ISSUE & BEYOND

- **Terrorism**
  If incidents are down, why are people more worried?

- **Hacking**
  Experts say that Russian cyberattacks are the new propaganda.

34 RETAIL LOSS

44 THEFT

50 MANAGING

56 AIRPORTS
PROVEN THE WORLD OVER.

DahuaSecurity.com/ProvenSurveillance

For product info #1 securitymgmt.hotims.com
SIMPLY SUPERIOR.

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

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

TALKAPHONE.COM | 773-539-1100

VISIT US AT ISC WEST
BOOTH #10109
To Secure an Airport...

success is all about choosing the Right Products.

- The right Barriers
- The right Sensors
- The right Gates
- The right Fences
- And most important of all, the right Guard Station/House

If you don’t protect your staff and systems, they can’t protect the airport and its traffic

A B.I.G. guardhouse is different from all others because we have invested over 40 years in studying and understanding what goes on inside—and outside—of a superior guard station. This expertise comes to you in the form of a full line of B.I.G. Enterprises guardhouses—the cornerstones of your “hardened” perimeter. With B.I.G. your guardhouse doesn’t have to appear hard and unattractive—it can be your steel fist inside of a velvet glove.

We Asked B.I.G. to Go Where Others Can’t Go.

“I want to compliment B.I.G. on giving us what we needed. I was expecting to hear, “That’s something we’ve never done before”. When all was said and done, the B.I.G. structures exceeded our expectations. According to our engineers, these are built better than any shelters they’ve ever seen. The B.I.G. design and engineering people were extremely helpful and flexible. If you want quality product, buy from B.I.G.”

—Transit Facility Architect

For product info #3 securitymgmt.hotims.com

When extreme threat levels are an issue, call in the security heavyweights—because an airport perimeter without B.I.G. is like a holster without a gun.

WWW.BIGBOOTH.COM
Ph. 626-448-1449
Toll Free 1-800-669-1449
“It’s time to reconsider how retail companies understand and measure the losses they experience.”

Adrian Beck, professor of criminology at the University of Leicester. He undertook the recent study Beyond Shrinkage: Introducing Total Retail Loss, commissioned by the Retail Industry Leaders Association’s Asset Protection Leaders Council. PAGE 36

“Clearly, I underestimated the willingness of Russia to use disruptive attacks on the United States.”

Adam Segal of the Council on Foreign Relations speaking to the American Bar Association on his prediction that the former Soviet states would attack each other, not the United States. PAGE 32

“Terrorist operatives generally possess poor surveillance tradecraft and are not difficult to spot if people are looking for them.”

Scott Stewart, vice president of tactical analysis at Stratfor.com and lead analyst for Stratfor Threat Lens. PAGE 62

“Empathy is a significant leadership competency—especially in 2017. Employees who think their employers care about them as people are more likely to give above and beyond.”

Management expert Bob Kelleher, who runs the Employee Engagement Group consultancy. PAGE 53

40% Percentage of shoplifters who are juveniles. PAGE 44

29,376 People killed by terrorist attacks in 2015. PAGE 25

$41.5B The projected value of the global biometrics market in 2020. PAGE 28
Hidden or Front and Center
Ideal for covert and aesthetic installations
RETAIL THEFT
SURVEILLANCE AND STEREOTYPES
Through original research, these authors found that criminal stereotypes impact the surveillance and sanctions of juvenile shoplifters.
By Lauren R. Shapiro and Marie-Helen Maras

MANAGING
CULTIVATE ENGAGEMENT
Low employee engagement is a widespread challenge. But there’s a host of best practices security managers—and organizations—can employ to address the issue.
By Mark Tarallo

AIRPORTS
THE EVOLUTION OF AIRPORT ATTACKS
Terrorists have been targeting airports since the 1960s in a continual game of cat-and-mouse with security professionals.
By Scott Stewart
Avigilon Appearance Search™ video analytics technology is a sophisticated search engine for video data. It sorts through hours of footage with ease, to quickly locate a specific person of interest across an entire site.

