberwar. In the waning days of the Second World War, U.S. President Franklin D. Roosevelt, U.K. Prime Minister Winston Churchill, and Soviet Premier Joseph Stalin met in Yalta to demand Nazi Germany’s unconditional surrender. Stalin emerged from that conference with control over Eastern Europe. The Soviet Union’s collapse half a century later eviscerated Russia’s sphere of influence, but the country is dramatically reasserting its claim as a world power player largely through its vast cyberwarfare activities. Russia’s return to prominence, the diversification of nation-state hacking among new actors, and the cyberthreat to both governments and businesses emerged repeatedly as areas of grave concern at the OSAC 33rd Annual Briefing, held in Washington, D.C.

Russia is effectively out to create a “Yalta 2,” said Heather Conley, a senior vice president at the Center for Strategic and International Studies, during a session on new-generation warfare. Russian President Vladimir Putin’s objective is to “retain his power structure, restore Russia as the United States’ equal, and stave off long-term Russian decline,” Conley said.

Cyber activities are key to Russia’s reassertion of dominance in Eastern Europe and beyond, where it is deploying a combination of cyber activities, including economic investment, politicized nongovernmental organizations, proxy groups, and political patronage. For their cyber activities, “Ukraine is the lab,” Conley said. Putin is looking to not only identify which techniques are effective, but also to gauge the West’s reaction, she said. A main objective: “Get U.S. citizens to lose confidence in elections” and other democratic institutions.

Of course, Russia is far from the only combatant on this virtual battlefield. China and Iran are also prevalent sources of advanced persistent threats, with instances of unauthorized and stealthy access to a network for an extended period of time. Kevin Mandia, CEO of FireEye and the author of the groundbreaking 2013 report documenting the Chinese military’s cyberattacks on 14 Western organizations, noted in a separate OSAC session that Iran has been vastly improving and increasing its cyber aggression. Even Vietnam has joined the fray, he said.

“Eighty percent of breaches we respond to are corporations hacked by nation-states,” Mandia said. And...
almost every breach reflects geopolitical conditions or developments.

Given the vast resources of Russia, China, Iran, and countless other nation-state cyberwarriors, how can corporations mount their relatively meager resources in defense? Emily Heath, the CISO of United Airlines, who presented on Mandia’s panel, noted that the airline emphasizes sharing intelligence between its physical and cybersecurity departments. “Almost every incident has a cyber component today,” she said. Boeing Senior Director Scott Regalado added that security executives should be closely following the news and proactively reaching out to the C-suite, especially if a development might somehow involve their company or industry.

Panelists stressed that tabletop exercises are critical, as is creating an enterprise-wide information security committee. “Consider preparedness for media response as well as internal response,” advised Heath. Preplanning is essential because breach-disclosure regulations put victimized organizations on the clock.

Defense starts with good cyber hygiene, security consultant Stevan Bernard told Security Management following the panel. He is in a good position to know: Bernard previously served as executive vice president for Sony Pictures Entertainment, which was the victim of a high-profile breach believed to have been committed by the North Korean government. The key is to change behavior, which is best accomplished through personalizing the message, he said.

For example, companies can encourage cyber vigilance by explaining how employees are personally at risk and how they have assets worth protecting. Good home habits transfer to the workplace. In addition, companies might consider providing employees with dedicated computers—that aren’t connected to the corporate network—for personal Internet browsing. Corporate cybersecurity basics should include 12-character passwords that must be changed every 90 days, two-factor authentication, regular encryption and purging of data, and phishing-education campaigns. Yet despite increasingly sophisticated attacks and the growing involvement of state actors, Bernard said, “the biggest vector is still email.”
Travel. In early 2018, due to work commitments, a U.S.-based corporate executive was unable to join his wife and two teenaged daughters at a resort on the Riviera Maya in Mexico. He felt comfortable sending them, despite general travel warnings issued by the U.S. State Department and highly publicized media accounts about tourists caught in gang crossfires, because the incidents were remote and isolated, and he was familiar with the airport, the transportation, the travel route, and the resort.

Additionally, transportation to and from the resort had been set up in advance, his family followed good travel security practices, and the executive had assets on the ground to assist if necessary.

Happily, the family had a great time and returned safely. But during their stay an American tourist was killed only a few miles from their resort. In the aftermath, the CEO questioned the executive’s judgment, citing the murder, media reports, his recall of travel advisories for Mexico, and third-hand horror stories of trips gone awry. What the CEO lacked was an objective assessment of the risk.

Many organizations turn to travel risk management firms to drill down into specific locations, routes, times of year, and other factors to protect their traveling staff, students, and volunteers. But OSAC has recently introduced a free matrix tool available to its constituents that enables a nuanced view of travel risk for specific locations.

With the OSAC framework, a user selects a country and completes six modules related to risk—crime, terrorism, civil unrest, environment, health, and operational/information security. For each of these modules, companies answer a series of questions, typically with checkboxes or prepopulated answers contained in a pull-down menu.

OSAC provides the links to objective data, such as the types of natural disasters that have occurred in the last 24 months, while companies answer many of the questions based on their interests in the country and their own risk tolerance.

Despite increasingly sophisticated attacks...the biggest vector is still email.

For example, under the “civil unrest” module, a travel security manager might identify recent civil demonstrations and gauge the prospect for future incidents, as well as discern the underlying cause, average size, and participant makeup of demonstrations. The manager can also determine their frequency, location, and the frequency and nature of any attendant violence. In one possible example, the framework can help a travel manager conclude that demonstrations reflect opposition to host-country politics or practices, average between 500 and 1,000 participants, occur in areas where the company has significant operations, and spill over into looting and rioting that local security forces cannot control. That information would help inform the company’s security practices, for example choosing alternate travel routes or rescheduling visits.

At the end of the framework is a section on countermeasures and guidance. It includes space for travel security managers to enter risk summaries, travel requirements, traveler guidance, and transportation countermeasures.

Questions for the matrix were chosen based on their ability to provide clarity on the overall security picture, says OSAC Regional Analyst Morgan Dibble. For instance, to gauge crime, organizations frequently consult homicide rates, which most nations report. But homicide rates—which can be underreported, unavailable, or manipulated—do not truly reflect overall crime rates. Therefore the “crime” module also includes common crimes such as smash-and-grab theft and drink spiking, popular scams, discernible targeting patterns, and police response.

OSAC constituents can access the tool via the secure OSAC website.
WHY IS ABLOY® SUPER WEATHER PROOF THE WORLD’S BEST PADLOCK?


To secure critical locations in severe and rapidly changing weather, railway professionals in Asia were urgently searching for locks they could rely on in all conditions. They turned to Abloy Oy, a Finnish company with decades of experience in listening to customers and developing high quality locking systems that meet their needs.

ABLOY SUPER WEATHER PROOF (SWP) padlocks were born - a locking solution in which the components are extremely well protected to ensure operation in all conditions. Security is guaranteed even with regular exposure to extreme heat or cold, storm-driven salt water or fine desert dust.
I’ve always known that with the normal proximity cards there are vulnerabilities,” says Chris Christensen, director of cybersecurity and infrastructure protection for the State of Michigan. “On YouTube, you can figure out how to clone and copy those proximity cards quite quickly and efficiently and be able to get to places where you’re not supposed to.”

Thankfully, in the case of this security breach, it was a paid vulnerability test, in which a penetration testing team was tasked with finding ways to infiltrate the building’s security.

The test exposed a problem with the state’s physical security, which is important, according to Christensen, because of the growing emphasis on cybersecurity over the past decade. “We have a lot of firewall rules, we’re making sure applications are secure, but what about when somebody takes a key and copies it and walks into a building, a secure site, and then has access—what are we doing about that?” Christensen asks. “So, I think that’s a big thing that we’re missing in security. We’re trying to protect the castle from the inside, and we’ve just opened the front door for people to walk in.”

Tasked with access control for approximately 40 government buildings, including facilities in the capital city of Lansing and on Mackinac Island where the governor’s residence is located, Christensen notes that physical security can’t fall by the wayside as departments focus more on digital threats.

After the penetration test, he wanted to find a more-secure, cutting-edge solution to access control. “Once that happened, I knew that we needed to do something that was more safe and secure, and that had a little bit more of the ‘wow’ factor,” he says.

About two years ago, the state turned to the Vector Occupant app from Honeywell, a Bluetooth-enabled access control system that stores user credentials on individuals’ smart devices. Users download the Vector app from any smartphone application store and enter a code sent by the state of Michigan. Since the beginning of 2018, all new card readers installed at government buildings are equipped with Vector.

Having access via one’s phone is preferable to carrying around a traditional proximity card for several reasons, Christensen notes, including higher reliability and usability for the end user.

“When you go to work in the morning, if you’re at the first stop sign, and you look down and your phone’s not there, you turn around and go home and get your phone,” he says. “If you don’t have your card, you go all the way to the office and then go try to get a loaner card or have somebody else sign you into the building.”

He adds that the potential for sharing and swapping access control
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
we’re trying to protect the castle from the inside, and we’ve just opened the front door for people to walk in.

Alarms from door access panels also alert security when a person has entered a secure room at unusual hours. “We had an alarm go off on one of our Vector doors at 2:00 a.m., but it was actually the detective sergeant going back in and putting some more evidence in after a long day of protests,” he says. “So, it was valid, but we did look into that.”

Authorizing access for users is quick and simple, as is provisioning conditional, temporary access for contractors and employees who don’t normally have access to a certain building. “We’ve done that on various employees when they’ve needed access. So, let’s say the data server room at Michigan State Police headquarters had to be updated,” Christensen explains. “I’ll get the access for the individuals for a 24-hour time period, and after that time they don’t have access.”

As the person provisioning access, he says Vector offers added peace of mind that no one walks away with a card that they shouldn’t have. “It made it really easy for me, because by the time the week was done I forgot he was in the system,” says Christensen. “So, for the credentials to expire and him to not have access, I didn’t have to worry about it again.”

Eventually the state also hopes to take advantage of the building intelligence function of Vector—via the app, users can report their comfort level within buildings—if they’re too hot or cold; whether a conference room needs more chairs; and more. “At our agency, we’re all about trying to do customer service,” Christensen says. He adds there’s a cost-saving benefit to the building intelligence. “Knowing where people have come or gone, or where they’re moving with their Bluetooth being activated—it will help us save and use the power when we need to.”

FOR MORE INFORMATION: JULIO AMPUERO, JULIO.AMPUERO@HONEYWELL.COM, WWW.HONEYWELL.COM, 480.606.9569

For more information: Julio Ampuero, julio.ampuero@honeywell.com, www.honeywell.com, 480.606.9569

Applications accepted online only, 1 February – 30 April 2019
Visit asisfoundation.org/2019 to learn more and apply

Apply now

Career Development Scholarships underwritten by Securitas
New for 2019! IFPO CPO/CSSM scholarships
More than 40 scholarships will be awarded for certification and higher education

We’re trying to protect the castle from the inside, and we’ve just opened the front door for people to walk in.

Alarms from door access panels also alert security when a person has entered a secure room at unusual hours. “We had an alarm go off on one of our Vector doors at 2:00 a.m., but it was actually the detective sergeant going back in and putting some more evidence in after a long day of protests,” he says. “So, it was valid, but we did look into that.”

Authorizing access for users is quick and simple, as is provisioning conditional, temporary access for contractors and employees who don’t normally have access to a certain building. “We’ve done that on various employees when they’ve needed access. So, let’s say the data server room at Michigan State Police headquarters had to be updated,” Christensen explains. “I’ll get the access for the individuals for a 24-hour time period, and after that time they don’t have access.”

As the person provisioning access, he says Vector offers added peace of mind that no one walks away with a card that they shouldn’t have. “It made it really easy for me, because by the time the week was done I forgot he was in the system,” says Christensen. “So, for the credentials to expire and him to not have access, I didn’t have to worry about it again.”

