FRANK ARGENBRIGHT, SECURITY GUARD WANNABE
Calling All Security & Procurement Departments for Companies with National Account Bidding Opportunities

As previously mentioned, SecurAmerica is now the 5th largest security company in the US with $300 million in revenue.

We have boots on the ground in 500 locations.

Our goal in 2018 is to be on every preferred vendor list for companies with national accounts out to bid. What do we have to do to get on your preferred list?

Could you please pass on my contact information to your procurement and supply chain departments? If you have any questions, please call my direct line at 404-926-4202 or my cell at 404-536-1140!

WWW.SECURAMERICALLC.COM
A world of vital security news delivered to your inbox.

**Security Management Daily**
is an exclusive e-newsletter for ASIS members. It offers the top 10 security headlines and is e-mailed daily.

**Security Management Weekly**
is a free e-newsletter for anyone who would like to subscribe. Receive the week’s 15 security headlines.

Check out the Security Management newsletters’ new features and design. To subscribe or resubscribe, e-mail ASIS International: asis@asisonline.org.
To imitate another company, particularly an industry leader, is to chase a moving target that captures what was effectively yesterday’s success.

Chris Walker, a management development consultant, on becoming a strategic leader. PAGE 47

“The equipment that was purchased 15 years ago has come to the end of its life cycle.”

Thomas Hicks, commissioner and vice chair of the U.S. Election Assistance Commission, on the security of U.S. voting machines. PAGE 15

“The private sector is far outpacing us when it comes to research and development.”

U.S. Department of Homeland Security Senior Advisor Kathleen Kenyon on government efforts to develop new security technologies. PAGE 20

For managers, it’s important to recognize that all incentives have a potential to turn perverse.

Marc Hodak of Farient Advisors on the Wells Fargo scandal. PAGE 51

1.8M
The predicted number of unfilled cybersecurity positions worldwide by 2020. PAGE 24

8.7
The number of workplace violence incidents per 10,000 employees in hospitals, compared with 1.7 per 10,000 across all industries. PAGE 35

72
The number of hours the Las Vegas shooter left a “do not disturb” sign on his hotel door. Hotels are now reconsidering how such signs are used. PAGE 33

“The equipment that was purchased 15 years ago has come to the end of its life cycle.”

Thomas Hicks, commissioner and vice chair of the U.S. Election Assistance Commission, on the security of U.S. voting machines. PAGE 15

“The private sector is far outpacing us when it comes to research and development.”

U.S. Department of Homeland Security Senior Advisor Kathleen Kenyon on government efforts to develop new security technologies. PAGE 20

For managers, it’s important to recognize that all incentives have a potential to turn perverse.

Marc Hodak of Farient Advisors on the Wells Fargo scandal. PAGE 51

1.8M
The predicted number of unfilled cybersecurity positions worldwide by 2020. PAGE 24

8.7
The number of workplace violence incidents per 10,000 employees in hospitals, compared with 1.7 per 10,000 across all industries. PAGE 35

72
The number of hours the Las Vegas shooter left a “do not disturb” sign on his hotel door. Hotels are now reconsidering how such signs are used. PAGE 33

ACHIEVE THE HEIGHTS OF SUCCESS

Partner.Win.

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

#PartnerWin

hikvision.com

For product info #3 securitymgmt.hotims.com
ADVANCE
YOUR PROFESSIONAL DEVELOPMENT IN 2018.
JOIN ASIS IN ORLANDO, FLORIDA

Professional development is a key driver for career advancement. In addition to staying on top of the latest threats and risk management strategies, a solid understanding of core security principles and field-tested best practices is essential. This is the type of vital information you’ll find in our March line-up of educational programming in Orlando.

CPP Review Program
March 12-13, 2018
Benefit from an accelerated, high-level overview of the security concepts and practices assessed on the Certified Protection Professional (CPP®) exam so you can develop a personalized study plan.

PSP Review Program
March 12-13, 2018
Intended to supplement your other certification exam preparation activities, this program provides a high-level overview of the three key domains assessed on the Physical Security Professional (PSP®) exam.

Assets Protection Course™: Principles of Security (APC I)
March 12-15, 2018
You can’t advance in the profession without a strong foundation. Make sure your fundamental knowledge of assets protection and its universal principles is rock-solid by attending APC!

REGISTER TODAY at asisonline.org/Orlando

“The APC series has been the cornerstone of my loss prevention knowledge and the basis for the quick rise in my career.”
NEWS & TRENDS
U.S. election officials prepare to fend off hackers and grapple with outdated equipment. 
By Mark Tarallo

SECURITY MANAGEMENT
ONLINE
New online this month: a study on laboratory safety, a report on election security, and a survey on intellectual property rights when doing business in China.

EDITOR’S NOTE
Do your incentives work as intended?

NATIONAL SECURITY
The U.S. government is attempting to engage the private sector in developing new security technology. 
By Lilly Chapa

CASE STUDY
A police department integrates gunfire detection technology into criminal investigations. 
By Holly Gilbert Stowell

CYBERSECURITY
New training and assessment programs seek to uncover hidden cybersecurity talent. 
By Megan Gates

ASIS NEWS
Meet the ASIS Commission on Standards and Guidelines.

ASIS BOARD OF DIRECTORS

LEGAL REPORT
Courts issue decisions on use of force and corruption. 
By Megan Gates

INDUSTRY NEWS
Video analytics targeted drivers for special billboard ads. 
By Flora Szatkowski

MARKETPLACE

ADVERTISER INDEX

SNAPSHOT
Intellectual property rights.
DOING BUSINESS IN CHINA

While U.S. companies saw increasing sales performance in China over the past year, access and uncertainty about policies towards foreign companies are undermining American companies’ confidence in China. The finding is from the 2017 US-China Business Council Annual Member Survey, which surveyed more than 200 American companies doing business in China about the business climate and the top challenges for American companies there. One major area of concern was intellectual property protection, with 94 percent of respondents saying they remain concerned about intellectual property rights enforcement in China.

NEW ONLINE THIS MONTH at www.securitymanagement.com

SM ONLINE

CYBERCRIME
A new U.S. law creates an institute to train local law enforcement and other partners to investigate and prevent cybercrime.

PARTNERSHIPS
The U.S. Department of Homeland Security released an industry guide designed to facilitate partnering with the private sector in creating technologies to address national security concerns.

ELECTION SECURITY
U.S. states and localities can take measures to secure the upcoming midterm elections, according to a recent report issued by the Center for American Progress, a liberal think tank.

CRIME STATISTICS
Crime in the United States, 2016, is the FBI’s annual compilation of crime statistics that are reported by more than 16,000 U.S. law enforcement agencies. The most recent report shows that violent crime rose from 2015 to 2016. Aggravated assault made up more than 64 percent of this type of crime. Robbery followed at 26.6 percent, rape accounted for 7.7 percent, and murder made up 1.4 percent of violent crime.

CYBER STAFFING
The cybersecurity workforce gap is on pace to increase 20 percent from 2015—leaving 1.8 million unfilled positions by 2020, according to the most recent Global Information Workforce Study.

EXCESSIVE FORCE
A jury must decide whether a police officer used excessive force when he tased a man for nearly two minutes, a U.S. court of appeals said in a ruling that revived a plaintiff’s suit.

DISABILITY
American Airlines Inc. and Envoy Air Inc. will pay $9.8 million to settle charges that they denied accommodations to disabled workers.

Go to SM Online for these and other links mentioned throughout this issue.
Maximum Reliability...

...Minimum Size!

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

GAI-TRONICS
A Hubbell Company

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

For product info #5 securitymgmt.hotims.com
EDITOR’S NOTE

B
et

ew 1955 and 1970, approximately 11,000 people were afflicted by a mysterious illness in Japan. Named sub-
acute myelo-optic neuropathy (SMON), the disease would eventually kill around 900 people in that country, and additional outbreaks would emerge in countries from Mexico to India to Australia.

The disease was crippling. What started as simple gastric distress soon became blindness and paralysis. Some victims developed a fuzzy green coating on their tongues. Medical professionals treated the disease with two different antibiotics, but the disease progressed unabated. Researchers worldwide sought a cure throughout the 1960s but each likely culprit—contaminated water, a virus, pesticides—was examined and eliminated.

This story, reported by Jeanne Lenzer in “When the Cure is the Cause: The Case of the Green Hairy Tongue” in Undark magazine, a publication devoted to science journalism, stymied researchers until 1970. That year “a pharmacologist made a forehead-slapping discovery,” she writes. “The two presumably different antibiotics, it turned out, were simply different brand names for clioquinol, a drug used to treat amoebic dysentery.”

The mystery went unsolved for so long because the disease looked and behaved like an epidemic. When someone came down with a stomach bug, family members took clioquinol as a preventative measure. “In short, what people thought was a cure for SMON was in fact its cause,” writes Lenzer.

In the business world, a version of this “cure as cause” is called a perverse incentive—an incentive that results in unintended consequences that are contrary to the goals of the incentive. About a year ago, Wells Fargo became a prime example of this phenomenon. A program to increase profits instead caused an expensive and embarrassing scandal. The company pushed employees to make more money by signing existing customers up for new services. Instead, Wells Fargo employees created almost 2 million deposit accounts and credit card applications—all without customer knowledge.

However, as Senior Editor Mark Tarallo points out in his article “Paved with Good Intentions,” starting on page 50, most corporate incentives do not become perverse. This means that managers can learn from the Wells Fargo situation and avoid the factors that created the problem. In that case, unrealistic goals for front line employees coupled with substantial financial rewards for their bosses led to an intense pressure to sell, and to cheat if those sales did not materialize. The final factor was a lack of program oversight that could have stopped the bad behavior before it did real damage.

The ending to the SMON story is also a warning to companies. According to Lenzer, legal documents show that clioquinol’s manufacturer Ciba-Geigy “was aware of the drug’s harmful effects for years.” In 1979, a Tokyo court ruled that it was responsible for the outbreak and ordered it to pay damages to the victims.

EDITOR-IN-CHIEF

TERESA ANDERSON
INTEGRITY. QUALITY. RELIABILITY.

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 braXos™ Integration
- Can use Mobile Ready Readers Smart Phone Credentials
- New Standard Software Features: AES-256 Encryption/DVR
- Integration Redundant Comm-Server (SQL Only)
- No “Per Seat” Licensing in System Pricing
- New User Interface Tabbed Organization
- Accountability Reports Last Use/Access Level History
- Mobile Initiated Incident Response
- Emergency Lockdown
- Email/text Notification
- “Who’s In/Muster” Reporting
- Backward Compatible: Hardware
- Virtual Environment Friendly

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

For product info #6 securitymgmt.hotims.com
But there’s another type of race already happening: a race against time. Namely, will officials be able to secure U.S. election systems when voters cast their ballots in November?

In recent years, election security has emerged as a repeated concern in the United States. The issue vaulted to prominence after the highly contested presidential election of 2000, which led to unprecedented levels of attention regarding voting methods and machines.

In a 2006 congressional race in Sarasota County, Florida, more than 18,000 votes went uncounted due to electronic voting errors.

Later, a New York University study examined three types of voting machines that were used in the 2006 elections, finding significant security and reliability vulnerabilities.

(For more background from Security Management, see “Will Your Vote Count,” May 2008, and “Machine Politics,” October 2012.)

This year’s election features another big concern: potential interference from Russia. That country attempted to hack the 2016 presidential election, U.S. officials have said, and concerns persist about a repeat performance.

“There is no doubt that Russia interfered in our 2016 election, and targeted 21 states’ voting systems,” U.S. Representative Robert Brady (D-PA) said at a recent Capitol Hill hearing on election security. “And we can expect them to return.”

Brady is cochair of the Congressional Task Force on Election Security, which was created last...
Hackers originally approached machines in all 50 states. But some were more locked down than others.

firmed publicly, but authorities have been unwilling to name the states affected.

However, according to Thomas Hicks, commissioner and vice chair of the U.S. Election Assistance Commission (EAC), the hackers originally approached machines in all 50 states. But some were more locked down than others, so the other 29 states were not hacked. (The EAC is an independent, bipartisan commission charged with developing guidance and adopting voluntary voting system guidelines.)

“Make no mistake, it’s all 50 states that were scanned. And it was just a little bit of—by the foreign actors or whomever—jiggling the handles and trying to get in. But some of those states were prepared enough that hackers weren’t able to get in,” Hicks said at the hearing. “So, as we prepare for the 2018 election cycle, we want to make sure that, from voter registration lists, to voting machines, to securing the voting equipment after the election, to election night reporting—from A to Z, all those aspects are taken care of.”

To help in the election security effort, EAC representatives have been flying out on a weekly basis to meet with state-level election representatives to advise on security protocols and systemic issues, Hicks said. The EAC has also been working with the U.S. Department of Homeland Security (DHS) to help get information on election security to state and local officials.

“I think there’s a lot more that needs to be done, because I believe that not only are there foreign actors that are looking to mess with our elections, but also folks within our own country who are looking to meddle in our election process,” Hicks said.

Besides the threat of bad actors, U.S. election security faces another risk—aging and outdated equipment. After the disputed 2000 election, Congress passed the Help America Vote Act in 2002, which brought about an equipment update in many states. But some of those machines now need replacing.

“The equipment that was purchased 15 years ago has come to the end of its life cycle,” Hicks said.

And even some of the older machines that are still in decent operating shape were not designed to withstand the type of cyberattacks and tampering methods that are possible today. “With the older equipment out there, security, if it was thought about at all, was really an afterthought,” said Virginia Elections Commissioner Edgardo Cortés at the hearing.

Voting machine modernization and better voting security is possible, but it takes significant investment, according to Rhode Island Secretary of State Nellie Gorbea. At the hearing, she offered her own state as an example, saying that when she took office in 2015 “our voting equipment was on the brink of total failure.”

So, the state invested $10 million in an upgrade, featuring paper ballot optical scanning machines with four layers of security and encryption.

Besides the equipment upgrade, there was the “second challenge” of building capacity in the public sector to manage election cybersecurity issues, Gorbea explained. It took a 40 percent increase in staff to do this, she added.

One of the lessons learned from this process, Gorbea said, was that better communication is needed between DHS and state officials regarding topics like threat information sharing. And more officials need to understand that effective cybersecurity does not mean arriving at a specific “destination,” but is rather a continuous process of assessment and improvement.

“Cybersecurity is at the forefront of election conversations at every level of government across the country,” she said.

Given this, Gorbea said she would “absolutely” be in favor of federally mandated baseline cybersecurity requirements for new voting equipment, especially given the precedent of the Russian hacking in 2016.

“These attacks are real, and are focused on undermining our representative democracy,” she said.

Besides replacing old voting machines and beefing up cyber defenses, states and localities can take other measures to help ensure that the upcoming midterms are secure, according to a recent report, Nine Solutions to...
Secure America’s Elections, issued by the Center for American Progress, a liberal think tank. In the report, Liz Kennedy, director of democracy and government reform at the center, and Danielle Root, voting rights manager for democracy and government report, set out nine tasks to improve election security.

Although a few, like replace old voting machines, are similar to the measures discussed at the Capitol Hill hearing, others touch on points not raised, such as requiring voter-verifiable paper ballots or records for every vote cast; conducting robust postelection audits to confirm election outcomes; updating and securing outdated voter registration systems; performing mandatory pre-election testing on all voting machines, as well as continuous vulnerability analysis; and providing federal funding for updating election infrastructure.

“As it currently exists, America’s election infrastructure is dangerously insecure and susceptible to hacking, machine malfunctioning, and Election Day disruption,” the authors write. “... It is critical that we begin building our defenses to protect against election intrusions before it is too late.”

Meanwhile, the Defending Digital Democracy program has issued a handbook offering guidance on how political campaigns can help make elections more secure. Written by a wide-range of security experts, including the CSOs of Facebook and Aetna, the Cybersecurity Campaign Playbook offers best-practice guidance on topics like using cloud services, two-factor authentication, and strong passwords.

The Defending Digital Democracy program is run by the Belfer Center for Science and International Affairs at the Harvard Kennedy School. The program was established last year, and its leadership includes top campaign officials from both the Republican and Democratic parties.

“Cyber adversaries don’t discriminate. Campaigns at all levels—not just presidential campaigns—have been hacked. You should assume that you are a target,” the playbook says.

CONTAINMENT STRATEGIES

MORE THAN 200 labs in the United States conduct research on hazardous pathogens, such as anthrax bacteria and the Ebola virus. These are called high-containment laboratories. Sometimes, security lapses occur.

For example, in May 2015, the U.S. Department of Defense (DoD) discovered that a DoD laboratory had inadvertently shipped live anthrax bacteria to nearly 200 other laboratories worldwide over the course of 12 years.

Then in late 2016, the U.S. Department of Homeland Security (DHS) discovered that a private laboratory had inadvertently sent a potentially lethal form of ricin to one of its training centers multiple times since 2011. (For more background on lab safety breaches from Security Management, see “Lax Lab Safety,” November 2014.)

Given these lapses, the U.S. Government Accountability Office (GAO) recently examined the oversight of these labs. Under the current system, high-containment laboratories are regulated by the Federal Select Agent Program, which was established to regulate the use and transfer of select agents in response to security concerns following bioterrorism attacks in the 1990s and early 2000s.