Avigilon Appearance Search technology can dramatically improve incident response time and enhance forensic investigations by allowing operators to build robust video evidence and create a powerful narrative of events.

- Improves incident response time
- Enhances forensic investigations
- Accurately provides search results
- Easy to learn and use

Learn more at avigilon.com/Appearance-Search
RISK MANAGEMENT

For federal agencies, enterprise risk management (ERM) provides ways to better anticipate and manage risk. In a recent report, Enterprise Risk Management: Selected Agencies’ Experiences Illustrate Good Practices in Managing Risk, the U.S. Government Accountability Office describes its enterprise risk management framework. It enumerates six essential elements for implementing ERM. The report also identifies strategies that work and provides real-world examples of best practices from federal agencies that are using ERM.

ONLINE HIGHLIGHT

NEW ONLINE THIS MONTH at www.securitymanagement.com
Everybody.

Everywhere.

Every day.

Ordinary days require extraordinary protection.

Find out more about the software behind the everyday at genetec.com/protectingeveryday

For product info #6 securitymgmt.hotims.com

© 2017 Genetec Inc. GENETEC and the GENETEC LOGO are trademarks of Genetec Inc., and may be registered or pending registration in several jurisdictions.
EDITOR’S NOTE

T

rees are competitive. Long-standing scientific theory tells us that trees race towards the forest canopy to access the light. Thus, weaker trees suffer, eventually withering and dying in the shade. Suzanne Simard begs to differ. She says that this theory of forest life is far too simplistic. Simard, a professor of forest ecology at the University of British Columbia in Vancouver, Canada, found that trees cooperate rather than compete.

In experiments ranging over decades, Simard found that trees fare best when they live in diverse groups. For example, Simard found that a birch tree and a fir tree could live harmoniously near one another in the forest. However, when the birch was removed, “the Douglas fir became diseased and died,” Simard told the hosts of the RadioLab on their podcast titled “Tree to Shining Tree.” Simard continued, “There was some kind of benefit from the birch to the fir; there was a healthier community when they were mixed, and I wanted to find out why.”

It turns out that a complex underground web of fungi connects the trees allowing the transfer of food, nutrients, and beneficial bacteria. The fungus draws the water and minerals that the tree needs from the ground. And the tree reciprocates by giving the fungus the sugar it needs to survive.

Not all trees tap into this network. But those that do, have the advantage. “You find twice the amount of life-giving nitrogen and phosphorous in plants that cooperate with fungal partners than in plants that tap the soil with their roots alone,” writes Peter Wohlleben in his book The Hidden Life of Trees.

The fungi serve as a communications network: A tree damaged by a beetle infestation can send a warning to other trees, so those trees can emit a chemical to repel the invaders.

Through this underground infrastructure, trees can also help one another. “Paper birch send carbon to Douglas fir seedlings, especially when they are shaded in summer, probably enhancing their survival.” writes Jennifer Frazer in her blog “The Artful Amoeba” on the Scientific American website. “In spring and fall, the Douglas fir return the favor when the birch have no leaves.”

This symbiosis may be startling when discovered in a forest, but it should be commonplace within companies. Within ASIS International there must be cooperation among magazine staff, headquarters personnel, and members. These groups are most successful when advancing a common goal.

In this spirit, this issue of Security Management includes several changes. “Homeland Security” is now called “National Security” to reflect the concerns of nations around the world. Updated graphics will better connect the written word with the visual to present compelling and vibrant storytelling. And, a new standalone “ASIS News” department now serves as one more conduit for information sharing among headquarters staff and members from around the world.
Everything you need to stay secure. G4S brings innovation to the forefront to help you leave risk behind. We can assess, equip, integrate and staff an end-to-end solution to secure your people, property and assets. It’s physical security for your company and emotional peace of mind for your people, all created by the integration of our unique products. To learn more about G4S Integrated Security Solutions, please visit www.g4s.us or email us at info@usa.g4s.com.
The report, *Terrorist Incidents and Attacks Against Jews and Israelis in the United States, 1969-2016*, examines the FBI’s annual hate crimes report for the years under study. For example, in 2015, 1,354 hate crimes were recorded in the report. Of those, 695 incidents, or 51 percent, targeted Jews. “This is a consistent finding of the FBI report over many years,” writes the report’s author, counterterrorism expert Yehudit Barsky.