Eventually the state also hopes to take advantage of the building intelligence function of Vector—via the app, users can report their comfort level within buildings—if they’re too hot or cold; whether a conference room needs more chairs; and more. “At our agency, we’re all about trying to do customer service,” Christensen says. He adds there’s a cost-saving benefit to the building intelligence. “Knowing where people have come or gone, or where they’re moving with their Bluetooth being activated—it will help us save and use the power when we need to.”
The role of today's Chief Security Officer is changing in extraordinary ways. In addition to assessing risk across the enterprise and supply chain, it is essential for the CSO to engage and advise executive leaders on best practices and SOPs for business continuity and strategic leadership in all disciplines.

Join leading security executives from the largest and most influential organizations for three days of intensive idea sharing, problem solving, and relationship building you won’t want to miss!

Learn more and register at asisonline.org/CSOSummit. This event is open only to CSO Center members and those eligible for membership.
How did Mallory and the agent initially connect? Via LinkedIn, when the operative—called Michael Yang—reached out to Mallory, posing as representative of a PRC think tank—the Shanghai Academy of Social Sciences—and requested to meet with him.

Mallory ended up traveling to Shanghai with eight classified documents, which he gave to Yang and his supervisor during a meeting. When Mallory returned to the United States, he was detained by U.S. Customs and Border Protection (CBP) for a secondary search and interview.

During the interview, Mallory claimed he had traveled to Shanghai for business and met with an individual he knew through his church to consult on anti-bullying and family safety development. He also checked on a form from CBP that he was not carrying more than $10,000 in U.S. or foreign currency.

Upon a search of his belongings, however, CBP found $16,000 in Mallory’s carry-on bags. The FBI later interviewed Mallory, who told agents that he had been contacted on social media by a Chinese recruiter, had phone interviews with that recruiter’s client, and traveled to Shanghai on two occasions to meet with the recruiter’s boss.

Mallory was ultimately arrested, charged, and convicted of conspiracy to deliver, attempted delivery, delivery of defense information to aid a foreign government, and making material false statements.

“This trial highlights a serious threat to U.S. national security,” Nancy McNamara, the FBI’s assistant director in charge of the Washington Field Office, said in a statement. “Foreign intelligence agents are targeting former U.S. government security clearance holders in order to recruit them and steal our secrets.”

U.S. Director of the National Counterintelligence and Security Center William Evanina went on record in the summer of 2018 to discuss what he—and the U.S. intelligence community—had been seeing on LinkedIn. In an interview with Reuters, Evanina explained that China was conducting a campaign to target thousands of LinkedIn members at a time to recruit Americans with access to government and commercial secrets.

Evanina declined to say how many of these recruitment accounts U.S. intelligence had discovered or how much success China has had in using them.

While individuals and organizations have been using social media to target users for government secrets or corporate intellectual property, LinkedIn is especially attractive for social engineering, says James Car-
From deciding whether to accept a connection request to displaying contact information on your profile, you control your interactions on LinkedIn.

Nefarious actors can use LinkedIn for a honeypot attack, like they might use a dating site, to appeal to that feeling of being appreciated and wanting to connect with someone to obtain information about their business or level of access.

This is a tactic that Don Aviv, CPP, PCI, PSP, president at Interfor International—an investigation and corporate intelligence firm—says he sees others using against his corporate clients.

“When you break it down to its bare bones, utilizing LinkedIn is another attempt at using social media to engineer an attempt at fraud, theft of proprietary information, whatever the company does for a living,” Aviv says. “We work for Fortune 500 companies that have been hit by these attacks...and the goal is to figure out who is reaching out and why.”

Besides espionage, one of the most prevalent reasons malicious actors are targeting individuals on LinkedIn is to find out more information about a company’s financial protocols and procedures so they can carry out CEO or CFO spoofing attacks.

For instance, a fraudster might look to connect with various individuals in a company’s finance department to learn who is responsible for initiating wire transfers and when that individual might be traveling.

Aviv himself set up a test to teach Interfor employees and clients how this works. He created a fake profile for himself on LinkedIn, connected with other individuals, and shared his travel plans on the account.

Shortly after Aviv left on his fake trip, a fraudster sent an angry email that appeared to come from Aviv to Interfor’s finance director. The email had information about the company’s vendors, contained an invoice requesting payment, and contained a modified wire transfer code to use for the transaction.

Aviv says he sees roughly six or seven requests per month from companies that received similar emails and are looking to find out who is perpetuating the fraud and how to prevent it.

This type of fraud is also more prevalent in the Asia and Pacific regions, as opposed to the United States and Europe, where Aviv said there is more awareness of CEO and CFO spoofing.

“It has become much more publicized—a lot of the compliance departments are catching on,” Aviv says. “In Asia, there’s a demographic difference. A lower-level employee will be much more reluctant to not follow that transaction order.”

Security Management reached out to LinkedIn to discuss the matter, but the company declined an interview. Instead, spokesperson Anne Trapasso sent over three blog posts by the company on cultivating trust, fake account detection, and reporting spam, inappropriate posts, and abusive content.

“When you’re on LinkedIn, you want to know that you’re talking to real people, you feel safe, and you’re engaging with professionally relevant content,” wrote Madhu Gupta, director of product management, trust, and security for LinkedIn in a post.

DIGITAL INVESTIGATIONS

BY JASON SACHOWSKI; CRC Press; crcpress.com; 348 pages; $79.95.

Forensics has long been a crucial part of law enforcement and police investigations. It’s also an important part of the judicial system, and one of the first things a defense attorney will do is to try to find ways to get evidence dismissed. When it comes to digital forensics, the stakes are equally high.

In Digital Forensics and Investigations: People, Process, and Technologies to Defend the Enterprise, author Jason Sachowski creates a helpful reference on how to effectively use digital forensics in a manner that can stand up in court in front of a judge, jury, and aggressive defense attorney.

Forensics does not exist in a vacuum, and as the title implies, people, process, and technologies must work together to ensure that forensics can withstand scrutiny. The book shows how to integrate those facets within an organization.

Practical methodologies and strategies can immediately be used to create an effective forensics program. While there is no shortage of texts on how to use the many forensics technology tools, this book stands out by effectively detailing how to make all of the various elements of a forensics program realistically work together.

The author is the director of cyber and security investigations at a large bank and brings significant real-world experience to the book. Those looking for a tactical guide to the topic will find it here.

REVIEWER: Ben Rothke, CISSP (Certified Information Systems Security Professional), PCI, QSA (Qualified Security Assessor), is a senior security consultant with the Nettitude Group.
LinkedIn is especially attractive for social engineering.

After Evanina’s statements. “One of the most important ways we do this is by empowering you to control your LinkedIn experience. From deciding whether to accept a connection request to displaying contact information on your profile, you control your interactions on LinkedIn.”

This control includes deciding how to present yourself on LinkedIn—the content of your profile, posts you make, and who can see this information is visible—and vetting your community of connections, Gupta explained.

“Examples of these features include filters for who you can receive messages from and invitation controls that allow you to accept, deny, or ignore a connection request,” she wrote.

Mark Folmer, CPP, vice president, security industry, TrackTik, is a robust social media and LinkedIn user who joined the network roughly 10 years ago. He does not share a lot of personal information in his profile but does have his phone number and main business email posted. Folmer also regularly receives what he would call “fishy” connection requests from other LinkedIn users.

“It happens all the time—the standard no personalized message, just an invite from x, y, or z, with one connection or no connections in common,” Folmer says.

Other signs that a profile might be fake are connection requests from someone based in a country TrackTik does not do business in, an incomplete profile, titles that do not seem to line up with the general business market, or someone whose employment record jumps around.

“If it’s too good to be true, someone who sounds like they would be the perfect connection—why are they writing to me from Romania?” Folmer says.

“Why are they interested in connecting with me?”

Instead, Folmer says he will likely connect with those who are in the same industry, have connections in common, are ASIS International members, or include a personalized message in their connection request.

“When I reach out to someone—especially someone I haven’t met yet—I try to put some context into the invite, such as, ‘Hey these are the people we have in common, certification, or I’ve seen you write about this and I’d like to meet,’” Folmer explains. “It’s my way of saying...”
I’m a real person and I’m not going to sell you something or try to skim something off of you.”

These are good rules to follow, and both Carnall and Aviv say employers should discuss best practices for LinkedIn hygiene with employees to help prevent them—and the company—from being targeted by malicious actors.

For example, Carnall suggests creating guidelines that prohibit discussing secret projects on social media or posting about budgetary amounts.

“Looking from a criminal perspective, that provides too much information for people to socially engineer,” he says.

And if an employee is posting information online that could make the company vulnerable, Carnall says security and human resources should speak with the employee to use it as a teaching moment.

“HR should incorporate a conversation about social media as part of any onboarding for any new employee,” he adds. “It’s important for the organization to work with the employee; there’s a balance of promoting themselves as an individual to be proud of themselves and advertise to others the work they and the company are doing.”

LinkedIn has a process for reporting suspicious activity and fake user accounts, which Carnall says works well if you are able to establish that a malicious user is posing as a real user.

He also recommends that visible people, such as executives, create legitimate accounts on social media services in their own name to claim that name and “because it’s much easier to have a site take action” if you are a user.

And approach all connection requests with a certain level of skepticism, Aviv says.

“Look at their profile and ask why they are reaching out to you—and be willing to ask them via the message function,” he adds. “When you challenge it, they may go away. And the people who talk to you, you’ll be able to figure out if they’re up to no good.”

ELECTION SECURITY

Following the 2018 midterm elections, most Americans were confident that election systems in their state were secure from hacking or technological threats.

**Level of confidence in security of state election systems:**

- **Very confident**: 29%
- **Not too confident**: 15%
- **Somewhat confident**: 49%
- **Not confident**: 6%

**SOURCE:** Most Voters Have Positive Views of Their Midterm Voting Experiences, Pew Research Center, December 2018.

In its role as an accredited Standards Developing Organization (SDO), ASIS seeks experts from around the globe to participate in upcoming projects throughout the year.

By volunteering in standards developing activities, ASIS members contribute their knowledge to others who are making decisions that could affect your business, your processes, and your bottom line. **Shouldn’t you be involved?**

Learn more about the work we are doing at asisonline.org/standards or email us standards@asisonline.org.
Security Management conducted interviews with three prominent security professionals in the retail sector to gauge the current landscape of retail security operations: what’s important, what’s causing headaches, and how are they successfully fulfilling their mission? Alan F. Greggo, CPP, CFE, senior regional asset protection manager, Microsoft Corporation; Peter Chie, CFI, operating vice president, asset protection and risk management, Bloomingdale’s; and Kathleen Smith, CFI, vice president of loss prevention, Albertsons/Safeway Inc. are all members of the ASIS International Retail Asset Protection Council and have more than 75 years of combined security experience.

On workplace violence being a primary focus:
Greggo: “When you look at it through risk assessment, I know what my primary assets that need to be secure are: the people who work in my stores and the customers. And a primary risk is that acts of violence can hurt them. We’re going to do everything we can to reduce that risk.”

Chie: “When you think about the retail environment and how it has evolved over the last decade, the typical mall environment has shifted from a place where people would go to shop for clothing or other merchandise to becoming more of a lifestyle experience. You’re seeing a lot of anchors going away and being replaced with higher end restaurants and movie theaters—lifestyle types of venues being created in malls to transform shopping spaces into multipurpose destinations and increase customer traffic. For the domestic and international terrorist, they see this and think ‘This is a group of soft targets. I can do a lot of damage to a lot of people all at once.’”

On security’s role in preparing retail staff for potentially violent situations:
Smith: “We have some computer-based training that all employees are required to complete, and that is what really sets the baseline. After that, you periodically reinforce what is in the training. When
there is an incident at a location, it’s a learning experience you talk through at that location, but then you can use that at other locations. And it’s not just that, things that are in the news at the time can rise to the top and be a good source to reinforce the security messaging that the training provides.”

**Greggo:** “Keep in mind, in retail, employees of the store are focused on sales, their goals, and on engaging and creating the customer experience. The threat of violence is not the first thing on their minds. The training is designed to give them something to fall back on when a situation occurs.”

**On working to mitigate the effectiveness of organized retail crime, or ORC:**

Greggo: “ORC is still a big cost to retailers. We have some techniques that are helping—the organized retail crime associations, or ORCAs, for example. These are partnerships between retailers in an area together with law enforcement and the courts. They get together regularly, discuss the issues affecting their area, learn from each other, and learn how the three components can most effectively work together to prevent criminals from being successful. These associations have had quite an impact. Of course, criminals are always changing their methods and they’re always able to recruit people to assist their efforts. It is a constant cat and mouse game.”