Two agencies share oversight responsibilities for this program: the Division of Select Agents and Toxins in the Centers for Disease Control and Prevention (CDC) and the Agriculture Select Agent Services within the U.S. Animal and Plant Health Inspection Service (APHIS).

To measure oversight, the GAO formulated five key elements of effective oversight for programs where low-probability adverse events (such as a toxic spill) could have far-reaching effects.

Independence. The organization conducting oversight should be structurally distinct and separate from the entities it oversees.

Ability to perform reviews. The organization conducting oversight should be structurally distinct and separate from the entities it oversees.

Technical expertise. The organization should have sufficient staff with the
expertise to perform sound safety and security assessments.

**Transparency.** The organization should provide access to key information, as applicable, to those most affected by operations.

**Enforcement authority.** The organization should have clear and sufficient authority to require that entities achieve compliance with requirements.

The GAO’s report focused on two questions. Does the Select Agent Program have effective oversight, and do strategic planning documents guide its oversight efforts? What approaches have other selected countries (such as the United Kingdom and Canada) and regulatory sectors used to promote effective oversight?

On the first count, the GAO found that the Select Agent Program’s oversight is sometimes inadequate. For example, the program is not always structurally distinct and separate from the labs it oversees, so it does not fulfill the key component of independence.

The program also fell short in the area of performing reviews, the GAO found. There was no assurance that the program’s reviews were targeting the highest-risk activities because the program had not assessed which activities pose the highest risk. In addition, the program does not have joint strategic planning documents, including a joint workforce plan, to guide its shared oversight efforts.

On the second count, the report found that the program could learn from other countries when it came to oversight. For example, the United Kingdom’s Health and Safety Executive, which oversees laboratories that work with pathogens, is an independent government agency, distinct from any of the labs it oversees.

And when it comes time for reviews, regulators in both the United Kingdom and Canada apply a risk-based approach by assessing laboratories, and then targeting those that conduct higher-risk activities or have a documented history of performance issues.

In response to the report, the U.S. Departments of Agriculture and Health and Human Services will outline actions they will take to improve oversight.

Go to SM Online for a link to the GAO’s report.

---

**The United Kingdom and Canada apply a risk-based approach.**

---

**Electro-mechanical High Security**

*ABLOY SECURITY*

an ASSA ABLOY Group Brand

1 800-367-4598
In Canada 800-465-5761

e-mail info@abloyusa.com

www.abloyusa.com

For product info #7 securitymgmt.hotims.com
Moreover, the document serves as a call to action to the private sector for its help in discovering and developing technology that will help DHS tackle some of its biggest challenges.

DHS Senior Industry Advisor Kathleen Kenyon acknowledges that this isn’t the first time DHS has reached out to the private sector for help in developing new technologies for government use, but this time around, officials are being more specific—and transparent—about the types of advancements they are willing to invest in.

“In the past, when we’ve talked to the private sector, many asked us what we need, and when, and how,” Kenyon says. “This time, we took a concerted effort to go into a little more detail, to really explain to industry not only what we need but where we’re investing our dollars and the types of technology we are looking for.”

Technology-sharing partnerships between DHS and the private sector have long faced challenges due to slow procurement processes, cancelled contracts, and a lack of detailed communication about exactly what S&T is willing to invest in. The directorate is stepping up its efforts to build a bridge between the public and private sectors—in addition to the industry guide, it’s conducting online and in-person outreach efforts. New contract rules that shorten application response times, as well as programs reaching out to nontraditional partners, take away some of the pain associated
Public-private partnerships will be mutually beneficial, allowing private organizations access to government funding.

with working with the government.

One such effort is the Silicon Valley Innovation Program, which allows startups to apply for a contract and receive government feedback more quickly—many contracts are issued within 10 days, Kenyon says, allowing companies to make investment decisions early on.

“I do understand the industry’s hesitancy to work with the government—we hear that quite a bit—so we want to take that information and translate it into ways that we can be more agile,” Kenyon says. “We’re trying to be a little quicker when it comes to working with us—speeding up deals and money and how we work and brainstorm together.”

Kenyon stresses that public-private partnerships will be mutually beneficial, allowing private organizations access to government funding and business. Additionally, Kenyon notes that the industry is only as secure as the government, so a more capable public sector means stronger business.

“Industry leaders like those in ASIS are security professionals who are looking to secure their company and contribute to the larger effort of securing the nation,” Kenyon says. “We want to make sure we are really reaching those who can be impactful in their own organizations to help secure the nation.”

S&T’s industry guide serves as a touchstone for the private sector and names six mission areas: securing aviation, securing borders, preventing terrorism, protecting from terror attacks, securing cyberspace, and managing incidents. Additionally, the document outlines the types of solutions it seeks from industry partners: future innovations, near-term capabilities, and new applications of existing technologies.

“The vast majority of what we’re looking at is going to be near-term or adapting in some way existing technology, because we have urgent needs right now that our homeland security operators need to have in use and be out in the field,” explains Melanie Cummings, deputy director of private-public partnerships. “We know there’s a lot of low-hanging fruit out there in terms of sensing and detection technologies that might not be an exact fit for a particular application, but we can modify and combine some things to get them out on the streets.”

This most recent push by DHS S&T to make meaningful connections with private sector manufacturers comes at a time when corporations are far outpacing the government in terms of research and development, Kenyon explains. Additionally, agencies are more often turning to off-the-shelf solutions, and Kenyon envisions a type of marketplace that would allow companies to tweak these solutions to perfectly fit governmental needs, as they would for any client.

FOLLOWING A DISASTER, the issues surrounding the mental health issues affecting both rescuers and survivors are frequently overlooked. Integrating Emergency Management and Disaster Behavioral Health is an excellent exploration of the topic, written by multiple contributors. Looking at mental health from both emergency management and behavioral health perspectives allows the authors to seamlessly transition between these two disciplines and make a convincing argument that both need to be considered throughout each stage of disaster management.

While the book sometimes reads like a research paper, the topic is fascinating. The chapters include ample references and diagrams to convey both the seriousness and credibility of the material. Real-world examples illuminate the text. Some chapters explore topics in a depth that may be too advanced for general security practitioners, especially those not involved with planning or coordinating emergency response efforts.

The ideal audience for this book would be emergency managers and those seeking to learn more about this discipline. The book would be a great addition to training courses on the National Incident Management System because those learning about emergency management for the first time would be exposed to the behavioral health implications following a disaster. Individuals working with or studying human behavior, such as clinical psychologists, mental health counselors, and aid workers, will also find value in understanding how people individually and collectively react to the stress of major disasters.

Overall, this book presents a unique and desperately needed argument for integrating two vital but sometimes distant disciplines. At a time when factions debate over what constitutes mental illness and what such a diagnosis means, this book becomes a timely resource.

REVIEWER: Yan Bivalk, CPP, is the security administrator for the City of Newport News, Virginia. He has 18 years of security experience in multiple industries, managing security officers, campus security officers, and special conservators of the peace. Bivalk is the assistant regional vice president for ASIS Region 5A in Southeast Virginia.
“The private sector is far outpacing us when it comes to research and development and spending billions of dollars more than we are on it, and in some cases they’re ahead of us,” Kenyon says. “How do we tap into that knowledge base and technology development so that the technology they’re developing can also be used by DHS?”

Kenyon describes the marketplace as one where a product could be used by U.S. Customs and Border Protection agents and commercial companies alike. The U.S. Department of Defense (DoD) has done this successfully for decades, she notes, but DHS’s breadth and people-based agencies require more specific products.

“We have a much more diverse mission set, and that requires us to explain better to our customers and technology developers, and those who also commercialize technology and put it in the marketplace, what our needs are,” Kenyon says.

Donald Zoufal, CPP, an independent consultant with CrowZnest Consulting, Inc., says S&T’s efforts are a long time coming—and seem promising.

“There’s always been a lack of communication, particularly on the government side, in terms of clearly articulating what its priorities are,” Zoufal tells Security Management. “We don’t know what the requirements and priorities are, so it’s hard for us to attune our R&D initiatives to meet those requirements.

I think this is a really positive step—it’s recognition by the government that if they’re more clear in providing direction about where they want to put their money, the market will positively respond to that. A lot of times DHS has paid lip service to the notion of partnership, but I see this as a really concrete effort to try to move that forward.”

Zoufal worked at Chicago’s Department of Aviation in the early 2000s and said the S&T industry guide touches on challenges he saw in airports—the upgrading of aviation security technology after 9/11 and the off-the-shelf purchases local agencies made to try to solve urgent problems in security.

“In a nutshell, this addresses a long-standing set of concerns that go back to when I was a security director at O’Hare and Midway, seeing big technology issues as inline baggage screening was brought in to replace other machines,” Zoufal explains. “This cooperative spirit is much needed and will benefit the...
industry in being able to understand the direction the government wants to go in, but also for government to understand that there may be other technologies out there that are able to help.”

S&T is looking ahead, too. The industry guide details its research and development investment outlook through 2021, outlining specific technologies it hopes to invest in.

“We really want to look at and be aware of what’s coming over the horizon, what technologies will be in place in five to 10 years, that are either going to change the way we operate, or that might potentially become threats to the homeland,” Cummings notes.

However, some private sector organizations may be wary of working with the government to develop an idea from the ground up, Zoufal says.

“Part of the problem with working with the government is that as administrations change, priorities change, so the current priorities may not be the same if there’s an administration change in three years,” Zoufal explains. “When you think about R&D and the investment of time, money, pace, and the lag to develop a new product, it’s a dedicated effort. Businesses tend to plan in long-term strategies, and the government may talk in those terms but oftentimes doesn’t plan as well. Better communication will help with that.”

Zoufal, who also teaches a course about homeland security technologies at the University of Chicago, says that the industry guide seems to be a sign of an attitudinal shift at DHS to connect with the private sector. However, the success of the outreach lies in the follow-through, he says.

“This part is the easy part—information sharing on the front end, brainstorming, discussing it,” Zoufal explains. “But at the end of the day, the part of this process that will be the most challenging is addressing technology issues in the procurement cycle. Having technology tested and procured and fielded is the part that’s probably more bedeviling than general intelligence about what they are looking for.”

Cummings says that S&T has already begun committing resources to show the private sector that the partnership will be a successful one—from start to finish.

“We’re putting a lot of our programs and non-R&D dollars into making sure that the technologies that we’re developing are getting out in the field and being commercialized for those operators and end users who primarily buy in the commercial market,” Cummings explains. “Beefing up commercialization, our transfer program, and working with the private sector manufacturing and distribution channels are priorities for us over the next fiscal year.”
So, when the Denver Police Department deployed shot-spotting technology in its districts with the most gunfire, the department knew it had an opportunity to add to its investigative abilities.

“When cops go to the scene of a shooting, they are fairly certain there are shell casings in that area, so they try to find them, rather than just rolling by,” says Lieutenant Aaron Sanchez of the Denver Police Department. “Because ShotSpotter triangulates to about nine to 25 meters from where the gunshots were heard, the officers go to that specific point, work their way out a little bit, and then recover those shell casings,” he says.

Detectives can merge the shell casing number with information from the U.S. National Integrated Ballistic Information Network (NIBIN), which tracks weapons usage. Denver’s police department has a program with the U.S. Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) to submit NIBIN numbers to federal law enforcement.

“NIBIN is basically the fingerprint of a gun,” Sanchez explains. “We set up an entire protocol on how to search for, recover shell casings, and separate them in case there’s a couple different weapons, and how to place those into evidence so they go to our ATF contractors.”

ATF then provides Denver police with more information on where that weapon’s shell casings have previously been recovered. “We can place that gun at the shooting, and that information goes to whatever investigative team needs it.”

ShotSpotter works by detecting gunfire, which has to hit three different audio sensors installed around the monitored area. When the correct succession of sensors goes off, a ShotSpotter technician reviews the audio to verify it is indeed gunfire. The technician then tells police that there have been shots fired, and an alert is sent out to officers on patrol.
The department’s data analysis unit identified the three geographical areas in Denver where gunfire, 911 calls related to gunshots, and gang violence are the highest. ShotSpotter was installed in those three neighborhoods in January 2015, April 2016, and August 2016, respectively. In January 2018, the department expanded the technology to a fourth neighborhood.

ShotSpotter sent engineers to install the sensors in the appropriate areas. “ShotSpotter goes throughout the community, and it tries to put the sensors on public locations, but from time to time we have to go into a neighborhood and ask people to put them on their houses,” Sanchez says, noting the community was relatively receptive to the installations. “We thought it was going to take time, but within about two days, we had the houses that we needed.”

Even the timing and succession of gunfire have played a role in bringing criminals to justice. ShotSpotter stores the recordings so that investigators can look back as long as the technology has been around. This helped Denver police solve a crime that was close to being ruled as self-defense, Sanchez says.

At a family gathering in a Denver neighborhood, a man shot another man, who died. The man who survived claimed it was in self-defense, saying he had just been shot moments before by the victim. Homicide detectives knew ShotSpotter was installed in that part of the city, and decided to pull the audio to verify the man’s story.

“So what they hear when they pull out ShotSpotter is one shot fired—boom—that’s the shot that shoots the first victim,” Sanchez says. “There’s then a five-minute gap, and then there’s shots fired again.”

Investigators were able to piece together that after being shot, the man had actually left the gathering to obtain a weapon. He came back, and killed the victim. “So now there’s premeditation. It wasn’t self-defense, and the only way homicide knew that was the differential in time,” Sanchez notes. “We brought back all the witnesses who said ‘yes, that’s the way it happened.’”

Denver police have access to a mobile app from ShotSpotter available on the iTunes store and Google Play. The app alerts officers when there are shots fired and displays the location on a map. A report view allows officers to review incidents from the last 24 hours, three days, or seven days and listen to the audio. “If the ShotSpotter app is on their phone, officers are getting that information within 30 to 45 seconds from the time shots were fired,” Sanchez notes.

ShotSpotter also keeps a historical record of all gunfire since the time the technology was installed. In one case, a man growing marijuana on his property was arrested for shooting two youths who were trespassing. A witness made the remark that the shooting was “just like last year.” Using ShotSpotter’s historical record and investigating further, police were able to trace yet another shooting back to the same gunman.

In rare cases the technology picks up on a false alert that isn’t truly gunfire, like the time a local man set off a propane bomb. In one homicide case, the gunshots set off several sensors when the noise echoed through a canyon, but failed to triangulate. “The sensors picked up the shooting for a mile and a half, but not just three sensors—a whole bunch of sensors,” Sanchez notes. The homicide unit was still able to use that information in its investigation.

Sanchez emphasizes that ShotSpotter combined with other investigative tools is what helps the department solve crimes. “When you just take ShotSpotter for what it is, it detects gunshots...So we’re using the technology as part of a bigger investigative strategy.”

FOR MORE INFORMATION: Jane Soderberg, jsoderberg@shotspotter.com, www.shotspotter.com, 720.361.6866

! STATS

U.S. Crimes Reported in 2016

<table>
<thead>
<tr>
<th>Violent Crime</th>
<th>Total: 1,248,185</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aggravated Assault..........</td>
<td>64.3%</td>
</tr>
<tr>
<td>Robbery........................</td>
<td>26.6%</td>
</tr>
<tr>
<td>Rape (Legacy Definition)....</td>
<td>7.7%</td>
</tr>
<tr>
<td>Murder........................</td>
<td>1.4%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Property Crime</th>
<th>Total: 7,919,035</th>
</tr>
</thead>
<tbody>
<tr>
<td>Larceny-Theft ................</td>
<td>71.2%</td>
</tr>
<tr>
<td>Burglary .....................</td>
<td>19.1%</td>
</tr>
<tr>
<td>Motor Vehicle Theft ..........</td>
<td>9.7%</td>
</tr>
</tbody>
</table>

SOURCE: CRIME IN THE UNITED STATES, FBI, NOVEMBER 2017
“I was sitting in the front row there, just shaking my head and praying everything would work out the way it was supposed to,” says Lisa Wiswell, former U.S. Department of Defense (DoD) bureaucracy hacker who oversaw the bug bounty program.

And work, it did. Dubbed “Hack the Pentagon,” the program allowed 1,400 security researchers to hunt down vulnerabilities on designated public-facing DoD websites. More than 250 researchers found and reported those vulnerabilities to the DoD, which paid them a total of $150,000 for their efforts.

“It’s not a small sum, but if we had gone through the normal process of hiring an outside firm to do a security audit and vulnerability assessment, which is what we usually do, it would have cost us more than $1 million,” Carter said in a statement.

Based on the program’s success, the DoD launched “Hack the Army” in 2016, followed by “Hack the Air Force” in 2017, to continue to address security vulnerabilities in its systems. This method of crowdsourcing cybersecurity is one that many organizations are turning to as they continue to struggle to recruit and retain cyber talent.

According to the most recent Global Information Workforce Study, the cybersecurity workforce gap is on pace to increase 20 percent from 2015—leaving 1.8 million unfilled positions by 2020.

Workers cite a variety of reasons why there are too few information security workers, and these reasons vary regionally; however, globally the most common reason for the
Sixty-eight percent of professionals believe there are too few cybersecurity workers in their department.