Going deeper, the report catalogs 104 incidents in 2015 to better characterize the attacks. The majority, 51 percent, targeted synagogues, followed by community institutions (14 percent), Jewish persons (13 percent), and educational institutions (10 percent). In terms of means of attack, arson, shootings, and explosive devices were used in about equal frequency.

Year-over-year, the total number of attacks has been declining, but they have been increasingly lethal and have claimed many more victims,” Barsky writes.

And the threat has been revived several times in the last few years. In October 2015, the Islamic State (ISIS) militant group directed its followers worldwide to kill Jews. ISIS’ Al-Masra Foundation issued a video, *The Slaughter of the Jews*, which called for followers to “Stab the Jew with a knife or run over him with a car; poison him; bring back explosives, the [use of] explosive belts and IEDs; burn their faces and their houses.”

Then in 2016, ISIS published an article in its *Al-Naba* publication that...
called for followers to help Palestinian Muslims by fighting Jews around the world: “killing them, destroying their property, and harming their interests in any way they can.”

The report also includes some lessons learned and related recommendations for future security. Jewish targets sometimes serve as precursors to larger attacks. The perpetrators of the 1993 World Trade Center bombing, for example, were previously involved in anti-Jewish attacks.

And in many of the incidents, the attackers conducted preoperational surveillance. For example, in 2014, neo-Nazi Frazier Glenn Miller carried out preoperational surveillance at two Jewish organizations that he later attacked.

“This phase of a typical attack cycle is the most likely point for detection, and thus recognizing it can avert or minimize an impending attack,” Barsky writes. “Training and engagement of community members is thus essential.”

While the U.S. Department of Homeland Security announced that it would step up efforts to support Jewish communities, others are working at the grassroots.

For example, the concept of the training and engagement of community members is at the heart of operations at Community Security Service (CSS), the non-profit group that sponsored the report and whose mission is the protection of the people, institutions, and events of the American Jewish community. CSS started in 2007 with a small group of volunteers. It now has more than 3,500.

“The differentiator is—it is an entirely volunteer organization,” says Don Aviv, CPP, PCI, PSP, who is COO and director of physical security at Interfor International and a founding member of CSS. Aviv is also vice chairman of the ASIS International Security Services Council.

CSS serves as a security partner for various Jewish institutions and events, ranging from the National Menorah lighting in Washington, D.C., to an annual sit-down dinner of roughly 6,000 rabbis held in conjunction with a religious conference in Brooklyn.

The idea was, no one can protect your community better than yourself.

However, community. “The idea was, no one can protect your community better than yourself,” Aviv says. And so volunteers from the community are trained in the basics of security, including practices such as recognizing threats and devising a system to report threats or other incidents.

The training includes aspects like scenario-based exercises and helping volunteers maintain a higher level of security awareness by checking their surroundings daily. An important component is helping volunteers develop a level of comfort with being part of the security effort. “It comes down to motivating the individual member to be a part of their community” in an “empowering and enfranchising” way, Aviv says.

Community members are treated as partners in security to be worked with, not as people to be ordered around by those leading the security effort. “We don’t enter into a community without being invited. We’re not forcing our way in,” Aviv explains.

The other key aspect of CSS’s model is that security is achieved through a partnership among community members and volunteers, contract security, and law enforcement. This is accomplished through training and by building up a framework of interaction for all stakeholders.

For example, community members are advised that, if they decide to use contract security, they should not just hire security officers and then walk away and expect them to take care of SAFETY CONCERNS

Most U.S. police officers say they have become more concerned about their safety as a result of high-profile incidents involving black citizens and the police.