Chie: “The trends in merchandise theft and methods they’re using have actually become less sophisticated in my opinion. Many organization’s security protocols are out there on YouTube, Google, or the dark web: they know if a retailer has a hands-off policy; they know if the security representative can’t go past a certain point outside the store. And they’re using that knowledge against companies. Additionally, rather than trying to locate and sneak out with a few high-value items, retailers are seeing more grab-and-run type of activity, where three or four bad actors at the same time are grabbing a bunch of coats, for example, and running out the door. This more aggressive approach is harder to mitigate. We have data analysis tools that identify patterns and analyze when and where someone might try this. We communicate with other stores in the area. We’re getting better at being able to predict some of the things that might occur and prevent them from happening, but criminals are always changing their methods, working to be creative, so it requires constant vigilance.”

Smith: “We try to build a predictive model based on a lot of different data points, from social media posts to crime data to individual store reports. We utilize all the information we can get to try to predict the types of criminal activity that are likely to occur in a given area and put procedures in place to protect against them. We always need to be changing it up, because they’re always changing it up. Our goal is to prevent negative events from happening.”

**On the relationship between store and corporate retail security:**

Smith: “You want to become a partner for the retail directors. You want to cultivate a relationship where you as security are not the bad guys, the ones trying to restrict what they do or are only there to enforce rules and regulations. You want a proactive mindset that is solutions focused. We share the same goals, so if we enter a dialog and come to a balanced solution together, that’s going to be win-win.”

Greggo: “We need to position ourselves as being trusted advisors to the retail business. When risks occur in a retail setting, we want to be the first people that leadership and store managers think of. We want them to reach out to us with what they see and collaboratively work on a plan to address the risk, a plan that makes sense for them and protects the business. It’s not us dictating. It’s us listening to the stakeholder knowledge and providing expert security and protection feedback to reach an agreed-upon solution.”

**On things they are on the watch for or trying to accomplish:**

Smith: “Technology is rapidly changing the world of retail. Just think of all the new and developing ways people are shopping and the number of new mobile pay solutions that are being used. Every new development is a potential opportunity that thieves will work to exploit. Staying ahead of that game while wanting to provide customers with the level of service and access that they want is a real challenge. Security needs to be involved with IT and service providers to a higher degree than before.”

Chie: “We use and employ a lot of different types of resources, from access controls to cameras to data analysis. But the single most important resource—without a doubt—is our people. Whether it is workplace theft, a data breach, workplace violence—in all security situations, our people are our number one asset. We have a very robust training program and we work to include them as partners. The key to it all is getting them to understand just how important they are. If we have a gap, if there is an opportunity for someone to take negative action, a well-educated workforce is our best defense against it and our best proactive resource to identify and help us close the gap before there is a negative impact to the organization.”

Greggo: “I think it’s an ESRM [enterprise security risk management] approach. Security is not a static function. It’s constantly changing and so we need to take a cyclic approach where we are constantly identifying our assets, assessing risks, and devising ways to best protect those assets from the risks. We’re doing two things: we are seeing and responding to threats, but we’re also trying to prevent those threats from ever arising in the first place. If we are collaborators across the organization, working with associates on the floor a well as the leadership of the company, that’s how we proactively create a safe, secure environment that positions the company to reach its goals.”
The ECL-230X-TDB is a heavy-duty, easy to install three-bolt multipoint lock whose construction takes panic hardware to a whole new level of toughness and eases your back-door security worries. It is designed with a larger deadbolt that goes deeper into the frame than other locks in the category. Connecting rods are solid steel, rather than the less reliable hollow rod/cable construction. Life safety and code compliant, the new Detex ECL-230X-TDB serves as both panic hardware and a maximum-strength locking device.

The ECL-230X-TDB includes a photoluminescent sign available in more than 10 color/language combinations, 100 decibel alarm and 3 locking points per door.

Combining the ECL-230X-TDB with Detex’s DX Bolts provides an additional line of defense against break-ins via additional locking points. Even if the exterior door hinges are compromised the DX bolts keep the door locked and secure. These passive deadbolts are easy to install and offer another layer of attack resistance.

How tough is the ECL-230X-TDB? Independent laboratory testing proves a door secured by the ECL-230X-TDB, and when combined with 3 DX Bolts can withstand 16,000 lbs. of pull force.

Add suffix DX3 (ECL-230X-TDB-DX3) for 6 locking points for even stronger security. Single- and double-bolt and weatherized models are also available. Optional accessories include hinge side locking bolts and inside pull handle.

Other 230X models include ECL-230X (Dead Bolt Only), ECL-230X-W (Weatherized Dead Bolt), ECL-230X-TB (Top and Bottom Bolt), ECL-230X-W-TB (Weatherized Top and Bottom Bolt), ECL-230X-TD (Top and Dead Bolt), ECL-230X-W-TD (Weatherized Top and Dead Bolt), and ECL-230X-W-TDB (Weatherized Top Bolt, Dead Bolt and Bottom Bolt).

Almost all hardware and accessories can be customized with different finishes, colors, sizes, and more.

Visit www.detex.com/230X to see what the ECL-230X can do for you.
License-Free Analytics with an Open Platform

Hanwha Techwin’s high performance Wisenet 5 chipset technology helps you profit from leading edge analytics for retail spaces both large and small for a complete end-to-end business solution.

- Tampering
- Enter / exit
- Virtual line
- Heat map
- Appear/ disappear
- Face detection
- Motion detection
- Audio classification
COVER STORY | BY MARK TARALLO
“Hard skills will get you the interview—soft skills will get you the job.” David Lammert, a 17-year veteran of security industry recruiting and current president of Pinnacle Placements, is a big believer in this adage. And he’s not the only one.

“We have all seen situations where the decision to hire—when two or more candidates present the same level of hard skills’ strength—is made with soft skills as the differentiator,” says recruiter Rebecca Bayne, the president of Bayne Consulting & Search Inc. who specializes in staffing the security integration space. “It triggers the gut-level instinct of the hiring manager and determines who will get the offer.”

“And soft skills,” Lammert adds, “will also determine how well you perform in the job, and how long you do it.”
Other recruiters are on the same wavelength as Lammert and Bayne when it comes to the importance of soft skills. Although hard skills like specialized security knowledge and technical expertise in an industry subsector are still essential, a successful leader needs a broad soft skill set to navigate different managing situations, recruiters say.

Given the importance of soft skills, Security Management asked five industry recruiters to discuss which skills they believed to be most crucial for security managers both current and aspiring. In these discussions, two broad soft skill sets—communication ability and emotional intelligence—came up time and again. Recruiters explained how these skills apply to specific managerial situations. They also shared some general employment trends and discussed the soft skills of the future.

Communication
For many recruiters, communication ability reigns supreme when it comes to soft skills.

“The most important soft skill is communication. It’s the foundation of every other soft skill,” says Jane Snipes, managing partner at NorthStar Recruiting.

“In my experience, communication skills are paramount to one’s capability to execute and deliver the day-to-day requirements of leadership and having oversight for a team, small or large,” Bayne says.

In Lammert’s view, communication skills are an umbrella that covers several individual talents that have many applications, both inside and outside the firm.

“It's such an important skill set—there’s so much interaction internally [in a company],” he says. “It covers speaking, active listening skills, presentation skills, and more.”

For example, a security manager’s speaking and conversation skills will be a huge asset in working with vendors and external business partners outside the company, as well as technical staffers, C-suite executives, and the CEO within the firm.

“In this fast-paced business environment, the ability to communicate clear and concise messages is crucially important,” Lammert explains.

Another key asset under the communications umbrella is the ability to be an effective storyteller. For an aspiring security manager, the value of this skill begins in the interview—the ability to communicate and frame one’s career progression as a purpose-driven narrative that is gaining momentum is “critically important for a successful candidate,” Lammert says.

After the manager lands the job, storytelling continues to be an asset. “It also helps you become an influencer wherever you are in the organization,” he adds.

Communication skills are also crucial for a manager in working with direct reports, recruiters say. Successful managers have a desire to coach, facilitate, and develop talent, and this takes continual—and sometimes nuanced and sensitive—communication.

“In general, those who achieve the greatest success in their careers have a genuine interest in those around them and are skilled in communicating,” Snipes says.

For years, employee surveys such as the ones taken by the Gallup company have found versions of “I don’t like working for my boss” as the most common reason for people leaving a job.

Although there may be various reasons why a manager is disliked, a common one stems from the manager’s failure to adequately communicate how valuable an employee’s contributions are. The employee winds up feeling undervalued and unappreciated, Snipes says.

“People don’t leave companies, they leave managers, and the common factor lacking in those managers who chase away great talent is the ability to genuinely appreciate the value an individual has to the company and to consistently communicate that value,” she explains.

For managers, the lesson here is not only that communication skills are vital, but that they need to be consistently used. Sometimes, otherwise articulate managers will fail to communicate due to being too self-absorbed—they are occupied with their own career advancement and impressing the organization’s senior leaders, rather than attentive to their direct reports. “Many managers focus on themselves instead of serving those they lead,” Snipes says.

Finally, there’s another communication-related skill that’s a key asset for security managers—the ability to establish a safe space for honest two-way communication, says Kevin Spagone, vice president of Reitman Security Search/Reitman Personnel, Inc.

This type of communication needs to be embedded in the company’s culture, so that employees feel comfortable in offering honest views without fear of reprisal or relationship damage, he explains. Not only will this help employee retention, it will also help the firm’s reputation among potential employees, which will help recruitment efforts.

“Leaders who foster a culture where open, honest two-way feedback is the norm,” he explains, “are savvy enough to realize that this gives them a competitive advantage in the marketplace.”

Emotional Intelligence
Recruiter Stephanie Campbell of Security and Investigative (SI) Placement, LLC, finds that, besides
communication skills, emotional intelligence has become an important attribute for candidates in the current security management job market. “I am finding more and more interest in that skill set,” she says.

Emotional intelligence (often abbreviated as EQ) is the ability to perceive another’s emotions, reactions, and perspective, and to handle interpersonal relationships judiciously and empathetically. In the world of the security manager, it has many applications, recruiters say.

Campbell illustrates by relating a question she asks clients when trying to go beyond the job description to get a strong handle on what type of candidate would be a good fit.

“When we’re working with a client, we will sometimes ask, ‘What is it that’s not in the description that you are looking for?’” she says. “What’s that extra bit, that’s sort of between the lines?”

The answer is often “a lot of EQ skills.” These include working well as a teammate, empathetic listening, building consensus, and an ability to be persuasive and to motivate.

Security professionals are rarely required to answer the question, “Why are we doing this?” she says. Emotional intelligence is a huge asset for a manager who is trying to explain this in such a way that will motivate teams to embrace initiatives, she continues.

EQ is also an asset in the interview itself, because it helps candidates demonstrate their value, Snipes adds.

“The high EQ ones are fine-tuned to how they are perceived,” she says. “They’re not just leaning on their laurels. They have actively done the research on the company, and so they can give examples of potential contributions that are directly relevant…. They are making really good impressions.”

Lammert is also convinced of the value of emotional intelligence, and says it bolsters a manager’s communication skill set.

For example, managers with high EQ are aware of their audience; they know that different employees have different learning styles and interests, and they can tailor messages and delivery to fit each employee.

“One case may call for more of a visual message, another case more of a technical type of message,” he says.

Skill Gaps

While there is a near-uniform consensus on the importance of communication ability and emotional intelligence for security managers, these skills are hard to find in some candidates, recruiters say. Some observe that overreliance on technology is eroding person-to-person communication.

“Communication skills are becoming seriously lacking,” Snipes says. “We’ve become a society, a world, so focused on communicating electronically that the ability to strike up a conversation in person with another human being is becoming a lost art, particularly with the younger generations.”

“The more the younger generations communicate electronically,” she adds, “the less practice they’ll have communicating in person and the more often that lack of skill will be noticed.”