Worker shortage is a lack of qualified personnel,” according to the report’s findings. “Nowhere is this trend more common than in North America, where 68 percent of professionals believe there are too few cybersecurity workers in their department, and a majority believes that it is a result of a lack of qualified personnel.”

To help address this issue, study respondents reported that more than one-third of hiring managers globally are planning to increase the size of their departments by 15 percent or more. However, the report found that historically, demand for cybersecurity talent has outpaced the supply—which will continue to exacerbate the current workforce gap if the trend continues.

“It is clear, as evidenced by the growing number of professionals who feel that there are too few workers in their field, that traditional recruitment channels are not meeting the demand for cybersecurity workers around the world,” the report explained. “Hiring managers must, therefore, begin to explore new recruitment channels and find unconventional strategies and techniques to fill the worker gap.”

One technique to fill the worker gap is being used by the FBI, which has a long history of workforce training and development to keep agents—and Bureau staff—at the top of their game to further its mission.

In an appearance at ASIS 2017, FBI Director Christopher Wray explained that the Bureau has created a training program to identify individuals with cyber aptitude and train them so they have the skills necessary to identify and investigate cybercrime.

“We can’t prevent every attack or punish every hacker, but we can build our capabilities,” Wray said. “We’re improving the way we do business, blending traditional techniques, assigning work based on cyber experience instead of jurisdiction, so cyber teams can deploy at a moment’s notice.”

In an interview, Assistant Section Chief for Cyber Readiness Supervisory Special Agent John Caliano says the FBI is looking internally to beef up all employees’ cyber abilities.

“There is a notional thought that all the cybersmart people are in the Cyber Division,” he adds. “There are a lot of very talented people outside the Cyber Division, some have worked in other areas...the goal is to start to pick up in the investigative realm and lift the abilities of all employees, so they have a basic understanding of cyber and digital threats today.”

To do this, the FBI has employees undergo a cyber talent assessment which looks at the skill sets they brought with them when they were hired, the skills they have learned on the job, and their aptitude for formalized and informalized training on cybersecurity and technology.

The FBI then sorts employees into three categories: beginners, slightly
advanced, or advanced. Employees are then sent to outside educational courses, such as those provided by the SANS Institute or partnering universities, to learn more about cybersecurity and bring that knowledge back to the FBI. The FBI also works with the private sector to embed employees to teach them specialized skills, such as how SCADA networks operate.

In 2016, Caliano says, the FBI identified 270 employees for cyber training who were not part of the Cyber Division. Approximately two-thirds of those employees were categorized as beginners at the outset, and Caliano says the Bureau plans to continue the assessments and training for the foreseeable future.

And for its specialized teams, the FBI is continuously developing in-house training that will eventually be offered to the entire FBI.

“One day, all FBI employees will take these courses and pass these courses,” he says. “People will understand what depth and defense mean, how to secure networks, and trace IP addresses.”

These specialized teams include its Cyber Action Team (CAT), which is made up of employees who deploy when a major cyber incident occurs. For instance, when the Sony hack occurred in 2013 the initial FBI response team had a few members who were also CAT members who were sent to the scene.

Once the FBI became aware of the severity of the incident, it sent a full CAT to Sony’s headquarters to sit with the network operators to comb through their logs to see how the attack spread.

While this training provides professional development opportunities to current employees, the FBI is also focused on identifying future talent that can be recruited into the FBI.

“We can’t compete with dollars, but we can compete on mission,” Caliano says, adding that the FBI often gets to look at cyber threats and address them in a way that the private sector does not, providing employees a “deeper sense of fulfillment.”

To attract talent, the FBI has a variety of initiatives including an Honors Intern Program open to all college students. It also has a postgraduate program where the FBI will pay for a graduate or doctoral student’s degree.

It’s also reaching out to students at the high school level through its Pay It Forward program, which engages students in math, science, and technology who might show cyber aptitude.

“We are, as a workforce planning objective, training at schools—driving down to the high school level,” Caliano tells Security Management.

Another new recruiting channel has been championed by Wiswell since she left the DoD in 2017. After leaving the public sector, she went to work at GRIMM, a cybersecurity engineering and consultant firm, as a principal consultant. One of her main responsibilities is to oversee its GRIMM Academic Partnership Program that runs the HAX program.

Through HAX, undergraduate cybersecurity clubs can participate in friendly competitions and gain hands-on cyber experience. GRIMM has partnered with Penn State University at Altoona’s Security Risk Analysis Club and Sheetz Entrepreneurial Fellows Program, the Michigan Technological University (MTU) Red Team, George Mason University Competitive Cyber Club, and the Rochester Institute of Technology’s Rochester Cybersecurity Club.

Throughout the academic year, participants in HAX break into teams to complete programs designed by GRIMM engineer Jamie Geiger that are similar to computer Capture the Flag challenges. While participants have the option to compete individually, Wiswell says she encourages students to create a team to hone their communication skills.

“A lot of this field has an individualist focus a lot of the time, and what’s really needed is the ability to communicate well, both up and down, to work well on teams, and to have effective analytical skills,” she explains. “The kinds of things that you learn well by doing...
GRIMM chose these programs in particular to create a talent pipeline for the company, which has offices in the Washington, D.C., area and in Michigan—near two of the universities it’s partnered with. By engaging college students through HAX, GRIMM hopes to create a talent pipeline and increase diversity on its own staff.

“HAX is an effort to do both those things,” Wiswell says. “We are kind of do-gooders on one hand. If folks that are participating in the program have no interest in coming to work for GRIMM, that’s fine. We just hope that they use their talents and go somewhere.”

That’s why the challenges and the experience to connect with people working in cybersecurity are important, according to Wiswell, because it helps students make informed decisions about what they would like to do after graduation.

“We’re trying to think outside the box in ways that students feel very well rounded, so students can make decisions on what sliver of this workforce is most interesting,” Wiswell says, explaining that current challenges are focused on Linux and Microsoft systems, but in the future, might include hardware and other areas.

And to gain even more experience before graduation, Wiswell says she encourages students to take part in bug bounty programs to get connected to companies that might one day hire them.

“If you already have a lot of good skill and you’re trying to hone skill—and make some cash—we think that bug bounty programs are a great way to do that,” Wiswell explains to Security Management. “GRIMM is partnered with a couple bug bounty as a service providers to help them get in a broader group of individuals who are interested in participating, as well as companies that could benefit from hosting bug bounties themselves.”
The Las Vegas massacre on October 1, 2017, surpassed the 2016 Orlando Pulse Nightclub tragedy as the deadliest mass shooting in recent U.S. history. Fifty-eight people lost their lives and hundreds were injured when a gunman rained down automatic weapon fire from the 32nd floor of a hotel suite on concertgoers below. Months later, investigators are still struggling to piece together a motive for the tragedy. They classify the shooter as a nondescript, wealthy retiree who spent tens of thousands of dollars gambling at casinos on the very strip he attacked. But these clues offer little insight as to why he would carry out such a deadly rampage.

In the wake of the tragedy, security professionals must grapple with the known facts surrounding the event, and investigators continue to revise the timeline of events as details emerge. However, as reported by CBS News, the assailant managed to take nearly two dozen weapons contained in luggage to his room via a freight elevator in the Mandalay Bay Resort and Casino.
A do not disturb sign hung on the door of his suite for 72 hours after he reportedly checked into the hotel on September 28. He shot out of two windows from the hotel tower after shattering them with a hammerlike device, according to The New York Times.

The assailant also shot a hotel security guard, who was responding to an open-door alarm on the same floor, around the time he began firing on the crowd.

Whether or not the hotel and Live Nation Entertainment, Inc.—the event company hosting the concert—met their legal duty of care during these circumstances has yet to be determined, and several lawsuits have been filed by victims.

Difficult questions regarding security have been raised by the shooting, including whether hotels should apply airport-style screening measures to guests as they enter the property, and whether it’s possible to spot suspicious behavior in guests before an incident occurs.

As investigators continue to probe into the specifics of the massacre, hospitality, event, and gaming security experts all agree: While the circumstances in the Las Vegas shooting are unlikely to happen the exact same way again, the event underscores the importance of having strong security policies and procedures, staff training, and appropriate technological tools to combat future threats.

Event safety. The October shooting ravaged a section of the Las Vegas strip called Vegas Village, which has become a popular spot for festivals and other live events. The gunman attacked concertgoers at the sold-out Route 91 Harvest Festival, which featured country music performers. The event was growing in popularity, and attracted about 25,000 people a day last year, the Los Angeles Times reported.

Steven Adelman is an attorney at Adelman Law Group, PLLC, and vice president of the Event Safety Alliance, a nonprofit he helped form after a stage collapsed at the Indiana State Fair in 2011, killing seven people. He emphasizes that the Las Vegas shooting and the circumstances surrounding it are unlikely to repeat themselves, and calls the incident a “black swan” event.

“A black swan is a highly unusual, impactful event—and in retrospect people suddenly think it was inevitable,” Adelman says. “Las Vegas fits that profile. There had never been a shooting at a live event venue from a great elevation or from an adjacent building.”

While the University of Texas clocktower shooting in 1966 in Austin harkens closely to the positioning of the shooter, experts say it does not make what happened from the 32nd floor of the Mandalay Bay Hotel and Casino foreseeable.

“If we had been talking on September 30, the day before this happened, and you had asked me what the most reasonably foreseeable threat at a live event space is, based on what’s happened over the last year...it probably would have involved a truck,” he says, referencing the vehicular terrorist attacks that have occurred in cities including Barcelona, New York City, and Stockholm.

While Vegas may not have been preventable, Adelman underscores the best practices that can be applied to event safety moving forward.

“When there is an adjacent building to a live event, where someone potentially has a perch over a site where people are gathered, law enforcement and security should have eyes on that building,” he notes. “In fact, the smarter trend, if it’s in one’s control, is to just clear the building.”

At a major event in Phoenix just weeks after the shooting, event organizers did exactly that. Law enforcement cleared a nearby parking structure and used the building to have a crow’s nest vantage point over the event.

“That’s the kind of positive learning experience that can be applied from a
horrific event like the Vegas shooting,” Adelman adds.

Also, having a no-weapons policy is a simple way to at least deter people carrying guns, Adelman says, but he concedes that enforcing that policy is another matter. When possible, event organizers should limit the points of ingress and egress for attendees, and deploy magnetometers at each of those points.

“Make sure that applies equally to the production people, and even the talent who are doing set-up,” he adds. “Make sure the artists and their entourage all go through these magnetometers and security guard scrutiny while we’re at it, because they can have weapons, too.”

Adelman adds that the special event industry could spend all its time and resources focusing on trying to prevent black swan events, and he emphasizes that the key is to triage the reasonably foreseeable risks.

“You should spend your finite amount of resources addressing the risks that are most likely to happen at whatever venue or event it is that one is talking about,” he says. “That’s the reasonable thing to do.”

**Hotel security.** There is no one-size-fits-all approach for hotels when it comes to their security programs, says Russell Kolins, chair of the ASIS International Hospitality, Entertainment, and Tourism Security Council.

“Each hotel has its own culture of management, its own corporate attitude, so each hotel is going to address its properties differently than their neighbors next door,” Kolins adds.

This means that each property or hotel chain must constantly reinforce whatever safety protocols it has in place across management, staff, and guests.

Many hotel properties have policies on weapons, which vary from state to state. Nevada is an open-carry state, though most casinos don’t allow patrons carrying a gun to enter the property. Hotels have typically allowed hunters with weapons permits to carry guns to their rooms or store them in lockers. Kolins says a weapons check

Gaming Community Reacts to Vegas Tragedy

**CASINOS** are no strangers to security. With swaths of surveillance cameras, guards, and cash-protection measures, these venues are used to large volumes of people toting valuables. Most gaming properties have no-guns policies, and uniformed and plainclothes security officers keep careful eyes on the property.

Guests at casinos are looking for privacy and comfort, so hospitality professionals must strike a balance between providing security and making sure their clients feel at ease.

“Most security has to be unobtrusive, yet effective,” says Dave Shepherd with the Readiness Resource Group and a member of the ASIS International Gaming and Wagering Protection Council.

“We’re not trying to prevent people from crossing a border or boarding an airplane. We have to be very cognizant of the rights of people as they are coming onto the properties.”

In the wake of high-profile incidents, an opportunity arises to engage the C-suite, says Alan Zajic, CPP, with AWZ Consulting and chair of the Gaming and Wagering Protection Council.

“Any security director knows that when an event like what happened in Las Vegas occurs, your bosses are going to be asking you what you intend to do,” he says. “That’s the greatest opportunity to say, ‘I need a commitment out of you to be able to put some of these programs into place and help protect our employees and our guests.’”

He explains that gaming properties should prioritize training employees on situational awareness, and proposes a technique.

“Most security has to be unobtrusive, yet effective,” says Dave Shepherd with the Readiness Resource Group and a member of the ASIS International Gaming and Wagering Protection Council. “We’re not trying to prevent people from crossing a border or boarding an airplane. We have to be very cognizant of the rights of people as they are coming onto the properties.”

In the wake of high-profile incidents, an opportunity arises to engage the C-suite, says Alan Zajic, CPP, with AWZ Consulting and chair of the Gaming and Wagering Protection Council.

“Any security director knows that when an event like what happened in Las Vegas occurs, your bosses are going to be asking you what you intend to do,” he says. “That’s the greatest opportunity to say, ‘I need a commitment out of you to be able to put some of these programs into place and help protect our employees and our guests.’”

He explains that gaming properties should prioritize training
would have to be conducted on every guest and bag to enforce these policies. “If someone wants to get a weapon up to their room, they are going to do it, unless you’re inspecting every single bag and every single piece of luggage, including clothing bags,” Kolins says. “It’s not going to be absolutely controlled.”

Technology already plays a major role in hotels, says Stephen Barth, a professor of hospitality law at the Conrad N. Hilton College of Hotel and Restaurant Management at the University of Houston. “Hotels employ a variety of technological measures to enhance security and the smooth flow of business for guests,” he says. “We’ve got significant technology that’s helped a lot—being able to track guests that go in and out, making sure a key is changed from guest to guest.”

Barth, founder of hospitalitylawyer.com, argues that adding on more technology for security purposes wouldn’t necessarily be rejected by guests, if it’s obvious it keeps them safer. “Technology for sure needs to be involved in these conversations,” he says. “What if every hotel window had a sensor on it so that if the glass was broken, the hotel would know immediately what floor and which room it was in?”

Management may hesitate initially to go to such measures, but Barth argues that security should keep it in mind as a possible option. “There’s going to be resistance, no doubt, but it does seem to me that there is potential,” he says.

Training. Security experts agree that hotel staff, including housekeeping, engineers, bellhops, and front desk workers are the most likely ones to observe unusual behavior among guests. Therefore, training those workers thoroughly and consistently will help reinforce what they can look for as suspicious or possibly harmful behavior. “There needs to be ongoing training, so that there is an awareness given to the employees to be the actual eyes and ears for security and management of a property,” Kolins says.

While metal detectors and individual bag checks may be a far-flung approach, staff can be trained on behavioral cues to look for in guests, such as the way someone walks when they may be carrying a weapon.

“I think the trend now for all the hotels is going to be to take the See Something, Say Something campaign and make it effective,” says Darrell Clifton, CPP, executive director of security at Eldorado Resorts in Reno, Nevada, and a member of the ASIS Hospitality, Entertainment, and Tourism Security Council. “Right now
Housekeeping, engineers, bellhops, and front desk workers are the most likely ones to observe unusual behavior among guests.

it’s kind of a shotgun approach. If it’s working right, you get 10,000 pieces of data and 9,999 of them are useless, and it’s hard to comb through all that.”

Instead of just repeating the See Something, Say Something mantra, he says that managers should sit down with employees and tell them exactly what to look for, and what to do with that information.

“Frankly, the housekeepers know what’s suspicious better than I do because they see all the different people that come into the hotel,” Clifton notes. “They know what looks right and what doesn’t look right.”

When it comes to room inspections, Kolins suggests hotels conduct safety checks at least every other day, even if a do not disturb sign is on the door. These check-ins give hotel staff the opportunity to verify that the various sensors in the room are operating properly, such as smoke detectors and carbon monoxide monitors.

“I think the biggest change with that will be reinforcing that policy, more than creating a new one, for most hotels,” Clifton notes, adding that most hotels have policies to check rooms every other day or more often, but have not enforced them consistently.

As of January, four Disney hotel properties had done away with the do not disturb sign, The New York Times reported, swapping it out for a “room occupied” sign and alerting guests that staff may check on the room. In December, Hilton revised its policy to still allow the signs but will conduct a staff-led alert system if it stays up for more than 24 hours.

The data collected at these check-ins, as well as any other security concerns reported to management, should all be kept in a log.

“The security industry is data-driven, and it’s very important to record anything that gets reported,” Kolins notes. “And on a periodic basis, whether it’s a weekly basis or bimonthly basis, the reports should be part of an incident log.”

Down the road, these data points can be connected and lead to an impending threat or other incident, he says.

**Duty of care.** The Las Vegas shooting raises the question of duty of care—the reasonable level of protection a venue is legally obligated to provide its guests—and whether or not Mandalay Bay and Live Nation met that standard.