Behaviors Observed in Officers’ Departments

- Officers have become less willing to stop and question people who seem suspicious: 72%
- Interactions between police and black citizens have become more tense: 75%
- Officers have been more reluctant to use force when it is appropriate: 76%
- Officers have become more concerned about their safety: 93%

SOURCE: Behind the Badge, Pew Research Center, January 2017
everything: “You’re putting too many expectations on their shoulders,” Friedman says. Instead, by working with them, the community will receive a better return on its investment.

Similarly, volunteers embedded in the community will communicate with law enforcement officers, so that the officers know the community’s concerns and issues and do not have to “parachute in” blindly. “We’re a force multiplier for federal and local law enforcement,” Aviv says.

While CSS is dedicated to protecting the Jewish community, its cooperative community-based model of security is replicable for use by other populations as well, Aviv says. “At the end of the day, the threats facing us are similar to those facing other groups,” he says.

ERM BEST PRACTICES

**WITH THE RISE** of Enterprise Risk Management (ERM) programs in the security field, some leaders are on the hunt for ERM best practice guidance resources. One recent report, courtesy of the U.S. government, contains guidance that may be applicable to private sector security operations.

Last year, the U.S. Office of Management and Budget (OMB) called on federal agencies to implement ERM so that federal managers could more effectively manage risks that could affect agency strategic objectives.

Given OMB’s call, the U.S. Government Accountability Office decided to update the government’s risk management framework and identify good practices that some agencies have been using. The new report, *Enterprise Risk Management: Selected Agencies’ Experiences Illustrate Good Practices in Managing Risk,* identifies six components of successful ERM programs, and then describes best practices that apply to each.

The six components and their best practices are as follows:

**ELEMENT ONE:** Align the ERM process to goals and objectives.

Senior leaders are fully engaged and committed to the ERM process, and they support how ERM contributes to the agency’s goal-setting process. This engagement helps demonstrate the importance of ERM to agency staff.

**ELEMENT TWO:** Identify risks.

Successful agencies develop an organizational “risk-informed” culture in which employees are encouraged to identify and discuss risks openly. This openness is critical to ERM success.

---

**BOOK REVIEW**

**OPERATIONAL POLICY MAKING**

**BY ALLEN R. SONDEJ.** Butterworth-Heinemann; Elsevier.com; 242 pages, $49.95.

SECURITY professionals will want to keep this volume handy for constant use. As the title promises, *Operational Policy Making for Professional Security: Practical Policy Skills for the Public and Private Sector* offers a thorough treatment of policy making, from theory to execution, as well as everything needed to formulate, communicate, and implement necessary policies properly.

While a book that discusses policies and procedures is rarely described as an interesting read, this one is an exception. The author manages to turn a dry subject into a topic that keeps the reader turning page after page. The use of frequent case histories and real-world examples helps the reader understand how policy can protect a company or institution or, conversely, be its downfall in a court of law.

Good policy as a cornerstone of encouraging effective performance is the main idea that resonates throughout the book. While longtime security management professionals may not think of policy and procedure as the building blocks that drive their staff members to success, the author sets the stage for this truth. A successful security program must be grounded in security protocols based on fundamental and established policies and practices. Procedures are written to support those policies. Well-written policy and procedure allows staff to operate effectively and efficiently, while highlighting personnel and issues that do not. It all begins with identifying and developing necessary policy. This book shows security professionals how to do that.

The book is well organized, with a comprehensive table of contents and index, and it covers a wide spectrum of the information needed to understand, develop, communicate, and implement effective policies. Special features highlight and recap main points from each chapter, providing the reader with easy reference. The appendix contains examples of a job description and a general policy, illustrating what each should contain.

Almost everyone who serves in a leadership position is responsible for developing and implementing policy. This book can and should serve as a how-to-guide for creating powerful policies that will assist in the protection of the company or institution, enabling the security program to perform successfully and effectively.
When the situation turns dark, you can respond at the speed of light.

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

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

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

Whether your campus buildings are decades old or only a blueprint, visit www.detex.com/lockdown4 and let us help you identify your ideal lockdown system.
Successful agencies develop an organizational “risk-informed” culture.