Bayne voices a similar view. “I believe that some of the technology we use on a daily basis has changed our approach to communication and made some of us a bit lazy,” she says. “This has most clearly affected younger generations who have learned to communicate more frequently with those tools, instead of using traditional verbal or written communication.”

And Snipes sees another communication-related issue that is becoming more common with younger professionals. As the use of LinkedIn becomes ubiquitous in the business and employment world, some younger candidates are using it as a social network instead of a professional network.

“These users are using profile pictures from social situations, with nary a thought as to how the picture might be perceived by a prospective employer,” Snipes says.

Her advice is simple: keep professional photos professional. “I suggest
avoiding the four Bs in profile pictures—no beer, boats, baseball caps, or other people’s body parts (that is, no one else’s chin, arm, hair, or shoulder).”

Communication gaps are not the only deficiency, recruiters say. In the area of emotional intelligence, self-awareness can be a subtle yet important attribute for a security manager to have, but some lack it, Lammert says.

“It’s that seeking of feedback, the willingness to admit mistakes and take responsibility for actions,” he says.

One possible reason for that lack is that, unlike other skills that can be linked to performance metrics, “self-awareness is not as easy to measure,” and not as frequently talked about, he adds. Still, it is a great quality to have, and self-aware managers often realize the importance of continuous growth.

“It can also drive a desire for development, and a desire to take on leadership roles,” he explains.

Another subtle-yet-valuable soft skill that seems to be lacking in many security managers these days is the ability to question assumptions, says Spagone. With technology and analytics developing at lightning speed, a successful manager can’t hold on to traditional ways of solving problems.

“There is a key subtle difference in the ability to identify a challenge without assuming that it can be solved the same way it was a year or two ago,” Spagone explains.

Take for example a security manager who has found that one component of the firm’s security program has fallen out of compliance. That manager should not assume that the traditional methods of addressing that problem are still valid. “They must consistently question how decisions are reached, while still adhering to consistent standards, such as regulatory requirements,” he says.

Skill Sets
But while some security managers may need to fill skill gaps, others pulled together several soft skills to build a skill set that is especially effective in today’s industry.
For example, Bayne cites the common industry reality that companies continue to try to do more with less, even though the pace of business continues to speed up.

“Anyone in our industry who is good at what they do has more on their plate than ever, and is busier than they have ever been before,” she says. “Because of that, the job needs to be done right the first time, for efficiency in productivity and to maintain the highest level of customer retention.”

Security managers who can survive, and even thrive, in this environment usually combine communication skills with the ability to work under pressure, a knack for troubleshooting, and an insistence on maintaining integrity and a code of ethics so no corners are cut, Bayne says.

Spagone mentions another persistent reality in the industry—the view held by some company leaders that security is a cost center that is a distraction (albeit a necessary one) from the overall business goals and financial targets of the firm.

In this environment, certain security managers have the right combination of business understanding, executive presence, and a focus on vision, goals, and transparency, and this skill set helps top executives think of security in a less limited way.

“It’s about breaking the mold,” Spagone says.

Bayne agrees, and adds that some of the soft skills in a desired skill set evolve over time. She offers the example of executive presence.

“The executive presence which now seems to garner the highest level of respect is very different than it was in previous decades,” she explains. “More than ever, leaders are expected to be transparent, approachable, and in the trenches with their teams, rather than delivering orders from above.”

Furthermore, Bayne cites another important relevant trend in the industry: an organizational focus on developing a strong and distinctive culture. In that environment, managers who have combined the soft skills of coaching, team building, and teaching are often sought after.

“Coaching, team building, and teaching often tie back to specific areas of corporate culture, and because they are being demanded from the most recent additions to the talent pool, they are in the spotlight more than ever,” she explains. “They are now considered critical by both candidates and companies.”

Finally, Spagone says it is important to keep in mind that the combination of soft skills needed will also depend on the circumstances surrounding the position being filled.

“Companies and cultures are unique. And all new hires are about addressing an organizational challenge of some kind,” he says.

Skills of the Future

Looking forward, the soft skill set of coaching, team building, and teaching will continue to be vital for the security managers of the future, but with a new twist, Spagone says. He illustrates this by explaining a recent trend in the recruiting industry.

“We used to struggle with candidates that were heavily institutionalized—leaders who had been successful inside of their own insular corporate cultures, but who were unable to adapt in a different environment,” he explains. “They were not agile enough to be effective in a new or different organization.”

But this is becoming less common, as businesses are more interconnected than ever. To compete, companies must be increasingly agile.

Team building will still be crucial, but in a more strategic and fluid way, so that interdependent teams are staffed with members possessing portable skills. They may trade members, interlock if necessary, and work at an increasingly rapid pace, and managers must be able to make strategic decisions on the fly and nimbly rearrange all the pieces.

“Leaders must continue to understand where they need to add to their roster,” Spagone says, “and what skills can be groomed, what can be replaced or outsourced, or shared among their team—and themselves.”

MARK TARALLO IS SENIOR CONTENT MANAGER AT SECURITY MANAGEMENT. CONTACT HIM AT MARK.TARALLO@ASISONLINE.ORG. CONNECT WITH HIM ON LINKEDIN.
the INTOXICATION issue

Private parties regularly hire contract security firms. But often, those security officers have not received training in how to interact with, and manage, intoxicated guests.

It’s a typical affair. A company hosts a holiday party for employees and clients. It books a venue to handle the DJ, it hires a caterer to provide the food and wine, and it contracts with a security firm to make people feel safe while they celebrate.

But what happens if someone gets drunk at the party and gets into an argument with another guest? Or passes out? Or tries to drive home? What’s the security officer supposed to do?

This exact predicament arose when a woman, who’d just been promoted at work, was attending a private event. She wanted to celebrate her new professional accomplishment and ended up drinking alcohol to the point that she was intoxicated.

When she went to leave the event, she stumbled and fell. A security officer, whose firm was contracted for the event, helped her up, sat her down in a chair, and got her
some water. She reassured the officer that she was fine, and he escorted her to an elevator that went down to a sub-level parking garage.

The woman, however, was not fine. She got in to her car, drove up the wrong ramp to exit the parking garage, crashed into a drop gate, drove out onto the street, and ultimately killed a bystander.

A lawsuit was later filed against the security firm for allowing her to leave the venue in her vehicle while intoxicated. The suit was settled for a final amount that was not disclosed.

In a deposition, the security officer who had been on duty at the event was asked what training he had to handle interactions with individuals under the influence. The officer said he had never received any.

“If that guard had been trained, he’d have known better—that there are policies or something I have to do because this woman can’t drive,” says Russell Kolins, CEO of Kolins Security Group and an expert witness on security issues.

And, unfortunately, that lack of training is common for many security officers working for contract firms that provide services for special events, Kolins adds.

“The professionals who are the bartenders, servers, and security personnel who work at venues are trained—but in the private party arena, where you have contract guards who are assigned to protect the party, they are not trained because this is not something they would normally do,” he explains.

In the last two years, Kolins says he’s been contacted about five separate cases involving contract security agencies that were later sued because of their response—or lack of—to an intoxicated person at a private party.

Typically, contract agencies that are hired for events—like private parties—are focused on keeping uninvited people out of the venue, answering questions, and giving the presence of authority so people feel safe.

“But they normally don’t have discussions about whether or not alcohol is being

From page 43 of the February 2019 issue of Security Management.
served; it’s not something that would be in their normal course of operation,” Kolins says. “They are there for a specific purpose—to provide a deterrent to a crime or negative things that could occur. They don’t take into consideration how they are going to deal with intoxicated individuals.”

SIDE EFFECTS
Alcohol is a depressant and when consumed, it passes into the bloodstream to affect the brain, kidneys, lungs, and liver.

Its most visible effects, however, are on the central nervous system, causing physical and behavioral changes like relaxed inhibitions, impaired judgment, slowed reaction time, and reduced motor coordination.

The amount of alcohol it takes to make a person intoxicated depends on a variety of factors, including weight, gender, age, metabolism, food intake, the strength and type of alcohol, and any medication that the individual is taking. Women are more likely to feel the effects of alcohol sooner because they have lower levels of the enzyme that breaks alcohol down—meaning it will stay in their system longer.

The legal blood alcohol limit to operate a motor vehicle in the United States, Malaysia, Mexico, New Zealand, Norway, Puerto Rico, Singapore, and the United Kingdom is .08 percent.

Many other Western and European countries have a .05 percent blood alcohol limit, including Australia, France, Germany, Italy, and Switzerland. Other countries, like China and Sweden, have a lower blood alcohol limit of .02 percent.

Employees who work in restaurants, bars, and nightclubs are trained to recognize changes in behavior due to alcohol consumption. Many establishments have this training in place due to U.S. dram shop statutes, which allow the venue and the individual serving the alcohol to be held liable for selling or serving alcohol to individuals who then cause injury or death due to intoxication.

While security personnel are not engaged in serving people alcohol, by being employed directly—or indirectly via a contract—by a venue that does, they could be liable should an incident occur. Therefore, it’s critical for security personnel to receive Training for Intervention Procedures (TIPS), like bartenders and servers do, to recognize the signs that someone is intoxicated, Kolins says.

“The program teaches you how to handle people and how to interact with them, and gives you an understanding of how people might act if they are under the influence,” he explains. “People do stupid things when they are under the influence.” Security managers also need to have policies in place that explain what security personnel are expected to do if someone is intoxicated.

“These policies could be as restrictive as necessary, but should at least say, ‘We will stop people, talk to them, notify the supervisor for the event, and turn this job over to the supervisor to handle if necessary,’” Kolins says.

He also recommends that clients hiring contract security firms for special events cover what the policies and expectations are for security staff when interacting with individuals under the influence.

“Have a clear understanding, in writing, requiring guards be trained to understand the effects of alcohol and how to deal with people who are intoxicated,” Kolins explains. This can then be used to demonstrate, should an incident occur, that the security firm took reasonable steps to prevent it.

IN PRACTICE
Darrell Clifton, CPP, has worked in casino security for almost 30 years. As the current executive director of security for Eldorado Resorts, Inc., which owns the Eldorado, Silver Legacy, and Circus Circus in Las Vegas, he works with a proprietary security team responsible for three casinos, six nightclubs, and roughly 100 bars. And they interact with people under the influence every day.

“Being drunk, not only is it not a crime, it’s acceptable behavior at a casino and a nightclub—it’s what we market,” Clifton says. “Just because someone gets drunk doesn’t mean they are a bad person.”

This is the mindset that Eldorado Resorts starts with when teaching security staff how to interact with people who are under the influence. Even though individuals are intoxicated, security staff has a responsibility to treat them like valued guests.

“There are many states that have dram shop laws. Nevada does not, but it doesn’t excuse us from liability or moral responsibility of making sure somebody gets to where they are going safely,” Clifton adds.
In training, which involves role playing and then on-the-job training with a supervisor, security staff are taught how to recognize that someone is intoxicated, the policies in place to address that behavior, and that they are empowered to take action based on those policies.

For instance, security officers are taught to “work the line,” looking for minors who would not be allowed in, individuals who don’t meet the dress code, or those who are visibly intoxicated.

“We teach our staff that you have the power to keep those people out of the venue, because then they take it seriously,” says Clifton, adding that it helps prevent future incidents.

Clifton also stresses the importance of training security staff, and other employees like valets, to be on high alert when people leave the premises to ensure their safety. His staff is encouraged to engage people, especially those who show signs of intoxication, while they exit clubs, bars, or the casinos.

“You talk to them and get more information as to how intoxicated they are, and then decide if they are all right,” Clifton says.

If the security officer determines that that person is not safe to leave on his or her own, the officer is taught to ask if there is someone who can be called to pick them up. Other options include walking the person to their hotel room, if it’s part of the same venue, or calling a taxi or free shuttle service.

If the person has been driving, the officer and the valet can offer to hold the person’s keys and keep their car overnight. If the individual becomes resistant and insists on driving, security and the valet can tell them they will only surrender the person’s keys after the police have arrived on the scene.

“We tell people we don’t want to ruin your night, and that works 99 percent of the time,” Clifton says.

As a last resort option, security staff can call the police who will pick the individuals up and put them in a holding cell to sober up without being charged with a crime.