A victim who survived the shooting has already filed a lawsuit, and there is the potential for more litigation. In the suit filed against MGM, which owns Mandalay Bay, the plaintiff argues that the hotel failed to “maintain the Mandalay Bay premises in a reasonably safe condition,” according to court documents.

From a legal standpoint, Adelman says the hotel property or venue hosting an event has an obligation to provide a reasonably safe environment for its guests under the circumstances.

Experts say a number of factors come into play in the legal process, including whether the hotel followed its own security policies and procedures.

“I think most juries and most judges would argue, at least until now, that the event was not foreseeable in the United States,” Barth says.

Given the fact that the shooter brought in a cache of weapons and fired from a hotel suite, Barth says the property’s policies and procedures will come into question.

“Responding to a particular incident is a part of the duty of care in places of public accommodation like hotels,” Barth notes. “So, you would want to consider, what was their protocol for an active shooter situation? Did they have training, what was their communication system setup, what was supposed to happen, and did they in fact follow their training?”

He adds that the facts surrounding the Vegas shooting as investigators understand them are not necessarily unusual.

“This fellow in Vegas specifically requested a particular room. In and of itself, that happens all the time in a hotel,” Barth says. He adds that people travel to Las Vegas to gamble or party, and often stay up all night and sleep during the day. “This fellow also had a do not disturb sign on his door for 72 hours. Again, that in and of itself is not a big deal, particularly in Vegas.”

The large containers the weapons and other items were stored in wouldn’t necessarily sound the alarm bells, he notes. In a city like Las Vegas, convention exhibitors frequently bring large containers to their rooms, and guests who gamble may be protecting valuables such as cash.

The duty of care applies equally to event venues as it does to hotels, Adelman says. “The main duty for providing a safe and secure environment generally falls on the shoulders of the venue,” he points out, noting that the venue should know what its biggest risks are, and what resources are available to address those risks.

He adds that, when necessary, the location can contract with a private security company or with law enforcement to take on some of the security responsibilities.

All properties should take an all-hazards approach to security, paying just as much attention to the threat of a natural disaster as an active shooter. “The threat you prepare for probably isn’t going to be the precise threat that actually appears on your doorstep,” Barth says.

**HOLLY GILBERT STOWELL** is Associate Editor at Security Management. She can be reached on Twitter @HOLLYWGILBERT.
Several years ago, at a Milwaukee-area hospital, a patient came into the emergency room for treatment. The patient was flagged in the hospital’s system for a history of violent behavior; he was known to carry weapons. However, the attending nurse ignored the warning to involve hospital security and proceeded to provide care to the patient. During the triage process, the patient made several comments to the nurse, including threats to cut her with a knife. Instead of disengaging for her own personal safety and notifying hospital security, she continued triaging the patient. The nurse later filed a complaint about an unsafe work environment, and when asked why she continued triaging the patient even though he threatened physical harm, the nurse responded, “I have a job to do, and I had to triage him.”

Healthcare is one of the most violent professions in the private sector—the number of violent events in the healthcare workplace is on par with law enforcement and corrections. According to the U.S. Bureau of Labor Statistics, in 2015 all private sector industries experienced workplace violence at a rate of 1.7 incidents per 10,000 full time workers. However, those numbers jumped to an alarming rate in the healthcare industry—6.7 per 10,000 full-time workers at psychiatric or substance abuse facilities. At hospitals, the rate was even higher, with 8.7 per 10,000 full-time workers experiencing workplace violence. In such settings, security practitioners face the challenge of protecting both staff and patients—who are often the ones committing the violence.

With the focus on patient satisfaction, caretakers often forgo their own safety to produce results, creating a more unsafe work environment and potentially providing a lower level of care—when staff do not feel safe, they are less likely to spend time working with their patients, instead focusing on getting to the next patient as quickly as possible.

An unsafe work environment doesn’t just affect employees. Hospital surveys show that when patients choose a hospital, they base that choice on their experiences and what they have seen in emergency rooms or waiting rooms. When a patient feels comfortable and safe in a hospital that has subpar care, they will choose it over a hospital that has good care but a repu-
Adopting conflict management techniques can increase awareness and safety and achieve positive outcomes for staff and patients.

Context.

The concept of context encompasses all aspects of preparation for interaction within hospitals and clinics. Context begins with an understanding that, to produce positive outcomes, all people must be treated with dignity and respect, regardless of their background. Context also refers to knowing the inherent risks within the healthcare environment and planning for those risks through awareness of surroundings and escape routes.

Along with this awareness comes the possibility of encountering verbal abuse and conflict. To respond professionally, healthcare staff must understand that hot-button words can trigger an emotional response in the heat of the moment, leading to negative interactions resulting in workplace violence.

To set and enforce a social contract, a facility’s staff must identify triggers and develop safeguards to protect against an unprofessional response.

Keeping context in mind can help staff maintain a professional mindset by beginning interactions with patients on a positive note—if an individual or situation creates an uncomfortable atmosphere, healthcare workers should take a step back, take a deep breath, and conduct positive self-talk to encourage confidence.

Contact.

Caregivers should have a foundational understanding of a situation’s context to be mentally prepared to have positive interactions, which begin long before that first word is even spoken. Staff must take into account what message they are sending with their own body language and expressions. Understanding how nonverbal communication such as posture and facial expressions affects verbal communication can mean the difference between a positive and negative outcome.

Oftentimes caregivers focus on the task at hand and overlook crucial nonverbal warning signs from the patient, such as preattack postures or targeted glances at items the caregiver might be carrying such as pens, clipboards, or stethoscopes around the neck. Along with body language, understanding personal space has an equally important role in positive contact—entering an individual’s personal space begins to put pressure on them, and if individuals are angry and upset, encroaching on their space may begin to escalate.
their behavior because they feel that they are being cornered.

A real-life example of this happened not too long ago in a psychiatric facility when a nurse announced to several patients in a common area that it was time to head back to their rooms for bedtime. Most of the patients complied, but one woman began backing herself into a corner. Instead of retreating and attempting to verbally persuade the patient to come to her room, the nurse got closer to the patient, who then barricaded herself with a table. Two additional nurses came in, causing the patient to move into “fight” mode—she flipped the table, threw a chair at one of the nurses, and physically attacked another. This example demonstrates that when people are in conflict, managing distance and maintaining appropriate personal space can help avoid a potential physical attack.

However, as part of routine care, doctors and nurses have to touch, poke, and prod patients without regard to their physical or emotional state, developing what is known as presumed compliance. This approach leads to a staffer’s complacency, giving them a false sense of security. If a caregiver has been assaulted, it is common to hear them say, “I’ve done this a thousand times and nothing ever happened before.” Before entering a person’s personal space, caregivers need to determine if it is safe and appropriate to do so.

When a caregiver approaches an individual, they should conduct an assessment at specific distance intervals (such as 10 feet, five feet, and two feet) to determine their own level of risk at each stage, allowing them to either continue or disengage. As they engage physically, a caregiver’s relative position comes into play. Standing directly in front of someone or towering over them can imply dominance, so caregivers need to be positioned in a manner that allows them to stay safe, as well as make the patient feel comfortable. Positioning at an approximately 45-degree angle to the patient and communicating at his or her eye level helps avoid an unintentional show of dominance and continue positive contact.

After establishing a comfortable position, caregivers should use professional language to introduce themselves and communicate effectively. Verbal interaction begins with a proper greeting—beginning contact with informal greetings like “hey” or “hi” may send the wrong message to the other person. Proper greetings should be professional and tactical to begin the interaction on the right foot without unintentionally escalating the situation. After the proper greeting, caregivers should introduce themselves and communicate effectively.
themselves, state the reason for the contact, and bring the other person into the conversation by asking a relevant question. These four steps to a proper greeting help mitigate potential conflict.

Verbal communication, however, is a two-way street. When gathering information to better meet the needs of their patients, caregivers need to go beyond active listening and understand the emotions behind the words, allowing them to use empathy to find the hidden meaning of the words being spoken. By combining the knowledge gained through observations of body language, personal space, and relative positioning, caregivers can make assessments that allow them to remain safe and communicate effectively. Positive contact fosters a supportive atmosphere, and when done well allows the interaction to move into closure. When done poorly, contact can move into conflict.

**Conflict.** Simply defined as “emotional violence,” conflict can lead to stressful work environments and contributes to high staff turnover, leading to negative patient outcomes. Conflict typically begins when the expectations of individuals are not met, and in the healthcare environment usually arises because of someone’s perceived lack of dignity and respect.

A few years ago, one of the security staff in a local hospital was watching a patient on a psychiatric hold. The attending nurse came in and offered to get the patient something to drink, suggesting apple juice. The patient told her that she hated apple juice and didn’t want it. The nurse insisted on giving her apple juice, to which the patient said that she would throw it in the nurse’s face. However, the nurse proceeded to bring her a carton of apple juice and, after handing it to the patient, had it thrown in her face, as promised. Conflict is more likely to occur when healthcare professionals fail to listen and forget that all people should be treated with dignity and shown respect.

When involved in conflict, a caretaker’s goal is to de-escalate tensions, return to normal conversation, and end with a positive outcome. De-escalating conflict begins by deflecting verbal abuse and redirecting it, focusing on managing gateway behaviors. Caretakers should then take the context they have gathered and put it into action by asking relevant questions, providing explanations, offering options, and finally giving a second chance. This technique is more likely to generate voluntary compliance, cooperation, and collaboration, which will lead to closure in conflict situations.

It is important to incorporate all elements of context and contact when involved in conflict. This allows caregivers to maximize their safety and conduct themselves in a professional manner that gives them the ability to set limits and reinforce the social contract. However, if staff members do not manage conflict properly, they can unintentionally escalate a situation into a crisis.

**Crisis.** Some events have the potential to lead to an unstable or dangerous situation affecting an individual’s ability to make good decisions. Anything can be a crisis—sudden bad news, a traumatizing event, a physical injury, or withdrawals from alcohol or substance abuse. Individuals with brain-based disorders may display rumbling or self-stimulating behaviors such as rocking back and forth, flicking fingers, making unusual noises, or displaying uncontrollable or unexplained twitching. Individuals with psychological disorders may experience visual or auditory hallucinations.

Any of these may be warning signs that the individual is entering a crisis. If these behaviors are observed quickly and caretakers intervene effectively, they can begin to bring the individual back to normalcy. If the behaviors are not recognized for what they are, the individual may
To set and enforce a social contract, a facility’s staff must identify triggers and develop safeguards to protect against an unprofessional response.

To reduce incidents of workplace violence, caregivers need to know they are supported in the actions they take. This begins with support from their leaders, encouraging caregivers to report workplace violence incidents when they happen. Additional support can be gained through partnerships with local and state law enforcement and legislators, and development of a comprehensive training program.

Through these mechanisms, healthcare professionals can learn the skills to effectively manage and reduce incidents of workplace violence. By adopting a comprehensive conflict reduction plan into healthcare, caretakers can establish an environment of care that is incompatible with conflict and violence.

**Ryan Weber** is Training Assistant, Loss Prevention Security at Aurora Health Care, and is trained by VISTELAR as an organizational instructor of the Six Cs Concept. His colleague **Dennis Hafeman**, Training Coordinator, Loss Prevention Security, contributed to this article.
To complete mandated threat assessments, the Ontario Provincial Police made an unprecedented move—it reached out to the private sector for help.

AN EXPERT PARTNERSHIP

IT WAS A MONUMENTAL TASK. The Ontario Provincial Police (OPP) needed to conduct security assessments of all the courthouses in the province it polices—approximately 100 locations—with only three people to carry out the work.

In an unprecedented move, Security Assessment Unit Sergeant Laura Meyers, PSP, proposed bringing in outside help from the private sector. Senior executives approved of the idea, and Meyers reached out to the ASIS Toronto Chapter to bring on Michael Thompson, CPP, PCI, PSP, and Gregory Taylor, CPP, PSP.

Both had public sector experience—Taylor was former military and Thompson a former Toronto police officer. Meyers thought those qualifications, along with their extensive security backgrounds, would not only help them conduct the assessments OPP needed, but also gain the respect of OPP officers they would be working with in the field.

Her predictions were correct. Taylor and Thompson were well received, and the project was completed on time without exhausting OPP’s resources—funding or personnel—to complete. It also marked a new era with OPP bringing security professionals in-house to assist law enforcement in addressing security threats.

THE MANDATE

In 2007, the province of Ontario issued the Ontario Public Service Physical Operating Policy, which required all public service facilities within the province to complete a physical security threat risk assessment.

The OPP, which polices more than 1 million square kilometers of land and waterways in Ontario, was subject to this mandate. It’s one of North America’s largest deployed services with more than 5,800 uniformed officers, 2,400 civilian employees, and 830 auxiliary officers.

To comply with the mandate, the OPP’s four-member Security Assessment Unit was assigned to carry out threat assessments of more than 200 facilities across the province. The four members went to each region and trained OPP staff at the facilities on crime prevention through environmental design (CPTED) strategy and the Royal Canadian Mounted Police’s (RCMP) Harmonized Threat Assessment Methodologies.

“It was like a mass attack for the four-person unit to do that within a couple of years,” Meyers says. “By 2011,
During that time frame, Staff Sergeant Rob Fournier was placed in charge of the newly created OPP Justice Officials Protection and Investigations Section (JOPIS). The section was created in 2009 to ensure the safety and protection of justice officials and to address threats, harassment, and intimidation directed at justice officials.

The Security Assessment Unit and JOPIS regularly began working together to address threats, and in 2015, JOPIS was instructed to complete physical security threat risk assessments on all justice facilities in the province.

Meyers and Fournier both knew it would be a major task to carry out the assessments, especially if they had to train additional OPP staff to conduct them.

“In the police world, when you’re building your team you’re looking for an individual with a ton of experience,” Fournier says. “In the security aspect, we have to use that same premise. Why would you want to be retraining someone in security work, when you can get someone who’s been involved for years?”

Meyers and Fournier were both active in the ASIS Toronto Chapter, so they pitched the idea of contracting out the justice facility assessments to a few security professionals they knew through the chapter.

The idea was approved, and Meyers and Fournier recruited two security professionals with certifications and backgrounds in the public sector—Thompson and Taylor.

**JUSTICE SITE VISITS**

After Thompson and Taylor were brought on board, they traveled to 92 different sites across the province—ranging from remote areas to urban settings, with everything from historic courthouses to courtrooms in mini plazas.

Their job was to review each site, evaluate the training protocols, and identify any gaps that might pose vulnerabilities, Fournier says.

Thompson’s and Taylor’s recommendations were critical at one site in particular following a series of events over a six-month period that impacted the security of the facility in eastern Ontario.

During that six-month period, a local individual murdered three former lovers. Law enforcement launched an extensive manhunt to locate the person. During that same time frame, an OPP officer was threatened and forced to temporarily relocate for personal safety. And there was another unrelated high-risk threat to an officer at the facility.

“‘There were obviously a bunch of people at that older facility, and it needed attention,’” Fournier says. Thompson and Taylor were able to take the previous threat assessment of the facility and suggest specific actions to take to address the new vulnerabilities due to the heightened threat environment.

The facility then improved its exterior parking lot lighting, and made other changes that Fournier could not disclose due to security concerns.

This process of going back to reassess facilities has helped the province distribute its funds to better address security concerns, Fournier says.

“It’s helped paint the picture when we’re earmarking where limited funds are going, to say, ‘This might not be on your list but it’s on ours,’ and that helps get things done sooner,” he adds.

**OPP SITES REVISITED**

While Thompson and Taylor were wrapping up the justice site assessments, the OPP decided to update its original threat assessments that were completed in the wake of the 2007 mandate.

“Some of the recommendations from that set were dated, not the best security practices,” Meyers says.
“So, we came up with a criticality schedule—how often we should revisit them...looking at it as a continual working project.”

To carry out this work, OPP once again reached out to the Toronto Chapter; this time to Chapter President Patrick Ogilvie, CPP, PSP. Meyers knew that Ogilvie was looking to both build his personal brand as a professional and give back to the community.

Ogilvie is currently conducting this second round of threat assessments, using the RCMP methodology that was established during the initial round. Having that first set of assessments has been a useful benchmark, Ogilvie says, to score threats and vulnerabilities and then make actionable recommendations for the facilities.

“Even before I step foot onto a facility, I communicate with commanders that I’m looking for documented evidence or stories of different threats and occurrences,” he adds. “I get them thinking not as police officers, but essentially as security people who can identify different threats and vulnerabilities that they have experienced.”

This is because sometimes a security threat hasn’t been identified by law enforcement because it is not a deliberate act—such as vandalism—that is intended to harm the facility.

For instance, Ogilvie says he found that most facilities did not identify building structure or leaks as vulnerabilities. “What I found in getting out and talking to [people] was that accidents were happening, natural hazards that could have an impact on our business, and our business is policing,” he explains. But because these threats weren’t identified, nothing was being done to address or mitigate them.

Ogilvie has made it a point to educate OPP personnel at the facilities that he’s looking at all threats—deliberate acts, accidents, and natural hazards—that could harm the organization. For instance, a leak in the facility could cause structural decay and ultimately become a hazard for personnel inside.