ELEMENT THREE: Assess risks.
Successful agencies can integrate prioritized risk assessments into their strategic planning and organizational performance management processes. This integration of risk assessments helps improve the budget process, resource allocation planning, and other aspects of operations.

ELEMENT FOUR: Select risk response.
Successful agencies establish an ERM program that is customized to fit their particular operations. Once established, risk factors are regularly considered, and leaders select the risk response that is most appropriate for the structure and the culture of the agency.

ELEMENT FIVE: Monitor risks.
Successful agencies are able to continuously manage risk by conducting the ERM reviews on a regular basis. Leaders also monitor the selected risk response with performance indicators that allow the agency to track results and the response’s impact on the mission. Leaders can then determine if the risk response is successful or if it requires additional actions.

ELEMENT SIX: Communicate and report on risks.
Sharing risk information and incorporating feedback from internal and external stakeholders helps organizations better identify and manage risks. It also increases transparency and accountability to Congress and taxpayers.

See SM online for the full GAO report.
Smart access revolves around the entrance.

Smart access creates a welcoming entrance with a high degree of security. Meeting both aesthetic and safety requirements can be achieved for new construction or renovation with dormakaba physical access systems. Our comprehensive project support ensures your system performs as designed for the life of your building. From design consultation and specifications to installation and scheduled maintenance — **Smart access begins at dormakaba.**

Call 844-773-2669 for comprehensive project support. DORMA and Kaba are now dormakaba. Visit go.dormakaba.com/PAS-SMMag

For product info #11 securitymgmt.hotims.com
This redistribution of terrorist activity, along with less-organized but equally lethal homegrown extremist-style attacks, has kept fears of terrorist attacks high around the world, experts say. According to data from the National Consortium for the Study of Terrorism and Responses to Terrorism (START), the concerns of U.S. citizens when it comes to terrorism have not declined much since the September 11, 2001, attacks. Security Management spoke to Gary LaFree, director of START, to gain insight on these reports.

“We tracked a decline in worldwide attacks between 2014 and 2015, with fatalities and ISIS attacks reducing,” says LaFree. “You want to say that’s good news, but at the same time, we found there was a terrorist attack somewhere in the world every single day of 2015. You can interpret these statistics in a lot of different ways. It’s pretty easy to get the sense that we’re awash in terrorism, even though it’s still a relatively rare event [in the United States].”

LaFree tells Security Management that there are many different ways
Enable security staff to perform high quality inspection against explosives, weapons, narcotics and other contraband hidden under vehicles.

**CPAS Series under vehicle surveillance systems**

The CPAS series of under vehicle surveillance systems offer high resolution color composite scanning up to 900FPS for vehicles traveling up to 75KMPH. With no limit on scanning length, these ruggedized flush mount frames are ideal for secure vehicle entry points at Government, Military and Corporate facilities.

The CPAS series is the best system for:

- Vehicle inspection
- Seaports with container code readers
- Airport parking with pay tickets
- Embassy entrances with RFID
- Access control points with car tags and RFID
- DoD entrances for hot list tracking
- Law Enforcement Agencies with wanted list
- Toll Plaza collections with RFID and pay receipts

- **NEW:** Multiple Lane / Multi-Gate Support
- **NEW:** Support for RFID vehicle inspection
- **NEW:** ACDM software for computer vision analysis
- Detailed anomaly detection of foreign objects
- Standard 78 Ton weight capacity
- High resolution color area scan technology with up to 900 FPS
- Complete composite image with perfect capture up to 75KMPH
- Automatic ANPR / LPR (license plate recognition)
- Database management in local or networked versions
- Ruggedized to operate in the harshest environments
- Includes driver image / scene cameras
- Worldwide support available

Comm Port Technologies, Inc. | 1 Corporate Drive, Suite F | Cranbury, NJ | 732-738-8780
find out more at: www.comm-port.com | email: info@comm-port.com

For product info #12 securitymgmt.hotims.com
to interpret terrorism trends and the public’s resilience to attacks. On the one hand, he says, one of the goals of terrorism is to frighten and divide citizens, and, as his data shows, the public still thinks about terrorism almost as much as it did in the months after 9/11. However, LaFree says that citizens are more willing to report suspicious activity and be more engaged with the government overall due to their fears.