This all goes back to duty of care, Clifton says. Security owes this care to people at the venues it is responsible for protecting.

“What we should do as good risk managers is realize the liability is out there, the danger is out there, and we have a responsibility to the customers to keep everybody safe,” Clifton says. “If we do the right thing, we should be okay.”

CONTACT SENIOR EDITOR MEGAN GATES AT MEGAN.GATES@ASISONLINE.ORG. FOLLOW HER ON TWITTER: @MGNGATES.
Five people were killed in a shooting at the Capital Gazette newsroom in Annapolis, Maryland, on June 28, 2018. The gunman walked into the building and barricaded the rear exit of the newsroom before he began shooting. The newsroom’s design was open-concept, a popular design choice for news organizations.

“There are glass windows all around the room,” Terry Smith, a columnist for the Capital Gazette, told CNN in an article released shortly after the tragedy. “There is nothing except for a few half-walls at the editors’ offices on the left to impede a shooter.”

In addition to the open-concept layout, which left victims exposed, there was no receptionist or access control system the shooter had to bypass to enter the newsroom.

“They had no access control in the front of the building,” notes Pete Blair, executive director of the Advanced Law Enforcement Rapid Response Training Center at Texas State University. “And that was a decision...
they had made, saying, ‘Look, it’s a community newspaper and we want people from the community to be able to come in and find reporters to tell stories to,’ and that’s how they got a fair amount of their information.”

Blair spoke on a panel at GSX 2018 that addressed the security of newsrooms in light of the Capital Gazette shootings. He tells Security Management that since the shooting, the Annapolis newspaper said it would change the location of the newsroom. “Now they have made the decision that they are not going to allow easy access to places,” Blair says. “A lot of places were starting to talk about moving their newsrooms up off the first floor to the second floor, or something like that, to make it more difficult to find them and access them.”

The Annapolis shooting has raised questions about the challenges of open-concept designs in the event of an active assailant situation. While these sleek office interiors may be pleasing to the eye, experts note their design make it harder to seek cover or lock down in emergencies. And the challenges don’t stop at active assailant situations. Cybersecurity and information protection can also be an issue in open office environments.

Open-concept office spaces aren’t just popular with newsrooms—the design choice is on the rise. A 2017 survey by office staffing firm Robert Half shows that about one in five companies switched to an open-office configuration in the last five years. Forty-eight percent of respondents said they believed the open concept helped productivity; 32 percent said it was hindering to productivity; and 20 percent believed there was no impact.

Other studies show more negative feedback on open spaces. According to a survey of self-identified “high-performance employees” by software strategist William Belk, 58 percent of these individuals “need more private spaces for
OPEN OFFICES | BY HOLLY GILBERT STOWELL

problem solving.” His findings were published in a March 2017 article on CNBC. In addition, 54 percent of these employees said they found their office environments distracting.

Office design isn’t just critical for productivity considerations—it’s key to providing a safe and secure environment for employees, says Herbert Ubbens, CPP, PSP, president of Paratus Consultants Group and member of the ASIS International Commercial Real Estate Council.

“There are a lot of challenges within those open spaces where there are a lot of cubicles,” he says. In the open-concept office, there are fewer walls and office doors to close, potentially hindering employees’ responses in the event of an emergency. “When you have a reduction in hard surfaces... there’s some concealment but very little cover out there when a shooting does occur,” he notes.

Blair echoes Ubbens’ sentiment about active assailant situations. “The new designs look pretty—but they are not well designed for safety,” he says.

ACTIVE ASSAILANT
In the event of an active assailant, transparent designs—from conference rooms to office walls—don’t provide any type of concealment when fleeing an attacker. “The attacker would be able to see where everybody is, and be able to guide themselves that way, so that’s a problem,” Blair says. He recommends film that goes on the glass, even if it is simply to provide concealment.

“The films that you can put on windows that are affordable tend to be ones that are designed to maintain the integrity of the glass, but not to stop bullets.” While bulletproof film is available, most organizations find it cost prohibitive.

When it comes to active shooter training methods, the Advanced Law Enforcement Rapid Response Training Center teaches a three-step approach. “We teach ‘Avoid, Deny, Defend,’ which means you should avoid the attacker if you can and get out of there,” Blair says. “If you can’t, deny access to your location—close, lock doors, barricade, that sort of thing—and as a last resort, defend yourself.”

In cases where those three steps are difficult to implement, the casualties tend to be higher, he notes, such as the Aurora, Colorado, movie theatre shooting that claimed 12 lives.

Shopping malls, on the other hand, are designed to allow traffic to flow freely. “So very quickly people can hear the gunshot, know something bad is going on, and there are plenty of ways to move away from that and get out of the location,” he says.

For companies opting for the open-concept spaces, Hubbens recommends a saferoom for emergencies, a concealed and secure room not offered by many open-concept designs. “One thing we’re seeing is the use of saferooms, essentially secure areas that would be used for a tornado shelter, as well as an area for everybody to go into and lock,” he notes. “It would be located somewhere toward the core of the building.”

For example, one client he works with has a nine-floor building and decided to install a saferoom on every floor. “They wanted to make sure that all of their people have somewhere they can evacuate to, or a safe haven for a hurricane or other environmental incidents,” Ubbens notes.

While saferooms seem like a viable option at first glance, Blair points out there are considerations for security and management. “It could be that, depending on where the attack starts, the safe room is in a position that is totally wrong for you to get to,” he notes. “It’s just not reasonable for you to try, and yet if you’ve trained people to go to the saferoom they may try it anyway.”

Secondly, employees may have to keep others locked out of the saferoom, a difficult decision and scenario for anyone to be faced with. “Having a saferoom means getting your head around the idea that you could have coworkers outside the door banging trying to get in, and you’re not going to let them in,” Blair explains, “because you can’t be sure that it’s not the attacker pretending to be somebody, and if you open the door and the attacker’s right behind the person, then the attacker gets into the saferoom.”

Blair recommends designing an office layout that has clear escape routes and training employees on various points of egress in the event of an emergency. He says that all too often, in an emergency people get caught up on the idea of exiting the same way they entered a location.

“One of the examples we use a lot in our trainings is from the Station nightclub fire,” he says, referring to the deadly blaze in Rhode Island in 2003 that left 100 people dead. Many of those victims died at the front entrance to the club where they came in, trying to use that same route to escape.

“Why did everybody go to that exit? Well, when you get placed under stress you’re going to go where you know. So, people turned and they went to that place they came in from,” Blair notes. “And yet if you are in your calm state, your rational mind, you know that fire code says there have to be other exits here.”

With any open-concept office space, access control on the front-end is essential. “You might have an open office design in the back of your
workplace, but in the front end you have an entry vestibule where people come in and they are screened there,” he says.

Newer technologies like weapon and gunshot detection systems are also valuable, according to Mike Neugebauer, CPP, a security and business development consultant for Johnson Controls. These are especially useful in environments with public spaces like courtyards or restaurants attached to the building.

“The beauty of the newer systems is they take a lot of the human interaction or response out of the equation and set in motion responses,” he notes. “The more steps that we can extract and make automated, the smoother that event is going to run.”

The “See Something, Say Something” mantra is also more difficult in any larger corporate environment without permanent workspaces, where workers cannot be acquainted with everyone else. “Now with this open space, where you may travel 20 floors to go to a conference room that’s been deemed a public conference room, you don’t know who’s supposed to be there and when,” Neugebauer notes. “And when you work at a building with two or three thousand employees you can’t possibly know every one of them. So, it makes that situational awareness even more valuable to a company.”

**INFORMATION SECURITY**

The financial sector has faced new security challenges as it modernizes branch offices, says Neugebauer. “With the picnic bench design, so-to-speak, where you sit in a different spot every day, you may be sitting next to someone who is working on a sensitive project on his or her laptop, and you have no need to see it,” he explains. “Banks used to be very mindful about separating employees that have customer information versus ones that have no access and no need for customer information, and those folks kind of mingle today so it really presents a lot of other security issues.”

Neugebauer, who spent several years as the security director for a large regional bank, explains that the security culture of the organization must be instilled and reinforced in employees, from where they store their computers to where they choose to have confidential conversations. “They don’t want to stand in a social area and have that confidential conversation, because in a large company you may not know everybody, and you may not know the person sitting three seats away from you, not knowing that person sitting there is just collecting data and information.”

---

**SECURING LIFE**

NEW

MZ 6100
MULTI-ZONE DETECTION

SAFETY IS AFFORDABLE WITH GARRETT’S NEW MZ 6100 WALK-THROUGH

- Multi-zone detection technology
- Enhanced zone lights and LED visibility
- Special programs for schools, special events and other key applications
- Broad discrimination and sensitivity selections available
- Budget friendly and simple to program

For product info #20 securitymgmt.hotims.com
Companies opting for open-concept designs should take clean-desk policies into consideration to keep information as well as business and personal assets, safe, according to Neugebauer. “The organization has to make sure it has lockers or somewhere in that space to put purses or briefcases, or your laptop if you’re not taking it home,” he says. “You don’t want to leave it out.”

If organizations have the chance to design the open-concept spaces from the ground up, Neugebauer says physical security teams should collaborate with IT to consider the holistic security picture. “We’re moving from a hardwired environment, where you have a hardwired computer, to the laptop, so now you have open Internet available and more people—especially if you’re in a multitenant building,” he notes. “Someone may be able to pick up that signal and hack your network more easily, so that situational awareness has to be turned up a notch or two.”

To foster security awareness throughout a company, all departments—from human resources to legal to IT and beyond—must be involved. “It’s almost like a three-legged stool—you take one of the legs away and the whole thing collapses,” he says. “And the employee has to become more responsible for the holistic security of their environment.”

Regardless of design, Blair points out that there is a balancing act when it comes to any security plan. Providing an environment that makes employees comfortable can be just as critical as keeping them safe. “We could have massive screening up front...then another screening to get into actual building, and make things very secure,” Blair explains. “But it would be very uncomfortable. So, there’s always that issue of finding the right balance.”

HOLLY GILBERT STOWELL IS FORMER ASSOCIATE EDITOR AT SECURITY MANAGEMENT.
CARGO THEFT, LOSS PREVENTION, AND SUPPLY CHAIN SECURITY
Dan Burgess, CPP
A leading expert in cargo crime analysis and loss prevention brings to light the full magnitude of the problem and outlines steps companies can take to secure the supply chain.
Item 2015
$74 member, $83 nonmember $55 member, $62 nonmember

EFFECTIVE SECURITY MANAGEMENT, 5TH ED
Charles A. Sennewald, CPP and Curtis Baillie
This timely revision of a classic text teaches practicing security professionals how to build their careers by mastering the fundamentals of good management.
Also see the new edition: Effective Security Management, 6th Ed
Item 1946
$69 member, $78 nonmember $39 member, $49 nonmember

RISK ANALYSIS AND SECURITY COUNTERMEASURES SELECTION
Thomas L. Norman, CPP, PSP
This comprehensive resource explains how to evaluate the appropriateness of countermeasures, from a cost-effectiveness perspective, and details the entire risk analysis process in language that is easy to understand.
Also see the new edition: Risk Analysis and Security Countermeasure Selection, 2nd Ed.
Item 1878
$61 member, $65 nonmember $25 member, $30 nonmember

SECURITY AND LOSS PREVENTION, 6TH ED: AN INTRODUCTION
Philip P. Purpura
This edition contains updates on security and loss prevention practices as well as recent technologies such as social networks, digital evidence warrants, and advances in CCTV and their effect on security.
Item 2068
$65 member, $66 nonmember $38 member, $43 nonmember

BUSINESS THEFT AND FRAUD: DETECTION AND PREVENTION
James R. Youngblood
This book offers a broad perspective on business-related theft, providing a detailed discussion of numerous avenues of theft, including internal and external fraud, organized retail crime, mortgage fraud, cyber fraud, and extortion. This text is critical for those involved with loss prevention, security, or criminal justice.
Item No. 2323
$79 member, $87 nonmember

ENTERPRISE SECURITY RISK MANAGEMENT
Brian Allen, Esq., CISSP, CISM, CPP, CFE and Rachelle Loyear, CISM, MBCP
The authors present a step-by-step guide to using Enterprise Security Risk Management (ESRM) to manage all security risks. Whether related to information, cyber, physical, asset management, or business continuity—all risks can be mitigated through this holistic, all-encompassing ESRM approach. Gain tools and materials that will help you advance in your career.
Item No. 2951
$70 member, $82 nonmember

MANAGER’S GUIDE TO ESRM: ESSENTIALS OF RISK-BASED SECURITY (THE)
Brian Allen, Esq., CISSP, CISM, CPP, CFE and Rachelle Loyear, CISM, MBCP
This groundbreaking companion book to Enterprise Security Risk Management, referenced above, takes you through the steps of putting ESRM into practice throughout the enterprise.
Item No. 2952
$32 member, $35 nonmember

FIVE TECHNOLOGICAL FORCES DISRUPTING SECURITY (THE)
**ASIS International’s Book of the Year**
Steve Van Till
Explore the major technological forces currently driving digital disruption in the security industry, and what they foretell for the future. The book provides a high-level perspective on how the industry is changing as a whole, as well as practical guidance on how to incorporate these new technologies to create better security solutions.
Item No. 2953
$62 member, $66 nonmember

*Quantities are limited

To purchase or browse all titles, visit asisonline.org/pub19
Taking place 27–29 March in Rotterdam, The Netherlands, the ASIS Europe education program will cover technology as a friend and a foe—including focused discussions on artificial intelligence (AI) and drones, critical and emerging risks, and a training on biochemical terrorism.