Thus far, Ogilvie says the OPP officers he’s interacted with have been receptive to his suggestions, and Meyers adds that the feedback she’s received has been highly positive—including that security deficiencies have been pointed out in a respectful manner.

Due to the success of the program, Fournier says that several First Nation police services across the province have reached out to OPP for assistance on conducting similar threat assessments.

Many of these facilities, especially in the northern part of Ontario, are in remote locations and have deteriorated or don’t adhere to the same standards as other facilities in Ontario. To address this, OPP is working with the police programs to conduct threat assessments of approximately 15 different sites.

The Security Assessment Unit has also been called on to provide assistance to Ontario government facilities—overviews, recommendations, and security advice—because they have proved themselves in the field.

It has also showcased how civilian personnel can be brought in to a law enforcement agency to help in addressing security concerns.

Ogilvie, Thompson, and Taylor are all under contract right now using existing funding that OPP secured. Down the road, Fournier says he hopes to change a few positions in the Security Assessment Unit to hybrid roles that either a police or civilian security professional could fill.

CONTACT ASSOCIATE EDITOR MEGAN GATES AT MEGAN.GATES@ASISONLINE.ORG. FOLLOW HER ON TWITTER: @MGNGATES. LAURA MEYERS, PSP, IS A SERGEANT IN THE ONTARIO PROVINCIAL POLICE.
Make 2018 the year you get CERTIFIED!

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

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

Distinguish yourself as the best of the best by earning the CPP, PCI, and PSP! Get started today at asisonline.org/certify2018

“It’s improved my skills, built my confidence in my professional proficiency, and put me on a level playing field with colleagues, thus earning their respect.”

Michael Brzozowski, CPP, PSP, Risk Manager, Symcor
The Strategic Leader

What happens when risk managers must contend with a variety of threats using limited company resources? Strategy takes center stage.

In this current era of enterprise security risk management (ESRM), there are no shortages of risks to contend with. Most surveys of the top global business risks identify several that are security-related, including terrorism, cyberthreats, pandemics, national disasters, water security, and government instability or collapse.

But as ominous a backdrop as these risks may provide, they have not changed one of the fundamental realities of business: all functions within a company compete for a finite set of resources, and senior executives will fund those that are most likely to help fuel growth.

Given this reality, the problem for support functions like security is that, certain exceptions aside, they are not seen as revenue generators. As a result, the security department must prove that its efforts are strategically aligned with the objectives of the company, and that they are part of the company’s overall growth effort. This demands strategic leadership from the security manager.

And such strategic leadership goes beyond being the subject matter expert on all things security. It is not simply about possessing the right kind of knowledge. It is, instead, about being someone able to make that knowledge relevant to, and an integral part of, the company’s business goals.
To succeed in this effort, security professionals must fully understand the myriad ways security affects the larger company. With that knowledge in mind, they must focus on creating relationships inside and outside the organization that will enable the security function to produce results valued by the company. Delivering these valued results often requires the need to think and work differently—that is, to think and work strategically. It demands that security professionals become strategic leaders.

This article will focus on the need for strategic leadership by security professionals and what that leadership requires—namely, an alignment between the security function and the company’s business goals that is only achievable through the effective execution of strategies. It does this by first explaining the concept of strategy, and then offering several examples of strategic leadership to demonstrate how it plays out in the real world of security.

VISION AND EXECUTION
The concept of strategy emerged more than 2,500 years ago in ancient Greece with a one-dimensional perspective that focused on how generals waged war. Under this concept, a general is responsible for multiple units, on multiple fronts, in multiple battles, over various spans of time. The general’s challenge is to provide the vision and preparation for orchestrating the subsequent comprehensive actions.

The general’s strategy, then, consists of an integrated set of choices designed to achieve specific goals. But it is important to remember that strategy is not an accurate term for every important choice that the general faces. Sometimes these executives confuse actions or tactics—which are the means by which strategies are executed—with strategies themselves. They are then left to wonder why they failed to achieve their desired goals.
Strategy addresses how the business intends to engage its environment in pursuit of its desired goals. Without strategy, time and resources will be wasted on piecemeal, disparate activities. Sometimes, managers will fill the void with their own (often parochial) interpretation of what the business should be doing. The result is usually unsuccessful initiatives that are incomplete, disjointed, and confusing.

Strategic leadership rises above this confusion. But it does not come easy. Studies show that fewer than one in 10 leaders exhibit strategic leadership, a woefully inadequate number. It would be a mistake to believe that strategic leadership is only needed in times of crisis. During the good times, strategic leadership is just as important as during the bad times, because it ensures valuable resources are focused on the right areas and in the right ways.

At its essence, strategic leadership is the ability to learn, anticipate, challenge, interpret, decide, and align organizational capabilities and competing interests in ways that effectively engage the everyday opportunities and problems presented by the competitive environment. It is the ability to translate vision into reality by seeing the bigger picture and longer time horizons, then creating the strategies necessary to achieve goals that deliver valued results.

Here are five real-world examples to illustrate strategic leadership. The first is relatively simple and straightforward, to ease into the concept. The next four are more involved and complex.

**HONING A PROCESS**
A global security company once had a system for suggestions that required employees to fill out a four-page form each time they had an idea they wished to submit for consideration.

While the form was lengthy, executives believed the information it solicited was valuable and worth requesting. In a period of four years, 2,500 employees submitted 252 ideas for consideration, or about 63 ideas per year.

A lower-level manager in one business unit, who found the process frustratingly inefficient, successfully engaged the organization to change it. This manager realized that the information submitted on the four-page form held value to company leaders. But he also knew that if the submission process were made easier, the organization would ultimately receive more ideas, and it would benefit greatly from their implementation.

The manager’s suggested changes were made. Today, anyone at the company can submit a description of an idea for improvement via email, instead of a four-page form. Moreover, rather than waiting for a time-consuming process to unfold, the submitter is allowed to act upon the idea if there is no response by management within 30 days.

Under the streamlined submission process, employees sent in more than 6,000 ideas for improvement within the first year. When some of these were implemented, organizational performance was enhanced and operating costs reduced.

This is a textbook example of an individual who looks at the bigger picture, and sees an opportunity to change a process that would lead to a positive outcome. This is strategic leadership.

**ADVANCING ON MANY FRONTS**
A security executive sought an opportunity to show that security was aligned with his company’s transformational efforts in ways that would help produce clear and valuable results.

To do that, the security executive engaged in a brainstorming session with his staff, eventually arriving at a consensus decision to improve the company’s access control systems.

The executive knew this was no small undertaking. However, to have the desired outcome he needed buy-in from employees involved in a range of functions that were both inside and outside the business.

He began the process by meeting with people. He met with the finance department to work through the numbers and arrive at a reasonable capital expenditure budget. He met with legal to identify any liability issues that might arise from the new system. He met with human resources, operations, and legal to create a new policy to ensure that there would be progressive discipline for any violations.

He then met with outside suppliers to engage in an open bidding process and ensure the effective delivery of the approved products. He also met with his company’s business development group to ensure that the systems would be installed during site redevelopment to enable the costs to be capitalized, and thereby reduce the overall financial impact on the company. Finally, he met with senior management and presented the strategic plan. It was approved.

What this security executive’s experience shows is that the security function must position the business to succeed in a larger sense, through the involvement of the many, not the few. He realized that the new access control system would result in threat reduction combined with increased security visibility, while controlling costs.

To achieve that positive outcome, the security executive showed an ability to think, act, and influence others in...
strategic ways. Like the military general cited earlier, he designed a plan of integrated actions, working on several fronts—budgetary, legal, employee training, and logistics—and, in so doing, demonstrated strategic leadership.

**IMITATION IS NOT STRATEGIC**

When given the same challenges to improve security, managers may take actions that are not always strategic. For example, in an effort to improve security, a manager undertook a formal benchmarking process. In his benchmarking effort, the manager compared the overall security at his company to that of another well-known company, one with a long-standing, well-respected, and well-funded security department.

Since this second company was a competitor within the same business industry, a benchmarking comparison seemed apt, and so the manager expected the findings to be relevant to improving security. Flush with information and data, the security manager met with senior management and, in a highly professional set of Powerpoint slides, presented the logic for his budgetary request.

Now if we stop there, we might expect that the security manager met with success. After all, it is a common practice in business to identify processes and practices used by other successful firms to understand and recommend competitive positioning. One reason this approach is well regarded in business is that it can be efficient—it can help managers make effective choices by avoiding approaches already judged to be failures by other companies.

But contrary to expectation, the security manager’s proposal was rejected. Although the analysis was logical and the findings sound, the competitor’s values, culture, and operational capabilities were drastically different from the manager’s company. Senior leaders realized that, although something worked at a competing company, it would likely not work in their company, given the operational differences guided by their company’s strategies, core values, and organizational culture. These are important differences because they determine how a company chooses to grow through its current or desired product and geographic markets. Unlike a larger company with greater financial and operational capabilities, a smaller business is often less willing or able to fund new ventures.

So to imitate another company, particularly an industry leader, is to chase a moving target that captures what was effectively yesterday’s success. As mentioned above, identifying practices used by other successful...
firms can be valuable as a means of understanding competitors. But merely copying other firms, even those of industry leaders, is not strategic. Where a benchmarking effort becomes strategic, however, is when it seeks an adapted approach tailored to the individual needs of the organization.

**A PIECE OF THE PUZZLE**

Those in security who come from law enforcement, the military, or government service should recognize that the strategic role they are expected to play will be different from the one they previously fulfilled.

As one security executive once said, things improved when she recognized that success in government life did not necessarily translate into success in a business setting, because business offers fundamentally different challenges.

In her new business setting, this executive’s credibility came by demonstrating an ability to think and act strategically. This occurred early in her transition, when she was asked to help provide input toward improving the background screening process for new hires. This seemingly small-scale involvement actually had the potential for a large-scale impact across the business.

From her experience in government service, she knew the importance of hiring well, and how it provides longer-term employees who, over time, possess greater institutional knowledge. Consequently, rather than merely offering a single bit of input, she asked for and was given a place on the working group that was developing a better background screening process.

In this role, she helped develop a screening process that produced strategic and valued results by minimizing turnover, reducing overall costs, and limiting liability exposure.

With what appeared to be a small involvement in process improvement, this security executive helped deliver a larger benefit to the company. In so doing, she also created relationships that enabled security to meet other challenges that delivered value to the company. Without fanfare and without question, she was a strategic leader.

**ADJUSTING TO REALITIES**

A senior security manager had overseen the growth of his firm’s security function from humble beginnings. Once part of a small cadre of people responsible for investigations at a company aspiring to get bigger, he had seen the company grow through acquisitions into a business powerhouse. His responsibilities as a security manager grew accordingly.

As the company opened more offices and plant locations throughout the country, the manager’s budget and capital expenditures increased dramatically, in keeping with the need to secure the growing number of sites, assets, and employees.

However, a companywide satisfaction survey revealed that employees believed the security department was impersonal, bureaucratic, and unresponsive to employee needs. In turn, employees treated security procedures as mere suggestions.

Based on these findings, the security manager sought to determine the source of the dissatisfaction. He completed a strategic review of the security function, including a small but significant “employee as customer” survey.

What he discovered was surprising: the problem was rooted in the everyday interactions employees had with the security department, specifically the security officers.

This struck at a long-standing concern. Controlling costs was one of the company’s competitive strategies, and so the decision had been made to outsource the security guard function. But the security review discovered significant problems with this approach.

Over time, the number of security services firms providing guard services had grown. The company continually sought the lowest-priced local provider, but managing this operation became more and more problematic.

Hiring and retaining quality officers was particularly difficult; many were poorly paid and inadequately trained, and they felt disenfranchised from the company they served. This all contributed to a costly turnover cycle.

Recognizing an opportunity for positive change, the security manager recommended to his company that they forgo the use of contract services and make the security officers full-time company employees. He presented a
Although there was a strong argument, complete with supporting data, Nonetheless, senior management decided that this proposal was counter to the company’s cost control strategy. The security manager was told to consider another approach to solve the problem.

Rather than being defeated by this setback, the manager sought approval from senior management to increase the security services budget to obtain better quality services and reduce the confusion that stemmed from juggling multiple contracts.

Senior management agreed to a reasonable increase in the security budget, so the security manager began the improvement process by putting the contract out for bid, seeking a single company capable of providing nationwide service in various settings.

Subsequently, a new security company was awarded the nationwide contract to manage guard services based on a range of factors, including adherence to more professional business attire and a commitment to a process designed to develop and retain effective officers. And the selection of the new services company kept the contract within the budgeted increase provided by senior management.

A few months after the new services firm was in place, the security department conducted a new survey. Employees reported feeling that company security seemed more professional, more respectful of their needs, and more helpful. Gone was the adversarial attitude, replaced by a feeling of business partnership. And the company maintained its desired level of security, as evidenced by fewer security violations and fewer security issues.

At its essence, this story illustrates strategic leadership in action. Despite setbacks, the security manager adapted to the situation and aligned security efforts so that they were consistent with his company’s cost containment strategy and business needs, and fulfilled the firm’s protection and customer service requirements.

THE FUTURE

The only certainty about the future is that it is uncertain, and past success does not guarantee future success. These two maxims, sometimes applied to business in general, certainly apply to the security field.

Some of the factors driving this uncertainty include advances in technology and the quantity of information being produced; shifting customer needs; internal competition within companies for resources; struggles to maintain profitability as the economy changes and evolves; and the new normal of doing more with less for countless business operations, including security.

But we also see markets offering greater opportunities to those able to adapt. The ability to influence others to engage in efforts that enable organizational success, while acknowledging the constraints of time and resources, is at the heart of being strategic. It is why security leaders must prove they are capable strategic leaders.

These leaders recognize situational constraints and adapt to their environment. By necessity and design, they are flexible, and able to adjust their strategies to achieve the stated goals. What they do is measurably tied to goals.

Their attributes go beyond charisma, experience, and expertise. Aspirations are not enough; businesses want to see results. And results, more often than not, take strategic leadership.

CHRIS WALKER, D.B.A. (DOCTOR OF BUSINESS ADMINISTRATION), IS A MANAGEMENT DEVELOPMENT CONSULTANT AND A LONGTIME MEMBER OF ASIS INTERNATIONAL. A FORMER LAW ENFORCEMENT OFFICER RESPONSIBLE FOR HIGH-LEVEL FINANCIAL INVESTIGATIONS, WALKER SERVED AS THE HEAD OF GLOBAL SECURITY FOR A MULTIBILLION DOLLAR DIVISION OF A FORTUNE 50 COMPANY. HE IS FORMER EXECUTIVE PROFESSOR OF STRATEGY FOR NORTHEASTERN UNIVERSITY.

Studies show that fewer than one in 10 leaders exhibit strategic skills, a woefully inadequate number.
With unrealistic goals and high pressure, incentives to perform can become incentives to cheat. Mindful managers can reduce the likelihood of unintended consequences.

Paved With Good Intentions

The incentive may have seemed ordinary when Wells Fargo management first issued it. But it led to some extraordinarily negative consequences. Wells managers imposed what was sometimes called an “Eight is Great” target for their employees: sell eight accounts per customer. This type of cross-selling, in which bank employees encourage account holders to open another account, take out a credit card, or buy other services, is a common method for companies in the banking industry to increase their revenue.

But in late 2016, according to news reports and testimony before the U.S. Congress, company representatives publicly conceded that the incentive resulted in disaster. Over a period of at least five years, Wells Fargo employees created more than 1.5 million unauthorized deposit accounts, and at least 500,000 unauthorized credit card applications.
Polluted Ecosystem
The Wells Fargo case was a clear example of a perverse incentive—an incentive that results in unintended and undesirable consequences contrary to the interests of the incentive designers.

For managers, it’s important to recognize that all incentives have the potential to turn perverse, says managerial incentive expert Marc Hodak of Farient Advisors.

“Every incentive to perform is an incentive to cheat. You can’t have one without the other,” he says.

In practice, the majority of incentives or performance targets in the business world do not turn perverse, despite the potential to do so. Why so with Wells Fargo?

Hodak says that a few factors came together in the Wells case, and collectively they sustained a “perverse incentive ecosystem.”

“Any one of the factors individually wouldn’t have resulted in the debacle [that happened],” Hodak explains.

One crucial factor, Hodak says, was an unrealistic goal. While cross selling is common in the industry, eight accounts per customer, even as an aspirational goal, does not seem realistically achievable on a widespread scale.

Other factors compounded this problematic goal, Hodak explains. High-level managers were offered lucrative financial rewards if their staff hit the targets, and managers’ bonuses were dependent on the degree to which sales goals were achieved. By some accounts, certain Wells managers began checking their progress toward the sales goals twice a day, thus helping to create an office environment that felt like a pressure cooker.

In addition to rewards for upper management, incentives were also offered at lower levels of the organization, such as promotions and job security for sales staff who fulfilled the performance goals.

Still, in most other companies, these factors do not blow up into a catastrophic situation, because there is usually some sort of safety valve. For example, some companies have an internal system of controls that flags suspicious activity, such as an unusual surge in new account creation.

But at Wells Fargo, the situation was not checked internally and it spiraled out of control. Managers communicated to employees that there would be penalties for not reaching the goals, thereby increasing the possibility of risky behavior. And management punished some who complained.