“What the data shows is a fairly high level of concern, still, now that we’re more than 15 years from 9/11,” LaFree says. “That has not dissipated. People really are still concerned about terrorist attacks.”

In 2012, START conducted a survey of more than 1,500 Americans on what LaFree calls “a barometer of how the public was feeling about terrorism.” START found that 15 percent of respondents thought about terrorism at least once a week—significantly higher than those who thought about hospitalization or violent crime victimization—and as part of the survey methodology, the organization planned to conduct three more waves of surveys to track changes in attitude.

But following the April 15, 2013, Boston Marathon bombings, where two homemade bombs killed three people and injured several hundred others, START realized it had a baseline of behavior before the attack and could leverage that in its ongoing research. “Events in Boston provided us with an unexpected opportunity to examine how public attitudes toward terrorism and counterterrorism policies in the United States changed before and after an actual terrorist attack,” noted one of the resulting reports, U.S. Attitudes toward Terrorism and Counterterrorism before and after the April 2013 Boston Marathon Bombings.

Surprisingly, the surveys found that many of the attitudes sampled in 2012—such as the frequency at which people thought about terrorist attacks or the likelihood of an attack in respondents’ own communities—did not change after the bombings. Significant changes included a higher percentage of people who believed a terrorist attack could happen on U.S. soil; a decrease in those who thought the government could effectively prevent terrorism; and a willingness to call the police in situations relating to terrorism.

LaFree says that START continued the surveys to understand how an attack on American soil might affect citizens’ attitudes towards terrorism, including the lasting desire to cooperate with the government when it comes to terrorism threats.

“What happens with the public is they get more concerned about terrorism when there’s a high-profile event, and they also report greater willingness to cooperate with federal officials to prevent further attacks,” LaFree explains. “That however
When network dependability is critical, the transmission products you choose today affect how your network performs tomorrow.

ComNet - Communication Solutions for the Long Term

- Only ComNet Offers a Complete Fiber Optic, Copper, and Wireless Communication Solution
- ComNet Products are MADE IN THE USA
- Exclusive LIFETIME WARRANTY
- Experienced ComNet Customer Care Specialists Who Understand Your Application are Here to Support Your Every Need

www.comnet.net

Visit Us at ISC West 2017 | Las Vegas | Booth 4071 | April 4 - 7

Contact the ComNet Design Center for Free Assistance in Choosing the Correct Fiber Optic, Copper or Wireless Connectivity Solution - Call 1 888 678-9427 or 1 203 796-5300, or Email designcenter@comnet.net

info@comnet.net
www.comnet.net/register
Tel: 1 203 796-5300
Toll-Free: 1 888 678-9427
For product info #13 securitymgmt.hotims.com
dissipates over time—the longer you get away from a big attack, the less likely they are to see that, so the original change that’s produced disappears. What’s interesting is that their knowledge of the system doesn’t change over time—they continue looking for information to inform themselves, and that part they keep long after the attack.”

Despite the sustained public mindfulness of terrorism since 2001, LaFree says that he is heartened by the public’s ability to work with officials while knowing where to draw the line. “After Boston, respondents were more likely to say they would cooperate with police and government officials, but they didn’t give carte blanche either,” LaFree explains. “A lot of people said they would report people that look suspicious with regard to bombmaking, but only a tiny minority said they would report someone who had terrorist literature in their possession. We drilled down on those questions, and they said, ‘well this is America, we have freedom to read what we want to read, and it’s not against..."
the law.’ Even their responses in the aggregate were pretty reasonable.”