The program also features management topics, with sessions on developing soft skills, securing an innovation culture, constructing teams, and working in collaboration with consultants. “Rapid, interconnected change and shifting perceptions of risk and value are key challenges for us as security practitioners,” states Eduard Emde, CPP, conference chair, ASIS Europe 2019. “We will examine evolving security challenges from the perspective of leaders tasked with protecting their organization’s reputation and most precious assets in a manner that drives business and cultural goals.”

The event will feature an Innovation Track of sessions that present solutions to today’s complex, connected challenges; a Career Center for coaching, skills, and career advice; plus exclusive networking opportunities for CSO Center members.

There are three ways to attend:
• Leadership Pass, allowing full conference access
• Professional Pass, providing great learning at a budget price
• Free Show Pass, offering access to the Career Center, Innovation Track, and exhibition

Visit asiseurope.org for full registration details plus sponsorship and exhibit opportunities.

ASIS EUROPE EXPLORES SMART CITIES

THE RAPIDLY EVOLVING technology landscape gives rise to a wide range of threats—but also the opportunity to make our cities smarter and safer. ASIS Europe 2019 will kick off with a morning of spirited discussions focused on cities of the future. Speakers include:

• Theo Veltman, innovation program manager for the municipality of Amsterdam, who will share Amsterdam’s smart city vision, including insight into the technologies and business models applied.
• Arnoud Molenaar, chief resilience officer, City of Rotterdam, who will examine how resilient city methodology is changing day-to-day and business life.
• A panel of these keynotes, chaired by Christina Duffey, CPP, president, ASIS International, which will address key questions around how security teams need to adapt as our cities evolve.

Taking place 27–29 March in Rotterdam, The Netherlands, the ASIS Europe education program will cover technology as a friend and a foe—including focused discussions on artificial intelligence (AI) and drones, critical and emerging risks, and a training on biochemical terrorism.
Did you make a New Year’s resolution to become a certified security professional? What if your employer doesn’t cover the cost of industry certifications? ASIS may have a solution.

The ASIS Foundation is now accepting scholarship and grant applications for the 2019 award cycle.

New this year, the Foundation is partnering with the International Foundation for Protection Officers (IFPO) to add Certified Protection Officer (CPO) or Certified in Security Supervision and Management (CSSM) certification scholarships to existing CPP, PCI, and PSP scholarships. With a 30 percent increase in the number of awards given compared to 2018, ASIS scholarships and grants support member professionals in achieving the industry certifications they need to advance their careers and increase their overall earning potential.

Qualified members can apply through 30 April at the new online portal on asisonline.org/foundation. The online application is the only way to apply; mailed and emailed applications will no longer be accepted. If you have previously applied and did not win, you are eligible to re-apply. Past winners are not eligible for 2019 grants.

Grantee and scholarship results will be announced in June. Applications are assessed by members of the Foundation Board’s Scholarship and Grant Committee and industry expert volunteers.

Visit asisfoundation.org/scholarships to learn more.

**DO BETTER THAN BUY: PARTNER**

ASIS has joined with SecurityXchange, a strategic partnership summit taking place 8–9 August in Park City, Utah, USA. ASIS member John Nemerofsky, chairman of the board for SecurityXchange, explains the value of strategic partnerships. Learn more at verticalxchange.com/SecurityXchange.

When you read “strategic partnership,” what comes to mind? Typically, it’s used to refer to co-branding: companies joining forces to amplify their reach, add brand value, and accelerate

---

**ASIS BOARD OF DIRECTORS**

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

**PRESIDENT-ELECT**
- Godfried Hendriks, CPP
- Revolution Retail Systems
- Alkmaar, The Netherlands

**TREASURER**
- John A. Petruzzi, Jr., CPP
- G4S Americas
- New York, New York

**SECRETARY**
- Malcolm C. Smith, CPP
- Qatar Museums
- Doha, Qatar

**CHAIRMAN OF THE BOARD**
- Richard E. Chase, CPP, PCI, PSP
- General Atomics
- San Diego, California

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

---

**#MYASIS IMAGE OF THE MONTH**

**EMILY SULLIVAN, PSP, ON TWITTER**

Meet the 2019 @ASITulsa038 Board. @ASIS_Intl
#securitymanagement
success. But there’s an entirely different partnership that often goes overlooked, and it’s one that can make a huge impact on your strategic plans and bottom line. That’s the partnership you ought to have with your solution providers.

As a security professional, you’re buying complex solutions—technologies that require significant investment but change rapidly. These technologies must work in concert with other solutions, and their performance is mission-critical. This is where strategic partnership comes in.

Sales reps can be excellent partners, but their jobs are to sell what the company has on offer today, not to be experts on technology in development. How much better could you plan strategically if you had insight into where your technology partners’ solutions are going in the next two years...or five years? Even better, what if you had input into that development?

When you have insight and input into the solutions you are buying, you have a meaningful strategic partnership. But how do you make that happen?

• Create a relationship with senior executives at the companies you buy from (or are considering buying from).
• Dedicate some face-to-face time regularly to sharing ideas, challenges, and solutions.
• Partner with an integrator who believes and invests in strategic partnership with technology providers, too.

Create an executive-to-executive strategic partnership with your most critical technology partners, and you can stay ahead of the technology development curve, help refine solutions that could better meet your needs, and ensure the best possible performance, not to mention create a powerful resource if a technology ever fails you. This is the kind of partnership that industry leaders rely upon to stay on top, and it’s a strategy that can work for you, too.

---

**THIS MONTH IN ASIS HISTORY**

In February 1985, U.S. Secretary of State George P. Shultz announced the formation of the Overseas Security Advisory Council (OSAC) in an address to members of ASIS—which at the time was still known as the American Society for Industrial Security.

Citing a rise in terrorism around the globe, Shultz established OSAC to foster greater operational coordination between the U.S. government and private sector security teams worldwide. “By working together to enhance security,” he said to the ASIS members in attendance, “we can be more effective in saving lives.”

More than 30 private and public sector member organizations comprise the OSAC Council—many ASIS members currently serve on it—and the partnership between OSAC and ASIS International continues to this day. OSAC regularly attends and presents at Global Security Exchange (GSX) and CSO Center events, including holding joint meetings with ASIS chapters around the globe.

Read more about OSAC in “National Security” on page 20.

**CRISIS MANAGEMENT AND BUSINESS CONTINUITY COUNCIL SPOTLIGHT**

You don’t know when a crisis will happen, but you need to be prepared. And, as ASIS International Crisis Management and Business Continuity (CMBC) Council Vice Chair Erik de Vries notes, “You can never learn too much in preparation for a crisis.”

This tenet underscores the council leadership’s approach to education. Every industry needs to prepare for the unexpected—and the CMBC Council seeks to be the bridge through which organizational resilience best practices are communicated to security professionals across all sectors.

The council’s annual workshop, considered by Council Chair Brendan Monahan to be the cornerstone of its educational content, enables CMBC gurus to share their joint expertise with attendees over the two-day course. The 2018 workshop—“Strategy and Tactics in Crisis Management: From Prevention to Recovery”—was held in December in Scottsdale, Arizona, USA. It introduced a modernized approach to its format. Listening to the feedback...
The council takes steps to deliver these best practices to the ASIS membership at large, posting takeaways from these discussions in the Open Forum on ASIS Connects. If you have a CMBC question, connect with council members of previous participants, the council introduced interactive tabletop exercises that allow attendees to get hands-on experience with crisis management scenarios throughout the process. Monahan notes an “enthusiastically positive” attendee response following the change. This year’s workshop will be held November 4–5 in Seattle, Washington, USA.

At Global Security Exchange (GSX) 2018, the council also proved to be one of the busiest suppliers of educational content, sponsoring several timely CMBC sessions—including “Converged Security: All Risk is Shared,” “Hostility Management: Defusing Hostile People,” and “Ransomware: Managing Data Extortion Crises.” On March 28 at ASIS Europe 2019, the council will also present training on “Reputation Risks from Fake News—Crisis Management Response.”

“We have monthly calls where we share best practices and lessons learned. In 2018, our members spoke on suicide as a workplace violence issue, crisis management in the airline industry, incident command systems for private sector emergency response, adaptive business continuity, and more,” says Monahan. “After we share knowledge and experiences, we then work together and find ways these lessons apply to scenarios across various industries. We’re helping to raise the bar of global CMBC practice.”

The council takes steps to deliver these best practices to the ASIS membership at large, posting takeaways from these discussions in the Open Forum on ASIS Connects. If you have a CMBC question, connect with council members.
bers by visiting their community. Go to community.asisonline.org and search for “Crisis Management and Business Continuity Council.”

LIFE MEMBERS
ASIS congratulates its newest Life Members: Reggie L. Clark, CPP; Kenneth R. Cole, Jr.; Anne M. Gibbons, CPP; and Richard A. Michau, CPP.

Reggie L. Clark, CPP, has been an ASIS member for 35 years and a CPP since 1990. He has been active on the chapter and regional levels, serving as chapter secretary, chapter vice chair, chapter chair, assistant regional vice president, and regional vice president.

An ASIS member for 37 years, Kenneth R. Cole, Jr., has served in leadership for the Central Illinois Chapter over many years, with multiple terms as chair, treasurer, and secretary.

Anne M. Gibbons, CPP, joined ASIS in 1995 and earned her CPP in 1999. She has been active in her chapter, serving as chair, vice chair, secretary, and treasurer. Gibbons was a longtime member of the ASIS Physical Security Council and served on the Diversity Council.

Richard A. Michau, CPP, has been an ASIS member for 36 years. He was on the Professional Certification Board and served as its president. Michau was a member of the Petrochemical, Chemical, and Extractive Industries Security Council for several years, and he also served as a chapter chair.

MEMBER BOOK REVIEW
Serial Killers and The Aftermath.
By Rosemary J. Erickson, Ph.D.
CreateSpace Publishing; amazon.com; 252 pages; $19.95.

An intriguing combination of a memoir, a novel, and a serious work of nonfiction, Serial Killers and The Aftermath explores the author’s work in premises liability security civil cases. The author states in the preface that the book is “a personal, first-person, sometimes fictionalized account.” Some passages are also written by her husband, Arnie Stenseth, and describe his point of view.

Throughout the book, the author describes her upbringing, education, professional career, personal life, and thoughts about the profession of a forensic sociologist. She also details case work from four serial killer cases she was involved with. Throughout the cases she provides diagrams, newspaper articles about the cases, checklists, figures, and photos of perpetrators and victims. That is the serial killer part of the title.

The aftermath concerns the author’s role as an expert witness in civil cases that arise from violence, such as when a person is injured or killed as the result of a violent crime at a shopping center or other public place, and the owners are sued for not providing a safe environment. Her research on each case includes understanding the mind of the perpetrator and how and why he selected a particular place or victim.