“The safety valve got short circuited somehow,” Hodak says. “The cheats were getting ahead, and the honest were afraid of getting fired.”
A Variety of Perversities

Of course, the Wells Fargo sales goals are not the only type of perverse incentive. While they can take different forms, management experts say that there are a few specific types of incentive that can run into problems.

One is an undermining metric. This type of metric may fulfill a short-term goal, but it is ultimately not in the organization’s long-term interest.

For example, a company that wants to become more prepared for an active shooter incident may decide to require an annual active shooter training session. Once the session is complete, company leaders then say they have fulfilled their goal.

But it is possible that the training was ineffective, so the metric has the unintended or perverse effect of convincing managers that the company is prepared, even though it is not. Instead of this metric, the company should focus on performance improvement metrics that can measure the effectiveness of the training.

Another type of perverse incentive, experts say, can come in the form of budget pressure. Company leaders may indicate to the security manager that proposed budget reductions will be looked favorably upon, because they will save the company money. The security manager may then make personnel cuts that can be covered for in the short term, which are approved by the CEO. But in the long term, they may have the unintended effect of compromising the company’s security.

Some financial rewards can also become perverse incentives if they alter an employee’s motivation. When performance is rewarded with financial compensation, an employee’s motivation can change, so that the driving force of his or her behavior becomes the extrinsic motivator of financial reward, not an intrinsic motivation to do good work.

This can have the unintended effect of decreasing an employee’s overall intrinsic motivation, which can hurt performance in other areas. And studies show that reliance on extrinsic motivators can diminish creativity, which is an important component of learning and performance.

In addition, Hodak says that a performance target is more likely to have perverse effects if it contains an all-or-nothing threshold—that is, employees get a significant reward if they hit a goal of eight accounts per customer, but get nothing if they come close, like selling seven accounts.

Avoidance Strategies

In as much as no one can predict the future, no manager can guarantee that his or her company’s incentives will never turn perverse. However, there are strategies for minimizing their likelihood, and in a recent interview with Security Management, veteran security manager Bill Wipprecht offered some best practice guidance.

Wipprecht was CSO for Wells Fargo for 23 years, until 2010. He was not involved in the incentive situation and was long gone when it came to light; he says he remembers Wells Fargo as a great company and great place to work, albeit with the business ups-and-downs that every firm experiences for creating incentives.
“I never saw the Wells Fargo incentive as being illegal. It was unethical,” he says.

Wipprecht agrees with the argument that setting an unrealistic goal was one of the key reasons why the Wells incentive turned perverse. And that can sometimes be difficult to avoid, he adds, because most managers have done this at least occasionally in their career.

He gave the common example of a manager who sits with an underachieving employee in a review and sets an even higher performance goal, even though it seems unrealistic given past performance.

“Almost every manager has set unrealistic goals and objectives, and asked that the employee meet them,” he says. However, the pressure cooker atmosphere that can drive an incentive toward perversity can be avoided if managers self-regulate their own behavior, Wipprecht says. To illustrate, he gave the example of how a security manager deals with vendors.

“I’ve had managers call a vendor and beat them to a pulp for minor performance issues,” he says. “It’s almost abusive, and then what are you going to expect in return?”

What they might get, he adds, is a vendor who will say anything to avoid that type of abuse in the future, including unrealistic claims about the products or services being used that could lead to unintended negative consequences down the line.

Attitude checks by security managers are also useful in dealing with employees, he adds. Wipprecht remembers how, as CSO, his temperament set the tone of the department. When he was happy and smiling, his employees were too; on days when he came into the office in a bad mood, the department darkened.

“That was the mood for the entire office for the whole day,” he says.

When the manager’s darker moods strike, employees are more likely to present issues in a positive light. For example, they may pretend that their performance is higher than it really is, or they may avoid the manager altogether—even though a pressing security issue needs to be discussed.

Finally, friendly competition among employees may work to increase productivity, but managers need to realize that it’s unwise “to set up an overly competitive situation in an organization, rather than a teamwork environment, which is what you want to instill,” Wipprecht cautions.

Along the same lines, perceived favoritism can lead to unintended consequences, because employees may get the sense that the game is rigged, and they need to do something drastic to compete. “If you’ve got a favorite in the office, it sets a negative tone for the rest of employees,” he says.

In the end, experts say that incentives can still be used in a positive fashion, but managers need to be continually mindful of where they could go wrong.

“Whenever you put incentives in play, you are playing with fire,” Hodak says. “Fire is terribly useful, but it can also be dangerous.”

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

Protection of Assets

Protection of Assets (POA) is considered the premier reference for the security industry. Written, edited, and peer-reviewed by security subject matter experts, this comprehensive source covers all aspects of security.

POA is available in print (set or individual books), on Kindle, and as an online subscription. Titles are also available in Spanish.

For more information and to order, visit www.protectionofassets.com/sm
Retail Risk Management and Asset Protection

When using big data and analytics for security purposes, it is important for loss prevention practitioners to understand foundational issues. Following are some common analytical methods and data handling procedures often used to tackle problems.

**Measure Impact**
A large part of executing new ideas in retail and loss prevention involves trial and error. Someone in the organization has a good loss prevention idea, but is not sure if it will work. If the idea is good enough, an executive will sponsor an in-store pilot test of the idea to determine its viability. Then the test is completed, and results are measured. If the results show that the test was successful, the program can move ahead.

Analytics and statistics are used in selecting pilot stores, structuring the test period, and conducting the analysis. The best general strategy for selecting stores is to use a complete randomization. This can be as easy as putting the store list into Excel, assigning a random number to each store, and then picking the top stores for the study. Following traditional statistical approaches for designed experiments and A/B testing will go a long way in setting up the experiments so that the results are defensible.

**Use Available Data**
Some retailers have used data to find relationships between those data points and shrink using multiple regression models. These variables may include, for example, store sales, employee tenure, crime in the surrounding area, the number of public cameras, the presence of a security guard, the number of apprehensions, manager tenure, training programs, store survey results, and metrics based on point of sale data to determine whether any are related to shrink.

Once the data is collected, statistical analysts will apply typical model-building procedures, which include cleaning the data, transforming predictor variables for optimal response, and fitting the algorithms using statistical software.

**Exception Reporting**
Most exception reporting systems combine data from the point of sale, employee records, item files, and store files into a single system that a loss prevention professional uses to find cases. These systems generally follow a query-based set of rules, which are historically known to identify a reasonable concentration of fraudulent and abusive individuals. Using these types of systems allows investigators to identify many actionable cases in a short amount of time.

**Predictive Modeling and Scoring**
Everything we do generates data and, thanks to the advent of big data, hundreds of predictions from models (often called scores) are calculated for every individual based on his or her past behavior in a wide array of industries. These scores, in turn, provide a likelihood of some future behavior, which can be used to drive anything from marketing decisions to banking decisions to crime prevention decisions. According to Intel, the highest value of big data is achieved through predictive modeling, which is applied using advanced techniques to predict future events and drive decisions in real time.

From a loss prevention viewpoint, predictive modeling involves performing statistical analyses that may uncover trends in the underlying risks that may indicate the likelihood of future loss. It also anticipates future behavior and improves strategic planning. For example, it can identify how an institution can effectively and deliberately target certain suspect employees, high-risk locations, and high-risk products—leading to a more efficient loss prevention process.

**Video Analytics**
The standard barriers to video analytics—excessive bandwidth needs, immature analytics software, high cost, and privacy concerns—are being whittled away over time and are likely to dissolve at some point. Big data tools are nearing a cost-effective state, bandwidths are continually increasing, and computing platforms can handle the massive amounts of computations. In less than a decade, centralized video storage and analytics are likely to be the norm for loss prevention.

**Social Media Data**
With the proliferation of social media through such services as Twitter, Facebook, and LinkedIn, there has been an explosion of data available to solve a variety of problems. It is often surprising how much individuals reveal, in a very public way, about their activities. These data sources have been incorporated in investigations to support retailers’ efforts to catch and prosecute serial offenders.

While there has been some use of this data, it is not being mined to its full potential. For example, if retailers could use social media postings in a proactive way to thwart, mitigate, and respond to crime earlier, this could result in tremendous savings.

The use of analytics and predictive modeling is a critical component in the future of loss prevention. The ability to assess patterns in data, measure loss prevention programs, and make decisions in real time will become fundamental in solving complex issues related to customers, sales, and loss. As criminals become more sophisticated, they will always target areas of weakness.

Loss prevention leaders should begin discussions, internally and with external partners, to create an infrastructure that can bring significant value to the organization through the use of data and analytical methods.

This article was excerpted from Essentials of Modeling and Analytics: Retail Risk Management and Asset Protection, Copyright 2018, by David B. Speights, Daniel M. Downs, and Adi Raz. Reproduced by permission of Taylor and Francis Group, LLC, a division of Informa plc.
NOTHING ESCAPES our customer service technicians. Not unique security problems. Not tricky installations. Certainly not inventory out your back door. Whether you need guidance with a challenging installation, are inquiring about training or want help making a hardware decision, you can access a team with nearly five decades of combined experience. A sharp mind will promptly help you secure a smart solution. Just call 800-729-3839.

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

DETEX.COM/MAx8

For product info #24 securitymgmt.hotims.com
We invite you to visit the site today and explore the host of opportunities to get involved in your global security community. Update your profile at the top-right of the homepage. Indicate areas of interest, add a profile photo, and revisit your communications preferences. January’s website upgrade is just the start of a multiphase web update plan. To help inform what the project will look like in the coming months, share your feedback to asifuture@asisonline.org.

WHAT’S AHEAD FOR S&G
The ASIS Commission on Standards and Guidelines expanded its membership from 12 members to 28 in 2018, on the heels of its first open application process. “Over the last decade, the global security standards landscape has changed dramatically,” says Sue Carioti, ASIS vice president of Certification, Standards, and Guidelines. “The ASIS Standards and Guidelines Commission understands and recognizes that change is necessary on multiple levels. To that end, the commission took purposeful steps to broaden its membership composition as well as to institute a new and formal membership application process.”

The 2018 Commission on Standards and Guidelines consists of:
- Chair Bernard Greenawalt, CPP, Securitas Security Services USA
- Vice Chair Eugene Ferraro, CPP, PCI, ForensicPathways, Inc.
- Charles Baley, Farmers Group, Inc.
- Bruce Braes, CPP, Jacobs
- Darryl Branham, CPP, Avnet
- Herbert Calderon, CPP, PCI, PSP, CCM2L
- Robert Carotenuto, CPP, PCI, PSP, New York Botanical Garden
- Werner Cooreman, CPP, PSP, Solvay
- Michael Crane, CPP, Securisks
- Michael Cummings, CPP, Cummings Security Consulting, LLC
- William Daly, Control Risks

OUT WITH THE OLD, IN WITH THE NEW
HAVE YOU CHECKED OUT the new ASIS website, www.asisonline.org?
Launched late last month, the revitalized site is built with your needs in mind, delivering what you want, when you want it. Gone are the text-heavy web pages, unfriendly navigation, and cumbersome shopping experience. From the top down, all functionality is designed with mobile in mind.

These strategic design choices along with our new taxonomy and tagging structure will enable quick access to our robust search feature and easy-to-browse navigation. Tap into the expertise of your 35,000+ ASIS peer group in ASIS Connects, our new member-only private community.

We invite you to visit the site today and explore the host of opportunities to get involved in your global security community. Update your profile at the top-right of the homepage. Indicate areas of interest, add a profile photo, and revisit your communications preferences. January’s website upgrade is just the start of a multiphase web update plan. To help inform what the project will look like in the coming months, share your feedback to asifuture@asisonline.org.
The new commission holds a diverse range of security expertise. Its 28 members represent eleven countries. Twenty members are new to the commission in 2018, although 21 have served on past technical committees. Furthermore, 24 are ASIS board certified, and 11 are involved with ASIS councils.

In 2018, the commission will consider the restructure of Standards and Guidelines programs; form static technical committees to address core security risk management discipline areas; review existing standards and guidelines with an emphasis on relevancy and gap analysis; chart a path forward to begin development of tools, guides, and handbooks; and increase integration in knowledge and learning.

Three technical committees remain busy in 2018, continuing their work developing standards in the areas of security awareness, private security officer selection and training, and workplace violence prevention and intervention.

**LIFETIME MEMBERS**

John Sullivant, CPP; Larry K. Stanley, CPP; and Michael J. Fagel have been granted lifetime membership to ASIS.

Sullivant has been a dedicated member for 31 years and has served as chapter chair, vice chair, and membership chair for the Granite State Chapter. He also authored two published articles in *Security Management*: “Is America Prepared for Today’s Threat?” and “Successful Project Planning.”

Stanley has been a regional vice president, an assistant regional vice president, and a member for 25 years. He also served as chair of the Central West Virginia Chapter.

Fagel has served on the ASIS School Safety and Security Council, the Fire and

**S&G COMMISSION STATS**

- 28 MEMBERS
- 24 ARE ASIS BOARD-CERTIFIED WITH A TOTAL OF 36 CERTIFICATIONS
- 20 ARE NEW TO THE COMMISSION
- 21 HAVE SERVED ON TECHNICAL COMMITTEES
- 11 SERVE ON ASIS COUNCILS
- 11 COUNTRIES ARE REPRESENTED
Life Safety Council, and the Food Defense and Agriculture Security Council. He was presented with the inaugural ASIS Security Book of the Year Award at the 60th Annual Seminar and Exhibits. Fagel has been an ASIS member since 1982.

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

- Andre P. Firlotte, CPP
- Rickey Gene Nelson, CPP
- Joseph F. Frawley, Jr., CPP
- Norman B. Taylor, CPP
- Bruce R. Sullivan, CPP
- Robert Chicarello, CPP
- Mary M. Vavra, CPP
- William R. Bogett, CPP
- Kirk A. McGee, CPP
- Mary M. Vavra, PSP
- Huan Chiang Lee, PSP

MEMBER BOOK REVIEW

In many smaller organizations—and those focused on cost-cutting—the facility leader may be tasked with overseeing the company’s security function. Professionals in this field often come from engineering or mechanical backgrounds, and they may possess limited knowledge and skills relating to the protection of an organization’s physical assets. Author John Henderson, CPP, wrote The Facility Manager’s Guide to Safety and Security to address that knowledge gap.

The author drills into fundamental security concepts, explaining not just what to do, but describing the goal of the task—for example, deterrence, incident response, guard force management, and even crime prevention through environmental design (CPTED). Overall, the book serves as a practical handbook for securing any building, with starting points and programs to steer the manager along the way.

The text guides the reader through the process of conducting a security assessment, determining a facility’s needs, and applying practical solutions. Specific areas of security addressed are lighting, access control, fencing, and fire/life safety. Although targeted towards those who manage buildings for their organizations, the text can serve as a practical guide and overview of physical security for anyone in the industry.

One excellent section in the book is titled “Not Much Happens Around Here.” It addresses the complicated issue of convincing executives to spend dollars on costly security initiatives when the consensus is that there are no real concerns. It is always difficult to measure security’s effectiveness when statistics don’t indicate true security needs. The author points out that conversations with employees can often provide a clearer picture of concerns and needs.

The Facility Manager’s Guide will serve as a valuable tool for leaders new to the responsibility of providing an overall safe and secure environment. REVIEWER: Michael D’Angelo, CPP, is the principal and lead consultant for Secure Direction Consulting, LLC, a Florida-based independent security consulting firm. He served on the South Miami, Florida, Police Department for more than 20 years, retiring as a major. He currently serves on both the ASIS Healthcare Security Council and the ASIS Transitions Ad Hoc Council.
CHAPTER ANNIVERSARIES
Congratulations to chapters celebrating milestone anniversaries in the last quarter of 2017.

40th Anniversary
• Texas Gulf Coast
• Greater Lexington

15th Anniversary:
• Southwestern Ontario

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

Pamela Cichon, CPP, began working as a letter carrier for the U.S. Postal Service (USPS) in 1987. Her career was postmarked for success. In the 30 years since, she has worked her way up to become a program manager in physical security within the Security Group at the U.S. Postal Inspection Service’s national headquarters. 

As her career evolved from letter carrier to supervisor in delivery to operations to federal law enforcement, Cichon saw the benefits of pursuing a role in security. “As an inspector, much of your attention is focused on the result of a crime...after the fact. In security, you have the chance to thwart security breaches, keep customers and employees safe, and protect U.S. postal assets.”

There is no such thing as a typical day for Cichon. In her current role, she provides guidance and assists with physical security policy interpretations for the USPS. She oversees programs that are responsible for assessing the physical security of more than 31,000 USPS facilities.

Sometimes, this means investigating mail fraud. In October, it meant dealing with the aftermath of a 300-pound bear’s intrusion into a mail facility in Alaska. The wide variety of situations that Cichon must adapt to is part of what makes each day interesting and unique.

In 2006, she was one of 36 postal inspectors selected to pursue the Certified Protection Professional® (CPP) certification. Memberships, study materials, and certification exam fees were covered through a national headquarters sponsored program.

Cichon was excited to be selected because “board certification offers tremendous credibility and accountability,” she says. “It shows your commitment to understanding key security concepts and applying them.”