While terrorism deaths declined in 2015 for the first time since 2010, it was still the second-deeadliest year since 2000, with terrorism claiming the lives of 29,376 people. However, 72 percent of the deaths occurred in five countries: Iraq, Afghanistan, Nigeria, Pakistan, and Syria. But the leap in high-profile terrorism-related deaths in OECD countries, including attacks on Charlie Hebdo in France, a museum in Tunisia, a bombing in Baghdad during Ramadan, and the coordinated attacks on soft targets in Paris, combined with the increased prevalence of social media makes it hard to keep today’s terrorism in perspective.

“Public opinion in the United States can now be affected by events that happen halfway around the world,” LaFree notes. “The interconnectedness of the United States has really changed, and that probably contributes to the public’s perception of this drumbeat of terrorism.”

In reality, terrorism-related deaths in the United States are historically low, compared to the 1970s, according to the START global terrorism database. The U.S. rates of terrorism are inversely related to world rates, which have continued to go up since 9/11.

While LaFree says he doesn’t think the public is being overly concerned, there is a more existential aspect to the sustained level of fear.

“Your chances of dying from lots of other things are much greater than terrorism, and that’s where we started this conversation,” LaFree states. “What we’re arguing is we need to stay vigilant and do a good job of protecting ourselves from the most serious threats, but we also need to realize that thus far in the history of terrorism, we haven’t faced existential threats of the nature we faced during the Cold War and nuclear annihilation,” according to LaFree. “It’s not a very flashy message if you think about it, but it’s as truthful as I think we can be.”

To view the reports, visit SM Online.

After Boston, respondents were more likely to say they would cooperate with police and government officials.
“There’s a great deal of skill and care that goes into producing the food that we provide to our customers,” says Richard Newman, director of corporate security at Gate Gourmet for the United States and Canada. “It’s important to Gate Gourmet that we deliver the highest quality product that we can, in the safest way we can.”

With approximately 25 catering facilities nationwide, Gate Gourmet serves airline clients that fly out of major U.S. airports.

One of Gate Gourmet’s larger facilities is located at the Washington Dulles International Airport near Washington, D.C. Employees at the location produce 18,000 to 25,000 meals a day, depending on the season. “The busiest fast food restaurant you can think of probably does about 8,000 meals a day,” Newman says. “We’re doing three to four times that just out of the Dulles kitchen.”

Who gains access to Gate Gourmet facilities is crucial. “As part of a layered approach to security, it’s important that we make sure that the people that are supposed to be on the inside can get inside, and the people that aren’t, don’t,” Newman says.

Beyond protecting its product and the customers it serves, Newman adds that the U.S. Transportation Security Administration (TSA) has its own security guidelines Gate Gourmet must adhere to. “Because we’re in the aviation industry—and there is a layer of security that the industry puts on everything that goes on an airplane—those rules apply to us as well,” he explains.

The operation at a Gate Gourmet kitchen is complex, Newman says. It includes preparing the meals, packing them onto trucks, and delivering...
Quantum Secure’s SAFE software suite streamlines and automates secure identity management, compliance and operational analytics across multiple sites and systems in a single, fully interoperable platform—allowing you real time visibility into your entire security infrastructure. Already the leader in physical identity and access management software, we are now partnered with HID Global, meaning your investment in best-in-class technology can be made with confidence. Find out how to lower your risk profile and operational costs by visiting quantumsecure.com/know.

NOW YOU’LL KNOW.
quantumsecure.com/know

Visit us at ISC West 2017 in the HID Global booth #11063

For product info #17 securitymgmt.hotims.com
them directly to the airplanes and the flight attendants who will ultimately serve the food.

“When the trucks come back from the airfield, they’ll bring the carts that have the dirty dishes into the kitchen, then we go through the dishwashing process, wash the equipment, and then the whole process starts again,” he says.

To monitor the employees coming in and out of work, Gate Gourmet had been using hand geometry at its Washington Dulles location. With this biometric technology, a user places his or her hand over a scanner that measures the shape of the palm.

While the palm method was effective at identifying employees, it wasn’t necessarily efficient for the company. “We wanted to move into something that was faster, easier, and touch-free,” Newman notes.