All things considered, this interesting book is a unique read with many focus shifts. It is and is not technical literature, and the reader is not quite sure what is real and what is fiction. Nonetheless, the author succeeds in her goal to “inspire young men and women to become forensic sociologists or...to think like sociologists.” The book will appeal to a general audience as a nontypical view into the world of serial killers and those who try to understand them.

REVIEWER: Poul Nielsen, PCI, Certified Security Manager, is an intelligence analyst at the Copenhagen Police Department. He serves on the ASIS International Investigations Council.

ASIS CLASSROOM PROGRAMS
FEBRUARY
25–26 CPP and PSP Review Programs, Savannah, Georgia, USA
25–28 ASIS Assets Protection Course: Principles of Security (APC I), Savannah, Georgia, USA

ASIS GLOBAL EVENTS
MARCH
27–29 ASIS Europe, Rotterdam, The Netherlands

ASIS WEBINARS
FEBRUARY
13 An Overview of the NIST Cyber Security Framework

View all education offerings at asisonline.org/education
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**
ELSEWHERE IN THE COURTS

U.S. LEGISLATION

This month’s “Legal Report” is a roundup of major security-related legislation considered by the 115th U.S. Congress, which concluded in January 2019. Included in this summary are public laws that went into effect and legislation that was introduced but failed to pass. The bills that failed were nullified, and members of Congress will have to reintroduce them in the 116th Congress.

BORDER SECURITY. The U.S. House of Representatives passed a bill that failed to advance in the U.S. Senate that would have created punishments for individuals who have been forcibly removed from the United States or denied admission who enter—or attempt to enter—the country. The bill (H.R. 3004) would have allowed the United States to fine and imprison—for up to two years—non-U.S. citizens who enter, or attempt to enter, the country after being excluded, deported, removed, or denied admission.

CLEARANCES. U.S. President Donald Trump signed legislation into law that...

DISCRIMINATION. The U.S. Age Discrimination in Employment Act (ADEA) applies to all public-sector employers regardless of their size, the U.S. Supreme Court ruled. The ADEA prohibits employers from discriminating against employees based on their age, and in its opinion by Associate Justice Ruth Bader Ginsburg, the Court said employers under the law include even public employers with fewer than 20 employees. The ADEA and other relevant laws “leave scant room for doubt that state and local governments are ‘employers’ covered by the ADEA regardless of their size,” Ginsburg wrote. (Mount Lemon Fire District v. Guido, U.S. Supreme Court, No. 17-587, 2018)

PREGNANCY. Nursing and healthcare facility Absolut Facilities Management, LLC, will pay $45,000 to settle charges of pregnancy and disability discrimination brought by the EEOC. Absolut “failed to accommodate disabled workers; denied leave as a reasonable accommodation to individuals with disabilities; refused to allow disabled employees to return to work unless they could do so without medical restrictions; and subjected employees to impermissible disability-related inquiries and medical examinations,” according to the EEOC. It also charged that Absolut fired employees based on their pregnancy status and failed to accommodate pregnancy-related medical restrictions. (EEOC v. Absolut Facilities Management, LLC, U.S. District Court for the Western District of New York, No. 1:18-cv-01020, 2018)

LEGAL HIGHLIGHTS

ISSUE: Earthquakes
BILL: P.L. 115-307
VENUE: U.S. Executive Branch
STATUS: Enacted
SIGNIFICANCE: Requires a federal program to gather information on community resilience to earthquakes, develop the Advanced National Seismic System, and other measures.

ISSUE: Pornography
BILL: P.L. 115-299
VENUE: U.S. Executive Branch
STATUS: Enacted
SIGNIFICANCE: Makes changes to the procedures for determining the amount of mandatory restitution victims can receive in child pornography cases.
requires the National Background Investigation Bureau (NBIB) to report on the security clearance backlog.

The SECRET Act of 2018 instructs the NBIB to report to the Executive Office of the President on the current security clearance backlog; the bureau must then create a mitigation plan to identify the cause of the backlog, along with recommendations to address it.

The act also instructs the Office of the Director of National Intelligence to report to Congress and the president about implementing “governmentwide continuous evaluation programs” and U.S. agency initiatives to meet requirements for “reciprocal recognition to access classified information,” according to the law.

CYBERSECURITY. President Trump signed legislation into law that created an institute to train local law enforcement and other partners to investigate and prevent cybercrime.

The law (P.L. 115-76) authorized a National Computer Forensics Institute within the U.S. Secret Service through 2022 to share information related to investigations and prevention of cyber and electronic crime, and to educate, train, and equip local law enforcement, prosecutors, and judges.

The institute will train attendees about methods to obtain, process, and store digital evidence for use in court proceedings. It will also help with the expansion of the Secret Service’s Electronic Crime Task Force by adding officers who have completed training through the institute.

Another new law created new requirements for agencies addressing cybersecurity risks.

The act (P.L. 115-236) required the National Institute of Standards and Technology (NIST) to consider small businesses when it creates and supports the development of voluntary, industry-led guidelines and procedures to reduce cyber risk to critical infrastructure.

The Senate failed to advance legislation passed by the House that would have required entities to create internal risk control mechanisms to safeguard and govern market data storage.

The Market Data Protection Act of 2017 (H.R. 3973) would have required the U.S. Securities and Exchange Commission, the Financial Industry Regulatory Authority, and the Consolidated Audit Trail—in consultation with a chief economist—to establish comprehensive internal risk control mechanisms to safeguard and govern the storage of market data, market data sharing agreements, and academic research.

After the Equifax breach, legislation stalled in the House that would have required some companies that store Americans’ data to meet specific security and privacy requirements.

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

Covered data would have included Social Security, driver’s license, and passport numbers; financial account and debit or credit card numbers in combination with PINs; usernames and passwords; and biometric data.

The Senate did not advance legislation introduced for the second time by U.S. Senator Bill Nelson (D-FL) that would have required companies to disclose data breaches within 30 days of becoming aware of the breach.

Under the bill (S. 2179), companies would have had to report the breach, and any individual who concealed data about the breach could have faced up to five years in prison.

Nelson introduced the legislation after it was revealed that Uber paid hackers $100,000 to destroy documents and hide evidence of a data breach of more than 57 million records—including personally identifiable information from customers and drivers.

DISCLOSURE. President Trump signed legislation into law that nullified a payments disclosure requirement instituted as part of financial reform after the 2008 recession.

The resolution (H.J. Res. 41) eliminated the “Disclosure of Payments by Resource Extraction Issuers” rule that the U.S. Securities and Exchange Commission finalized in July 2016. The rule required resource extraction issuers to disclose payments made to governments for the commercial development of oil, natural gas, or minerals.

FIREARMS. The House passed legislation that later stalled in the Senate that would have allowed people with concealed carry permits to carry firearms across state lines.

The bill (H.R. 38) would have allowed people with concealed carry permits and a valid government-issued photo ID to carry their firearms into another state.
It also would have required agencies to report criminal history records to the FBI’s National Instant Criminal Background Check System (NICS).

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

**Harassment.** As part of the new U.S. tax law (P.L. 115-97), businesses are now prohibited from deducting the cost of sexual harassment or sexual abuse settlements if the payment is subject to a nondisclosure agreement.

**Identification.** President Trump signed legislation into law that prevents the U.S. Coast Guard from implementing previous identification requirements.

Under the law (P.L. 115-230), the military branch will not implement previously required Transportation Worker Identification Credential (TWIC)-Reader Requirements for the time being.

The law also requires the secretary of homeland security to report to the House Committee on Homeland Security, the Committee on Transportation and Infrastructure, and the Committee on Commerce, Science, and Transportation about the effectiveness of the TWIC program. After this report, the U.S. Department of Homeland Security may propose a new rule to implement TWIC readers.

**Injuries.** A new law eliminates a rule requiring employers to create and maintain records of work-related injuries and illnesses.

The resolution (P.L. 115-21) eliminated the rule created by the U.S. Department of Labor in 2016, which required employers to record injuries and illnesses on U.S. Occupational Safety and Health Administration (OSHA) 300 Log and 301 Incident Report forms within seven calendar days of becoming aware that the injury or illness occurred.

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

**School Security.** The House passed legislation, which did not advance in the Senate, that would have provided grant money for school safety measures.

The Students, Teachers, and Officers Preventing (STOP) School Violence Act (H.R. 4909) would have authorized $750 million in U.S. federal funding for 10 years to train school personnel, students, and law enforcement to prevent student violence.

Grant money could also have been used to develop anonymous reporting systems for threats, implement deterrent measures like metal detectors, or install technology for expedited notification of law enforcement during an emergency.

The bill was introduced after the Marjory Stoneman Douglas High School shooting in Parkland, Florida, which left 17 dead after a former student opened fire on campus.
SURVEILLANCE. Congress reauthorized and President Trump signed legislation that allows electronic surveillance tools to continue for another six years.

The law (P.L. 115-118) renews Section 702 of the Foreign Intelligence Surveillance Act, which allows U.S. agencies to monitor communications of foreigners on foreign soil without a warrant.

The Senate failed to advance legislation passed in the House that would have protected diplomats from surveillance by consumer devices.

The bill (H.R. 4989) would have directed the U.S. Department of State to create a policy on the use of location-tracking devices at U.S. diplomatic and consular facilities. Government employees, staff, contractors, and members of other agencies working at those facilities would be subject to the policy.

The bill was introduced in response to revelations that a fitness app used by U.S. military personnel revealed sensitive information about base locations and troop movements.

TERRORISM. The House passed legislation that would have given nonprofit organizations access to grant funds to prevent terrorist attacks, but it stalled in the Senate.

The bill (H.R. 1486) would have authorized $30 million in grants for nonprofit organizations that the U.S. Department of Homeland Security (DHS) deemed to be at risk of a terrorist attack. The funds would have been used to purchase security equipment, physical and cybersecurity training, target hardening, and terrorism awareness.

President Trump signed legislation into law that created a program to protect food, agriculture, and veterinary systems from acts of terrorism.

The law (P.L. 115-43) directs the assistant secretary for health affairs for DHS to create a program to coordinate its efforts to defend food, agriculture, and veterinary systems against terrorism and other high-consequence events that are a risk to homeland security.

The program will be designed to lead DHS initiatives to prepare for and respond to agricultural terrorism. It will be coordinated with U.S. Customs and Border Protection on activities related to food and agriculture security and screening procedures for domestic and imported products.

TRAFFICKING. President Trump signed legislation into law that will enhance efforts to combat human trafficking in the transportation sector.

The Combating Human Trafficking in Commercial Vehicles Act (P.L. 115-99) directs the U.S. Department of Transportation (DOT) to designate an official to coordinate human trafficking prevention efforts across the U.S. federal government and consider the challenges of combating human trafficking when several transportation modes are used.

President Trump also signed the No Human Trafficking on Our Roads Act (P.L. 115-106) that directs the DOT to disqualify operators of commercial motor vehicles—for life—if they use vehicles to commit a felony involving human trafficking.

UTILITIES. The House passed legislation that failed to advance in the Senate that would have reduced the threat of wildfires to electric transmission and distribution facilities.

The resolution (H.R. 1873) would have amended the Federal Land Policy and Management Act of 1976 to ensure that all existing and future rights-of-way established by grant, special use authorization, and easement for electrical transmission and distribution facilities include provisions for utility vegetation management, inspection, and operation and maintenance activities.

The resolution also would have required transmission and distribution facility owners and operators to create a plan for vegetation management that “provides for the long-term, cost-effective, efficient, and timely management of facilities and vegetation within the width of the right-of-way and adjacent federal lands to enhance electricity reliability, promote public safety, and avoid fire hazards.”

This column should not be construed as legal or legislative advice.
ELBIT SYSTEMS LTD. has a contract with the European Maritime Safety Agency to provide maritime unmanned aircraft system patrol services to countries in the European Union. In cooperation with CEiiA, the company will operate its Hermes 900 Maritime Patrol and its Ground Control Station. The long-range maritime surveillance system is tailored for littoral and blue water operations with a maritime radar, satellite communication, and a receiver to enable persistent monitoring of vast areas of sea and shore and identification of suspicious activities and potential hazards.