Cichon, who now serves on the ASIS Physical Security Council, leverages her CPP certification and ASIS membership to work her way through tough situations. “My membership has opened up a whole world of networking contacts,” she says. “When I find a challenge at work, my ASIS contacts offer a wealth of knowledge and are a valuable resource.”

Looking to double up on ASIS certification, Cichon will sit for her Physical Security Professional® (PSP) exam in spring 2018. When prompted for advice she’d offer someone considering whether to pursue a certification, she recommends making a plan and committing to it.

“When I find a challenge at work, my ASIS contacts offer a wealth of knowledge and are a valuable resource.”

“Evaluate what is involved and be prepared to dedicate time each week to study the materials,” she suggests. “Select an exam date early, so you have a goal in mind, and work backwards from that date. Find out if your local chapter is conducting a certification review course. ASIS sponsors prep classes that offer a one-and-a-half-day intensive review, and there is an online review that may hold the key for someone who needs that kind of versatility.”

Cichon notes that in an age where security is touching every aspect of our lives, there is tremendous credibility in the fact that you have knowledge, and understand how to apply it, in the field of security. ASIS board certification, combined with its accompanying continuing education requirement, is a great way to demonstrate security expertise.

“I find it gives me street cred,” she concludes.

PROFILE BY STEVEN BARNETT, ASIS COMMUNICATIONS COORDINATOR

CERTIFICATION PROFILE
PAMELA CICHON, CPP
EXCESSIVE FORCE. A jury must decide whether a police officer used excessive force when he tased a man for nearly two minutes, a U.S. court of appeals said in a ruling that revived the plaintiff’s suit.

In 2010, Las Vegas Metropolitan Police Department Officer Mark Hatten pulled Anthony Jones over for a routine traffic stop. Hatten told Jones to get out of the car, so he could pat Jones down for weapons.

Jones initially obeyed the command, but then started to turn towards Hatten. Hatten, who said in court documents he was afraid of Jones, drew his firearm, pointed it at Jones, and ordered him to turn back around. Jones then ran away.

Hatten called for backup and chased Jones, who was not armed. He then used his Taser to subdue Jones, firing it twice and causing Jones’s body to “lock up” and fall to the ground. Hatten then knelt on Jones’s back in an attempt to handcuff him while he pressed his Taser to Jones’s thigh and continued to pull the trigger.

Hatten kept tasing Jones, even after four other officers arrived. Jones was taken to a hospital, where he was diagnosed as suffering from post-traumatic stress disorder. Jones filed a lawsuit against Hatten, alleging that he had used excessive force.

The ruling by the U.S. Court of Appeals for the Ninth Circuit, in Jones v. Hatten, No. 15-56809, held that a jury must decide whether Hatten used excessive force when he fired his Taser on Jones. The court said that the “use of force even if excessive, in response to a suspect’s nonviolent actions” is not per se excessive under the force protection methodology.

The court reversed the district court’s decision to dismiss the case and remanded it for further proceedings.

**DISABILITY**

American Airlines Inc. and Envoy Air Inc. will pay $9.8 million to settle charges that they denied accommodations to disabled workers. In a suit brought by the U.S. Equal Employment Opportunity Commission (EEOC), American and Envoy were charged with barring disabled employees from returning to work or transferring to other positions after being restricted on the type of work they could perform. The consent decree also prohibits the airlines from engaging in discriminatory employment practices, denying reasonable accommodation requests, or retaliating against employees who report discrimination. (EEOC v. American Airlines Inc., U.S. District Court for the District of Arizona, No. 2:17-CV-04059, 2017)

**CORRUPTION**

Two former executives at Dutch oil and gas services company SBM Offshore NV pleaded guilty to conspiracy to violate the U.S. Foreign Corrupt Practices Act (FCPA). Anthony “Tony” Mace and Robert Zubiate pleaded guilty for their roles in a $16 million scheme to bribe foreign government officials in Brazil, Angola, and Equatorial Guinea to assist the company and its U.S. subsidiary with winning bids, according to the U.S. Department of Justice.

Zubiate’s sentencing was scheduled for January 31, and Mace’s is scheduled for February 2. (U.S. v. Zubiate, U.S. v. Mace, U.S. District Court for the Southern District of Texas Houston Division, Nos. 17-cr-591, 17-cr-618, 2017)

**CYBERCRIME**

Former U.S. Secret Service agent Shaun W. Bridges, 35, was sentenced to 24 months in prison for money laundering. Bridges was on the team that investigated the Silk Road Dark Web market and admitted to transferring bitcoin out of a U.S. government digital wallet into other digital wallets only he had access to.

Bridges pleaded guilty to one count of money laundering, and in addition to prison time he will forfeit 1,500 bitcoin and other currency valued at approximately $10.4 million. (U.S. v. Bridges, U.S. District Court for the District of Maryland, No. 15-mj-02125-BFG, 2017)

**LEGAL HIGHLIGHTS**

- **ISSUE:** Drones  
  **BILL:** P.L. 115-91  
  **VENUE:** U.S. Executive Branch  
  **STATUS:** Enacted  
  **SIGNIFICANCE:** Re-enacts a requirement that owners of small unmanned aircraft—drones—register their crafts with the U.S. government.

- **ISSUE:** Cybersecurity  
  **BILL:** P.L. 115-91  
  **VENUE:** U.S. Executive Branch  
  **STATUS:** Enacted  
  **SIGNIFICANCE:** Creates an IT modernization fund to enhance digital defenses, a ban on Kaspersky Lab products, and withholds funding for the White House Communications Agency until cybersecurity requirements are met.
threatened Hatten, committed a serious to subdue Jones because he had not concluding that he should use his taser "began appropriately" with Hatten court said that the officers’ use of force on grounds of qualified immunity. The case could not have been dismissed Jones’s parents to correct the mistake, law. The district court did not allow estate,” which is required under Nevada sert their Fourth Amendment claims because it said Jones’s parents had incorrectly listed his estate—not the administration of the estate—as a plaintiff. Because of this, the district court said Jones’s parents had failed to “as- sert their Fourth Amendment claims as executor or administrator of Jones’s estate,” which is required under Nevada law. The district court did not allow Jones’s parents to correct the mistake, but also dismissed the case on grounds of qualified immunity. Jones’s parents appealed the ruling, which reached the U.S. Ninth Circuit Court of Appeals. The appellate court also found that the district court ruled in part and remanded the case for a trial • The indictment alleges that Conto- guris, working with employees of an interna- tional engineering consulting firm (Technical Advisor), including Kohler, devised a scheme with Rolls-Royce executives and employees, including Zuurhout, Barnett, and Finley, whereby Rolls-Royce would pay kickbacks to the Technical Advisor employees and bribes to at least one foreign official, and disguise these payments as commissions to Contoguris’s company, Gravitas, in exchange for helping Rolls-Royce win contracts with Asia Gas Pipeline LLP,” the DOJ said in a press release. After AGP won contracts with Rolls-Royce, worth approximately $145 million,
Rolls-Royce allegedly made commission payments to Gravitas, which Contoguris then passed on to Technical Advisor employees with the knowledge that it would be shared with a foreign official.

Rolls-Royce later entered a deferred prosecution agreement with the DOJ, incurring an $800 million penalty global resolution with the DOJ, the United Kingdom, and Brazilian authorities.

Contoguris had not entered a plea as of press time, and was believed to be outside of the United States. (U.S. v. Contoguris, U.S. District Court for the Southern District of Ohio Eastern Division, No. 2:17-cr-00233, 2017)

**DATA PROTECTION.** The U.S. House of Representatives passed a bill that would require 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 require the U.S. Securities and Exchange Commission (SEC), 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.

“The Equifax breach and the recent cyberattack at the SEC only exacerbate the need to ensure top cybersecurity controls are in place at our securities regulator, which is why I look forward to this bill swiftly making its way to President Trump’s desk and being signed into law,” said bill sponsor U.S. Representative John Ratcliffe (R-TX), who introduced the legislation, in a statement.

**LEGISLATION**

**United States**

**CYBERCRIME.** U.S. President Donald Trump signed legislation into law that creates an institute to train local law enforcement and other partners to investigate and prevent cybercrime.

The law (P.L. 115-76) authorizes 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.

Additionally, the institute will train law enforcement officers, prosecutors, and judges about the 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 Forces by adding officers who have completed training through the institute.

“At the end of the day, getting the upper hand against cyber criminals will make our nation safer, and I’m glad that this critical piece of legislation has been signed into law to do just that,” said U.S. Representative John Ratcliffe (R-TX), who introduced the legislation, in a statement.

**TRAINING.** U.S. House Speaker of the House Paul Ryan (R-MN) announced that all U.S. House of Representatives members—and their staffs—will undergo mandatory antiharassment and antidiscrimination training.

“Going forward, the House will adopt a policy of mandatory antiharassment and antidiscrimination training for all members and staff,” Ryan said in a press conference. “Our goal is not only to raise awareness, but also make abundantly clear that harassment in any form has no place in this institution.”

The training will be required when the Me Too Congress Act is passed (H.R. 4396, and S. 2159). The move to require the training was initiated following a hearing where two female lawmakers spoke about incidents of sexual misconduct involving sitting members of Congress.

U.S. Representative Barbara Comstock (R-VA) described an interaction where a staffer went to a lawmaker’s home to drop work materials off, and was greeted by the lawmaker in a towel. He then invited her inside where he exposed himself to her. The staffer quit her job soon afterwards.

Both bills have been introduced and are undergoing committee reviews. The House bill has 101 bipartisan cosponsors, and the Senate bill has nine Democratic cosponsors.

**LEGAL CASES**

**ISSUE:** Corruption

**CASE:** U.S. v. Steven

**VENUE:** U.S. District Court for the Southern District of New York

**STATUS:** Guilty plea

**SIGNIFICANCE:** Former executive at a Brazilian aircraft maker pleaded guilty to charges that he arranged a bribe to Saudi Aramco to secure a sale.

**ISSUE:** Discrimination

**CASE:** EEOC v. Trinity Health

**VENUE:** U.S. District Court for the District of North Dakota

**STATUS:** Settled

**SIGNIFICANCE:** Trinity Health will pay $95,000 to settle charges that it refused to provide light-duty work to a pregnant nurse with a lifting restriction.
Mark Your Calendars

The ASIS 28th NYC Security Conference & Expo returns May 16-17, with more education, more technologies, and more opportunities to connect with the best and the brightest in the profession.

Make plans now to join more than 2,500 security and law enforcement professionals from the public and private sectors as we examine the critical security issues facing organizations and communities.

JOIN US

in honoring the ASIS NYC Chapter’s “Person of the Year,”

Cardinal Timothy Dolan
Archbishop of New York

Learn more and register at asisonline.org/SMnyc
PARTNERSHIPS AND DEALS

**Acuant** partnered with **Nexistant** to streamline visitor management using automated information capture. The CLIQ locking system from **ASSA ABLOY** is protecting **REWE**’s new logistics center in Germany.

**ControlScan** and **Food Giant Supermarkets, Inc.**, are teaming up to protect the 110-store chain and its customers from data theft. **CyberTech Systems and Software** and **Esri** entered into an OEM agreement to fully embed ArcGIS Server into GeoShield, CyberTech’s advanced intelligence-led policing platform.

**DTT** loss prevention technology was recently used to stop employee time theft at a **Papa Murphy**’s location in Washington State. DTT also became the exclusive video surveillance provider for **Cellairis**.

**Exabeam** announced a partnership with **WireX Systems** to provide improved cybersecurity and incident response. **EyeLock LLC** and **ViaTouch Media** announced the integration of EyeLock embedded iris recognition technology into ViaTouch’s retail solution.

**Fidelix** is using **TOSIBOX** products to create remote access and monitoring of building automation systems. **FST Biometrics** successfully integrated its In Motion Identification solution with **Automatic Systems** SmartLane turnstiles at **CN**’s Montreal headquarters.

**Hikvision** surveillance system installed by **A-1 Security** is securing a marijuana growing facility in Colorado.

The new **Huawei** Mate 10 smartphone features an integrated fingerprint sensor from **Goodix**.

**IBM Security, Packet Clearing House**, and the **Global Cyber Alliance** launched a free service designed to give consumers and businesses added privacy and protection as they access the Internet. **iDenta Corp.** signed a contract with

**CUSTOMER TARGETING**

**LAMAR ADVERTISING** used digital billboards and video analytics to pinpoint drivers who might be interested in the latest installment of the blockbuster movie franchise **Transformers 5: The Last Knight**. Lamar knew that certain cars were important in the movie, so it employed video analytics to recognize makes and models of cars traveling on the road. When a likely vehicle was spotted, a digital billboard displayed a targeted message—such as “ATTENTION: Your Car is an Autobot!”

**Milestone Systems** software and **Canon** IP video cameras enabled the video analytics to identify the vehicles. Many factors had to be taken into account for the digital billboard integration, such as vehicle speed, lighting, and camera angles. Because each location is different, multiple images of targeted vehicles were used to create a database to identify cars as they passed by.

Working like a facial recognition system, the solution immediately recognized a target vehicle and delivered the custom billboard advertisements accordingly, incorporating the car make and model within the message.
Pro-gard, which will serve as a distributor for the U.S. law enforcement market.

Johnson Controls announced that its exacqVision video management system now integrates with Databuoy Corp.’s ShotPoint acoustic gunshot detection and localization system.

The Taktis Technology Platform from Kentec protects apartments and recreational facilities at Durham University.

MRM Solutions selected the system.

Kwikset is teaming with Amazon to offer homeowners two smart lock solutions to choose from when purchasing an Amazon Key In-Home Kit.

LockPath and RiskRecon are partnering to increase visibility into third-party risk management.

Carpenter & Company, developer of One Dalton Street in Boston, enlisted the help of Global Security & Innovative Strategies, Evol Technology, and Milestone Systems to create a security plan for the residential high-rise.

NC4 is partnering with CyberTech to deliver information-sharing solutions to law enforcement.

Near Field Magnetics, Inc., is integrating its sensors with turnstiles from Orion Entrance Control, Inc.

The AEOS system will be integrated into Kone elevators for Three Snowhill, an office building in Birmingham, United Kingdom.

GBE Fire & Security chose AEOS from Nedap Security Management for access control, lift destination control, and vehicle identification.

Netsurion announced a strategic partnership with Lucas Systems to bring network security and PCI compliance services to merchant businesses.

On the Move Systems announced that its subsidiary Robotic Assistance Devices deployed an unmanned security guard robot at the headquarters of Romeo Power Technology in California.

Open Options and OnSSI expanded their existing technology partnership to provide a two-way integration between the Ocularis and DNA Fusion applications.

Park Assist is implementing its smart sensor system at Capital One in McLean, Virginia.

Pelco by Schneider Electric joined forces with AMAG Technology for integrated, scalable access control and surveillance system management.

Razberi integrated its CameraDefense cybersecurity software with Milestone XProtect Corporate, enabling joint customers to manage video surveillance systems from a single user interface.

RTI announced a two-way driver for the complete line of DoorBird IP Video Door Stations.

Banco Bancrea, S.A., in Mexico is using Scati video management systems.

SecurityMatters will work with NIST’s National Cybersecurity Center of Excellence to study countering cyberattacks against industrial control devices.

Sofradir formed a distribution partnership with ATD Electronique to extend its European customer base.

Systech International will deliver a next-generation Digital Certificate of Authenticity for sports memorabilia at the Philadelphia Sports Hall of Fame.

TÜV Rheinland entered into a three-year collaboration with Gooee to examine its products and services against data protection and security requirements.

ELVEES has licensed UltraSoC embedded analytics technology for use in its next-generation video processing offerings.

Utility, Inc., is collaborating with Sony to develop an automatic license plate recognition application for existing Rocket IoT Vehicle video systems.

Visual Management Systems Ltd., developer of the TITAN VISION PSIM, joined the Acreont Technology Partner Program.

VoiceTrust and inBay Technologies announced a strategic collaboration.

GOVERNMENT CONTRACTS

Amika Mobile and Mobility Insight announced a collaborative project focused on intelligent border security and connected vehicle systems for the...
government of Canada.

Manchester-Boston Regional Airport installed more than 150 Arecont Vision cameras for video surveillance.

Axon Public Safety Canada Inc., announced that a number of Canadian agencies, including Abbotsford Police Department in British Columbia, are conducting trials of Axon Citizen.

The U.S. Integrated Public Alert and Warning System is being migrated to a disaster-resistant Amazon Web Services cloud platform, with support from eGlobalTech, IBM, and the Federal Emergency Management Agency.

iDenta Corp. drug identification kits are being used by European Union forces in Africa.

Iron Mountain Incorporated was awarded a contract from the U.S. Patent and Trademark Office to manage and relocate some 4.6 million patent files from their current storage location to Iron Mountain’s secure storage facility.

Leidos was awarded a prime contract by the U.S. Transportation Security Administration to provide support for new, current, and legacy transportation security equipment systems in airports, warehouses, and testing facilities.

Milestone Systems IP video management software and network cameras from Axis Communications are providing security upgrades for the city of Hartford, Connecticut.

Qognify expanded its security solution at Gardermoen Oslo Airport with its Situator situation management solution.

Racom created the unified security platform with the support of Siklu Inc. Etherhaul mmWave radios have been installed as part of an extensive upgrade to the town center surveillance network in Burnley, Lancashire, England.

Smiths Detection was chosen to supply solutions for people screening and search functions in Tokyo’s Narita International Airport following a national directive from the Japan Civil Aviation Bureau.

SuperCom was selected by the government of Bulgaria to deploy its PureSecurity Electronic Monitoring Suite for tracking and monitoring public offenders.

The Australian Department of Immigration and Border Protection signed a three-year contract for managed end-user computing and infrastructure support services with Unisys Corporation.

**AWARDS AND CERTIFICATIONS**


COPS Monitoring received a SOC 2 Type 1 Attestation Report, signifying that its internal controls and processes adhere to the highest standards.

ForeScout Technologies, Inc., announced that its flagship solution ForeScout CounterACT was recognized by the publications CRN and IoT Innovator as a cutting-edge IoT security solution.

Genetec announced that its Kiwi privacy protector module was re-certified with the GDPR-ready European privacy seal.

iManage was named IT Security Pro-

**STRATEGIC MOVES IN THE NEWS**

<table>
<thead>
<tr>
<th>WHO</th>
<th>WHAT</th>
<th>OF/WITH</th>
<th>RESULT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Omnigo Software</td>
<td>ACQUISITION</td>
<td>iView Systems</td>
<td>The acquisition will add a variety of visitor management, license plate recognition, and facial recognition technologies to the Omnigo platform.</td>
</tr>
<tr>
<td>Intermedix</td>
<td>PARTNERSHIP</td>
<td>Rave Mobile Safety</td>
<td>The companies’ emergency notification and crisis information management platforms help improve incident management and communications for higher education institutions.</td>
</tr>
<tr>
<td>ADT</td>
<td>ACQUISITION</td>
<td>Gaston Security</td>
<td>The purchase will help ADT better support its commercial and national account customers, especially in the Mid-Atlantic and southeastern United States.</td>
</tr>
<tr>
<td>Latch</td>
<td>PARTNERSHIP</td>
<td>Comelit</td>
<td>The two companies are integrating their intercom and access systems to create a complete intercom and access solution.</td>
</tr>
</tbody>
</table>
provider of the Year at The British Legal Technology Awards 2017.


LaaSer Critical Communications received a U.S. patent for its emergency caller location technology.

Mercury Security announced that its LP, 602 controller and access control platform won the Security Today New Product of Year award in the Access Control category.

Middle Atlantic Products was awarded a U.S. patent for its RSH Series 1 RU Custom Rackshelf.

The Mircom Group of Companies announced UL Listing for the TX3-CX-1 Single Door Controller.

Raytec’s VARIO2 IP Hybrid Illuminator was recognized for innovative achievement at the Detektor International Awards 2017 in the Video Surveillance category.

Redwall received a U.S. patent for communications systems and methods for enhanced security across wireless devices.

Rohde & Schwarz achieved U.S. Transportation Security Administration certification for its R&S QPS200 Security Scanner.

The Sharp INTELLOS Automated Unmanned Ground Vehicle was named New Product of the Year for Outdoor Perimeter Protection by Security Today and earned the Security Solutions Award for Security Monitoring from Security Sales & Integration.

SmartMetric announced that its biometric card is protected by five new patents.

Stabilitas Intelligence Communications Inc., received a National Science Foundation Small Business Innovation Research award to support the development of the company’s AI-powered security platform.

TerrorMate from TerrorTech LLC won the Best Mobile Technology Product award in the Law Enforcement, First Responders, and Emergency Services category at the 2017 ASTORS Homeland Security Awards.

TrackTik was recently awarded the Startup Canada Global Entrepreneurship Award for the Quebec Region.

Vigilant Solutions, was recognized with the 2017 ASTORS Homeland Security Award for its license plate recognition (LPR) technology, PlateSearch.

Vismo Global Tracking Solutions gained ISO 27001 certification.

ANNOUNCEMENTS

A+ Technology & Security Solutions, Inc., launched a redesigned corporate website with a focus on security.

Airport Operators Association and ITN Productions launched “Airport Matters 2017,” a news and current affairs program that explores security matters in aviation. An early episode features Dallmeier multifocal sensor technology Panomera in operation at Bristol Airport.

Asa Abiyo signed an agreement to acquire August Home.

Axis Communications announced the integration of ZN’s North American operations with Axis North America to help Axis grow in the IP-intercom market.

Digerati Technologies, Inc., plans to acquire Synergy Telecom, Inc.

The FIDO Alliance announced the launch of a FIDO Europe Working Group to accelerate the use of FIDO authentication standards in Europe.

Global Learning Systems launched gamified learning to engage and prepare employees for the European Union’s General Data Protection Regulation.

Life insurance startup Haven Life announced LifeLink, a free mobile app that connects users with 911 and instantly shares an accurate location.

Hikvision USA Inc. launched a cybersecurity hotline that its integrators, clients, and technology partners can call for direct support related to cybersecurity concerns.

IXP Corporation announced an asset purchase agreement for the managed services and consulting businesses of the Safir Companies.

KrollDiscovery opened an ISO 27001-certified data center in Ireland.

LexisNexis Risk Solutions created an advisory committee on governance of its Public Safety Data Exchange to assure adherence to federal, state, and local standards for security and privacy of law enforcement-provided data.

MONI Smart Security hosted the second annual MONI 5K for Children run, raising more than $36,000 for Mission 500 to help children in need.

NAPCO Security Technologies launched its Connected Home & Smart Business Authorized Dealer Program.

OfferUp, a mobile marketplace for local buying and selling, introduced OfferUp Community MeetUp Spots to designate public, well-lit, and surveilled locations for people to exchange goods with confidence.

Pinkerton added litigation support services to its list of security and risk management client offerings.

Point Blank Enterprises acquired substantially all the assets of Short Bark Industries.

San Diego Gas & Electric, in collaboration with the University of California San Diego and the Seismology Lab at the University of Nevada, Reno, unveiled the Alert SDG&E Cameras to improve fire detection via live streaming of San Diego’s most fire-prone areas.

The Secure Technology Alliance developed a white paper to provide a high-level overview of the landscape for payment-enabled wearables.

Working directly with international law enforcement and hazmat agencies, Smiths Detection Inc. adapted a range of existing technologies to be able to quickly and accurately detect fentanyl in an effort to protect first responders.


The University of California Berkeley School of Information is accepting applications for its new online Master of Information and Cybersecurity program, also known as cybersecurity@berkeley.
TERROR ALERTING

TerrorMate, a terror alert app from TERRORTECH, LLC, of Castle Rock, Colorado, is expanding its user alert capabilities to include mass shootings. The free proprietary mobile application alerts users to incident-specific information such as location of the event, number of reported perpetrators, areas to avoid, and number of casualties, along with safety tips and continuous updates during the event. TerrorMate’s solution unifies all channels, supporting communication and collaboration during critical events. On average, TerrorMate alerts users eight minutes faster than the mainstream media. Based in Belgium, TerrorMate’s 24-hour international operations center pairs expert analysis with cutting-edge technology to identify and track terror threats across the globe. 201

METAL DETECTOR

The WMD433 Walk-Through metal detector from ZKACCESS of Fairfield, New Jersey, features program modes for either 1-zone, 6-zone, 11-zone, or 33-zone detection. Alarms located on both sides clearly and precisely indicate where metal is detected. The WMD433 automatically counts people and alarms and readily distinguishes dangerous metal objects from harmless ones, including wristwatches, belts, and coins. Equipped with a 5.7-inch LCD screen, it offers infrared remote control and supports TCP/IP communication. The detector is completely safe to operate and walk through, and poses no harm to heart pacemakers, pregnant women, or magnetic storage media. The unit provides secure operation, because only authorized personnel can access the control panel. 202

CLOUD ACCESS CALENDAR

Google and Microsoft Outlook calendar integration is now available in infinias CLOUD from 3XLOGIC, INC., of Westminster, Colorado. Users can create exception schedules for their doors simply by booking a calendar invitation in a Google or Outlook calendar. Calendar integration requires no user training, so approved staff can easily modify door schedules to accommodate evolving needs and last-minute changes. Schedule modifications can also be managed directly from a mobile device. The infinias access control offers cost-effective security solutions that are easy to manage, simple to install, and scalable. 203
NEW YEAR

NEW RESOURCES

NEW OPPORTUNITIES

Become a member of ASIS International for less than $20 a month to gain immediate access to unparalleled networking, collaboration, and professional development in 2018.

To learn about the advantages of membership—and to join—visit asisonline.org/unleash today!
DRONE DEFENSE

San Francisco-based DEDRONETM released a major software upgrade to its platform to protect airspace from all drone threats. DroneTracker 3 includes automated summary reporting for instant diagnosis of drone airspace activity. Enhancements also include enabling security personnel to instantaneously analyze drone threats; enterprise-grade security and management, allowing for multi-user management and seamless integration into existing security programs; and increased simplification of platform setup, creating an intuitive and quick-to-deploy system. The software is a machine learning network using information from a proprietary database, DroneDNA.

PEDESTRIAN PROTECTION

Surface Guard is a British-designed road-block system that can withstand the force of a 5,500-pound vehicle traveling at 30 miles per hour. Developed by ATG ACCESS of Haydock, United Kingdom, the system is designed to protect pedestrians from targeted vehicle attacks, and it meets the latest international standards. No heavy machinery is required for installation, and four workers can close off a roadway in less than an hour. The system allows pedestrians and cyclists to move freely, and emergency vehicles can pass through when required.

VIDEO WORKSTATION

EQUIUS COMPUTE SOLUTIONS of Edina, Minnesota, unveiled the new i1087TW NVR high-performance video surveillance workstation, a powerful unit in an ultra-compact footprint. The robust video management system viewing workstation supports multiple video feeds on multiple monitors, as well as high-performance storage servers with hard drive capacity up to 48 terabytes. The unit uses an Intel i3, i5, i7, or E3-Xeon CPU with quick sync video. It features four hot-swap drive bays and optional Dual SSD for OS and live view storage. It supports HDMI, display port, and VGA displays and uses the Windows 10 Professional or Windows 10 IoT operating system.

THERMAL BULLET CAMERA

FLIR SYSTEMS, INC., of Wilsonville, Oregon, introduced the FB-Series ID, the latest fixed bullet thermal security camera in the FB-Series. Combining best-in-class thermal image detail and high-performance onboard analytics, the FB-Series ID provides narrow- to wide-area perimeter detection and sterile-zone monitoring. It offers accurate video analytics that are capable of classifying human or vehicular intrusions. Combined with FLIR’s custom Automatic Gain Control and Digital Detail Enhancement, the camera provides excellent image contrast and sharpness, which improves analytic performance, resulting in fewer false alarms. It is certified for integration with third-party video management systems.
Together we can

Educate

Inspire

Heal

Nourish

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

Get involved today! Visit mission500.org for more information.

Supporting Families Across America

For product info #27 securitymgmt.hotims.com
**MARKETPLACE**

**INTRUDER-PROOF DOORS**

Greenwich, Connecticut-based **ARMORED ENTRY** offers ballistic and intruder-proof entry and interior doors that are manufactured to look like standard doors. They can be made in a wide range of styles and colors, with or without ballistic glass packages. Tested to forced entry standard SD-STD.01.01 Rev. G, they can withstand a two-man team for hours. The doors feature drill-resistant manganese locks and a multipoint locking system fitted into 16-gauge galvanized steel frames. They come pre-hung, ready for installation.

**PUBLIC SAFETY**

**GENETEC INC.** of Montreal, Canada, announced the launch of its new public safety decision support system. Created for citywide law enforcement and public safety agencies, Genetec Citigraf features a powerful analytics engine that instantly detects and displays relevant information from disparate systems for interagency collaboration. It collects and manages information from integrated computer-aided dispatch systems, CCTV footage, ALPR data, and more, to identify and display the location of an event using a geographical information system. Integration with gunshot detection technology allows response teams to be notified via a map location and nearby cameras when a gunshot has been detected. This information enables officers and emergency responders to make more effective decisions for situations in progress.

**IMPROVED SURVEILLANCE**

**HONEYWELL** of Louisville, Kentucky, expanded its equiP Series of cameras and the MAXPRO video management portfolio to help security professionals deliver efficient and effective surveillance for complex building environments. The new equiP Series features multi-imager and low-light dome and bullet models supported by new versions of the MAXPRO network video recorder and video management system. The multi-imager equiP cameras help reduce the total cost of ownership by covering a wider area with fewer cameras and leveraging MAXPRO to combine multiple images into one high-quality picture. The new low-light cameras leverage advanced analytics, including Xtralis Loiter and IntrusionTrace, for improved automation monitoring and surveillance productivity.

**BIOMETRIC MODULE**

**LEXTAR ELECTRONICS CORPORATION** of Hsinchu, Taiwan, released the PR88 IR LED packaging module that is used for iris and facial biometric functions, making it one of a few IR LED modules in the industry with double biometric functions. In addition, the company released two IR LED modules with different beam angles that can be widely applied on security systems, access control systems, mobile phones, notebook PCs, and more. The iris and facial double biometric achieves double identification recognition functions with just one module, thus strengthening user security. Its 1.4mm ultra-slim design saves space for terminal applications.
REQUEST DETAILED PRODUCT INFORMATION THROUGH OUR MONTHLY E-RESPONSE, VISIT HTTP://SECURITYMGMT.HOTIMS.COM, OR USE YOUR SMART PHONE TO ACCESS THE QR CODE ON THIS PAGE.

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

CIRCLE # | PAGE # | CIRCLE # | PAGE #
---|---|---|---
07 | Abloy Security, Inc. | 17 | 03 | Hikvision USA |
28 | Brownyard Group | . | 75 | 06 | Mission 500 |
14 | Cognitec | . | 32 | 27 | Red Hawk Fire & Security |
15 | Commport Technologies | . | 37 | 29 | Research Electronics, Int'l |
24 | Detex Corporation | . | 55 | 11 | 27 | Special Response Corporation |
06 | DSX Access Systems, Inc | . | 13 | 08 | TSCM America |
05 | GAI-Tronics Corporation | . | 11 | 20 |

ADVERTISERS ONLINE

Abloy Security, Inc.
www.abloyusa.com

Brownyard Group
www.brownyard.com

Cognitec
www.cognitec.com

Commport Technologies
www.comm-port.com

Detex Corporation
www.detex.com

DSX Access Systems, Inc.
www.dsxinc.com

GAI-Tronics Corporation
www.gai-tronics.com

Hikvision USA
www.hikvision.com

Mission 500
www.mission500.org

Red Hawk Fire & Security
www.redhawkus.com

Research Electronics, Int'l
www.reiusa.net

SecurAmerica
www.securamericallc.com

Special Response Corporation
www.specialresponse.com

TSCM America
www.tscmamerica.com
The US-China Business Council found in its twelfth annual member survey that for those doing business in China, technology transfer requests are an “acute issue for those who face it.” Often these companies are concerned about intellectual property rights protection and data theft when transferring technology to China.

**Technology Transfer**

- **19%** were directly asked to transfer technology to China.
- **10%** complied to do business.
- **10%** withdrew from proposed business.
- **50%** mitigated request, but still transferred some tech.
- **30%** transferred tech.

**Intellectual Property Rights Protection**

- **94%** expressed concerns about enforcement.
- **22%** IP infringement of greatest concern.
- **16%** trademark.
- **6%** copyright.
- **6%** other.

**Cybersecurity and IT Issues**

- **82%** companies either somewhat concerned or very concerned about data flow restrictions and cybersecurity.
- **55%** inability to utilize global IT solutions or non-Chinese cloud-based applications in China.
- **53%** restrictions on cross-border data flows in Chinese regulations.
- **53%** consumer or company data theft.
- **51%** internet service within China (speed, performance, etc.).

**Top 5 Company Concerns on Cyber-related Issues**

- **65%** top 5 company concerns on cyber-related issues.

**Type of Activities Limited Under IPR Enforcement**

- **2016**
  - Research & Development: 42%
  - Product Manufacturing: 41%
  - Sale of Products: 30%
  - Product Licensing or Co-manufacturing: 39%

- **2017**
  - Research & Development: 37%
  - Product Manufacturing: 37%
  - Sale of Products: 38%
  - Product Licensing or Co-manufacturing: 32%

**Source:** 2017 Member Survey, US-China Business Council, December 2017
When the **UNEXPECTED** Strikes

**EXPECT THE BEST FROM BROWNGUARD® INSURANCE**

65 years of meeting and exceeding our Security Industry clients’ expectations.

**When it comes to insurance, there are no surprises with Brownyard Group.**

As the longest-running, family owned and operated specialty insurer, we set high expectations for ourselves – a continuing promise to apply our deep knowledge of security industry risks to deliver exceptional coverage, risk management and claims handling to Security Professionals.

Set high expectations for your insurance with BROWNGUARD – contact us for a competitive quote.

**Brownguard®**

*Insurance when you expect the BEST*

800-645-5820 brownguard@brownyard.com brownyard.com

For product info #28 securitymgmt.hotims.com

*We Insure: Security Professionals, Private Investigators, Security Consultants & Alarm Services*
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