**MARITIME SURVEILLANCE**

**AWARD**
The Forte Wireless Data Glove from BeBop Sensors was named one of TIME Magazine’s Best Inventions 2018. The affordable glove incorporates haptics and rapid sensing for a wide variety of applications, including industrial, medical, virtual reality, design, and more.

**CONTRACT**
The Central Bank of Armenia worked with Louisenthal to produce new banknotes using the latest security features, including a security thread with machine-readable design elements, a watermark, a window, and an iridescent strip. G+D Currency Technology contributed the design and printing of the series.

**ANNOUNCEMENT**
Nonprofit Warrior to Cyber Warrior Foundation announced a nationwide program to provide veterans of the U.S. armed forces with free cybersecurity training and certifications to help veterans succeed as cyber professionals.

**MERGERS & MOVES**

**Convergint Technologies ➔ SI Technologies, Inc.**
The acquisition will augment Convergint’s service capabilities.

**Infineon Technologies AG ➔ NEXT Biometrics**
The companies will develop a reference design for biometric payment cards that include a fingerprint.

**Moxa Inc. ➔ Trend Micro.**
Joint venture TXOne Networks will focus on the Industrial Internet of Things.

**PRÆSIDIAD ➔ Drehtainer GmbH**
PRÆSIDIAD’s Hesco will incorporate Drehtainer to innovate military and security technologies.

**PARTNERSHIPS**

**RETAIL SECURITY**
Edesix and CBES teamed up with British retailer Asda to create a wearable CCTV system.

**ACCESS AND VIDEO**
ISONAS INC. is integrating its Pure Access software with Panasonic Video Insight 7 for combined video and access control.

**COMMUNICATIONS**
Titan HST provided emergency communications for the Annual Rockefeller Center Christmas Tree Lighting.

**ARMORED VEHICLES**
The Arab Organization for Industrialization and the Armored Group, LLC, formed a strategic alliance to combat terrorism and improve armored vehicles.
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>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>Abloy Security, Inc. ................. 23</td>
</tr>
<tr>
<td>--</td>
<td>Altronix Corp. ..................... 08</td>
</tr>
<tr>
<td>08</td>
<td>Ameristar Security Products .......... 17</td>
</tr>
<tr>
<td>03</td>
<td>B.I.G. Enterprises .................. 06</td>
</tr>
<tr>
<td>31</td>
<td>Detex Corporation ................... 34</td>
</tr>
<tr>
<td>07</td>
<td>DSX Access Systems, Inc. ............ 15</td>
</tr>
<tr>
<td>06</td>
<td>G4S .................................. 13</td>
</tr>
<tr>
<td>02</td>
<td>GAI-Tronics Corporation .............. 04</td>
</tr>
<tr>
<td>20</td>
<td>Garrett Metal Detectors .............. 49</td>
</tr>
<tr>
<td>52</td>
<td>Hanwha Techwin America .............. 35</td>
</tr>
<tr>
<td>24</td>
<td>Mission 500 ........................ 57</td>
</tr>
<tr>
<td>27</td>
<td>NAPCO Security Services .............. 68</td>
</tr>
<tr>
<td>12</td>
<td>Red Hawk Fire &amp; Security ............ 25</td>
</tr>
<tr>
<td>01</td>
<td>SecurAmerica ........................ 2-3</td>
</tr>
<tr>
<td>19</td>
<td>Special Response Corporation ........ 45</td>
</tr>
<tr>
<td>21</td>
<td>Strong Poles ......................... 50</td>
</tr>
<tr>
<td>09</td>
<td>TSCM America ......................... 19</td>
</tr>
</tbody>
</table>

ADVERTISERS ONLINE

- Abloy Security, Inc.  
  www.abloyusa.com
- Altronix Corp.  
  www.altronix.com
- Ameristar Security Products  
  www.ameristarsecurity.com
- B.I.G. Enterprises  
  www.bigbooth.com
- Detex Corporation  
  www.detex.com
- DSX Access Systems, Inc.  
  www.dsxinc.com
- G4S  
  www.g4s.us
- GAI-Tronics Corporation  
  www.gai-tronics.com
- Garrett Metal Detectors  
  www.garrett.com
- Hanwha Techwin America  
  www.hanwhasecurity.com
- Mission 500  
  www.mission500.org
- NAPCO Security Services  
  www.napcosecurity.com
- Red Hawk Fire & Security  
  www.redhawkus.com
- SecurAmerica  
  www.securamericallc.com
- Special Response Corporation  
  www.specialresponse.com
- Strong Poles  
  www.strongpoles.com
- TSCM America  
  www.tscmamerica.com

*Best practices supplement denoted in orange.
DORTRONICS SYSTEMS, INC., of Sag Harbor, New York, provides customers with fast turnaround times and competitive pricing for customized products. The company’s versatile manufacturing facility delivers a wide range of tailored products, including switches with durable laser-etched or engraved paint-filled lettering, custom plate sizes, and annunciators in almost any shape and size. Dortronics also offers a comprehensive line of magnetic locks, push buttons, and key switches in special finishes such as chrome, brass, and color-anodized aluminum. The extensive suite of products includes electric strikes, maglocks, panic bars, key switches, push button controls, delayed egress systems, door prop alarms, and mantrap interlock controllers that can be supplied with alarm annunciators and security consoles.  

A new application from 3XLOGIC of Westminster, Colorado, will allow Mac users to deploy the video management features of VIGIL video management software. VIGIL Client Lite for Mac allows users to view live streams for up to 36 cameras across multiple VIGIL servers and use VIGIL Connect or Direct IP to connect to multiple VIGIL servers or standalone cameras. Other features include digital pan, tilt, and zoom support through the Live View window; instant playback to quickly view the last five minutes of video; playback search based on date and time; export of snapshots or videos; and more.  

E2S WARNING SIGNALS of Houston, Texas, offers the GNEx family of corrosion-proof GRP sounders, beacons, and manual call points that have earned approval from IECEx and ATEX for Zone 1, 2, 21, and 22 use. All the visual signals use a polycarbonate UV stable prismatic lens, available in amber, blue, clear, green, magenta, red, and yellow, and are field-replaceable. The GNExB1X05 beacon is a high-output Xenon strobe flash. Its GRP enclosure features a threaded flame path, dual cable entries, and a large termination area for quick installation.
SPILL DETECTION

COBALT ROBOTICS of San Mateo, California, unveiled its new leak- and spill-detection capabilities. Now Cobalt robots can be programmed to find a leak or spill within a predefined area. Once caught, the security robot can then send the appropriate notification. The robots are equipped with powerful sensors, including day-night cameras, thermal sensors, motion sensors, and badge readers, which help them identify anomalies and other risks that might not be detected by the human eye. 205

LICENSE PLATE READER

The AutoVu MLC (Machine Learning Core) is a new machine learning-based engine for Security Center AutoVu, the automatic license plate recognition (ALPR) system from GENETEC of Montreal, Canada. AutoVu MLC replaces traditional rule-based ALPR technology with machine learning-based algorithms to reduce common ALPR misreads and false positives. Customers can realize even greater plate-read performance, further reducing the incidence of false-positive reads to a fraction of a percent. Performance improvement includes advanced vehicle analytics, such as state origin identification. The AutoVu MLC is available now as a firmware update for new and existing AutoVu SharpV hardware. 207

SITUATIONAL AWARENESS

The new Symmetry Control Room from AMAG TECHNOLOGY of Torrance, California, provides a single operational window for situational awareness and management of video, alarms, and events. It integrates with AMAG’s entire Symmetry portfolio, which includes video, visitor, identity, incident management, intrusion, and access control. It works with third-party manufacturers that are part of the Symmetry Preferred Partner Program. Monitoring platforms through Control Room delivers real-time intelligence for better decision making, more efficient operations, and quicker responses to incidents. It comes with a powerful graphics engine, enabling users to create a custom graphic interface for clear and efficient navigation, and it integrates with OpenStreetMaps for easy geolocation of events and navigation of all sites. 204

SECURITY MANAGEMENT

MAVIN TECHNOLOGIES of Rochester, New York, introduced the Mavin Security Management Platform version 6.1. New functionality includes cardholder tracking capabilities and the ability to save custom reports as favorites associated with a user’s login profile. Organizations can be notified via text message or email when suspicious cardholder activity occurs, and they can keep real-time tabs on the whereabouts of a particular person or group of people. Mavin SMP 6.1 also offers the ability to assign a new card to an existing cardholder from the Mavin Access app, a new Application Engine Icon with expanded status displays, and new Windows Services for improved system recoverability. 206

DISASTER MONITORING

DisasterAWARE Enterprise from KAAZING of San Jose, California, provides accurate and timely information on threats, such as a storm’s expected path and changes in its severity. The same technology used by U.S. federal agencies and disaster management organizations pulls together data from hundreds of authoritative sources. The platform offers access to more than 200 layers of data, derived from sources such as GIS, sensor data, social media heatmaps, and historical hazard data. Businesses can overlay these onto existing maps and add data of their own, such as facilities, asset location, employees, and more. Filtering by 18 hazard types and five levels of severity allows enterprises to see which of their assets are affected. 208
GAIL ESSEN, CPP, PSP, is president of Professional Security Advisors, a women- and diversity-owned firm based in Minneapolis, Minnesota. Gail serves as a member of the board of directors for ASIS International and previously led the Global Women in Security Council.

Q. What does ASIS mean to you?
A. ASIS is a core pillar of my success. It provides a global network of experts and innovators that others seek to mirror. ASIS enlarges my sphere of influence and opens doors of opportunity.

Q. Advice for new folks in the industry?
A. Develop a broad network of friends and colleagues by serving others. Check your motives in actions, words, and deeds to minimize self-promotion and purposely help others.

Q. A mentor who inspired you?
A. Brian Dunn provided fatherlike encouragement coupled with a tough-love temperament. Brian sent me to my first ASIS meeting.

Q. Advice for your younger self?
A. Balance work and family better, schedule business travel around the kids’ milestone events, and highlight weekends with quality playtime.

Q. Describe yourself in 25 words or less.
A. I am a servant leader who rises and falls with my team. I surpass goals, but do not expect perfection because mistakes afford growth.
REACH NEW HEIGHTS in Professional Excellence

ASIS accredited certifications can help you reach your career goals.

“I encourage all security professionals at our organization to attain ASIS certification, and it is a requirement for our senior-level positions.”

– Nicholas Santillo, Jr., CPP, PCI, PSP, Vice President, Chief Digital Infrastructure & Security Officer, American Water

Learn more at asisonline.org/cert-feb
LifeSaver™ Locks ensure a lifetime of advantages for the health of your facility, patients & budget

Life Safety Lock Series for managed liability, accident prevention and security in behavioral & health care institutions (and correctional facilities)

- **Anti-Ligature Models** – Ergonomic shape and construction prevents sentinel events; restricts the attachment of lines, laces, etc.
- **Matching Models for Every Door** – Cylindrical, mortise styles, models & functions available, including electrified units, ideal for buss-in/nurse station applications; plus antimicrobial finishes
- **Saves Budgets** - Typically 40% less cost than competitive products, while exceeding durability standards by as much as 400%
- **Ideal for Retrofit or New Construction** – Easy, aesthetic installation for all popular preps and door constructions
- **Facility-Friendly & Longest Life** – ANSI 156.2 Grade 1; UL 3-Hour Fire Rated & Lifetime Warranty

Push/Pull Paddlesets “Gurney-Activation”Strong, Durability & Ease of Use

- **Maximum Durability Over 3.1 Million Cycles.** Exclusive cylindrical chassis (not tubular) - 3X the ANSI Grade 1 Rating (ANSI 156.2)
- **Easiest Hands-Free Entry** with shortened angle and less force required
- **Attractive Stainless Steel** – Neatly retrofits over all existing trims

For a No-Obligation Site Needs-Analysis Contact Marks Today!

1-800-645-9445 • salesinfo@marksusa.com • www.marksusa.com

Lifesaver is a trademark of Marks USA/ Napco Security Technologies. Marks Lifetime Warranty is a lifetime mechanical warranty; see full details online.