In 2013, Gate Gourmet was on the lookout for a new biometric access control solution, and came across the iCAM iris reader from Iris ID at that year’s ASIS International Seminar and Exhibits in Chicago. “I saw their booth at the convention; they gave me a demonstration, and I was impressed,” Newman explains.

“Many people it can take the picture and recognize your eyes through your glasses, through your contact lenses—that’s helpful to us,” Newman adds.

When the system is ready for enrollment and iris capture, a user walks up to the reader, standing about an arm’s length away, and a yellow light appears. Once the administrator presses the enroll button, and the user has the camera properly centered on the bridge of his or her nose, the light turns green. The technology also has an automated voiceover that guides the user through the process.

Once the iris is properly captured, the administrator adds the rest of the enrollee’s information and registers them as a user in the system. “There’s actually not a photograph stored; it’s all reduced to a code through an algorithm and stored in a database,” Newman explains.

The company evaluated four different solutions from vendors to replace the palm scanner. After narrowing it down to two technologies, including Iris ID’s iCAM, Gate Gourmet began pilot testing the products in February 2014 at Washington Dulles. During the testing, which lasted for two months, the company deployed one technology at the entrance where employees report...
to work and another at the exit where they leave the premises.

Gate Gourmet was impressed with the speed of the iCAM, as well as with the price point, which was similar to the palm technology already in place. Newman found that enrollment takes a matter of minutes, and daily use is even faster.

“It takes one or two seconds to check an employee in, which is four times as fast as the technology it’s replacing,” Newman notes.

He adds that iris identification results in fewer false positives—when the system thinks the iris belongs to someone else who is registered—than other biometrics like palm reading technology. This is because there are so many unique points within the eye that can be mapped out and recorded by the system, says Newman.

The company ultimately chose to go with Iris ID, and Newman says the deployment process has been seamless. “Of all the technology that I’ve deployed since I’ve started with the company, this has probably been the easiest rollout just because of the nature of the technology.”

Employees are granted access in and out of the facilities at the beginning and end of their shifts by having their irises scanned in nearly the same way in which they enrolled.

To be granted access, Gate Gourmet requires dual authentication. In addition to using the iris scanner, employees must introduce a credential to a card scanner. Newman adds that the iris enrollment process is only for employees. Visitors have a sign-in and escort protocol, and “visitors are issued specific media to identify them,” according to Newman.

The iris identification registration system is administrated from the Gate Gourmet headquarters in Dulles, Virginia, but each location with iCAMs has the ability to enroll and remove people from the system. This allows the company to keep the registration updated when employees leave Gate Gourmet.

The iris scanners are still being deployed across many of its locations, and Gate Gourmet hopes to eventually install the Iris ID iCAMs at all of its U.S. locations.

Newman emphasizes that upgrading from the previous biometric solution has not compromised security, but only enhanced it, for Gate Gourmet.

“We’re replacing biometrics with biometrics,” Newman says. “We haven’t surrendered anything by having the iris scanners—this is just the next generation for us.”

FOR MORE INFORMATION:
Tom DeWinter, Iris ID, tdewinter@irisid.com, www.irisid.com, 609/819-4724

Compact Design...

...Maximum Reliability!

GAI-TRONICS®
A Hubbell Company

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

For product info #19 securitymgmt.hotims.com
During the Cold War, VOA took on a new target—Soviet propaganda—and concentrated its message on communist nations in eastern and central Europe. By 1953, VOA was broadcasting 3,200 programs in 40 languages every week.

And America was not alone. The Soviet Union soon began adopting similar technology, attempting to influence elections through radio broadcasts, campaign funding, and recruitment efforts. In the 1970s, for example, during a U.S. presidential race, the Soviet KGB recruited a U.S. Democratic party activist to report on Democrat Jimmy Carter’s campaign and foreign policy plans.

Fast-forward to the present, when influence is no longer restricted to radio broadcasts or recruiting covert agents; it’s now being conducted on social media by nation-states. In an unprecedented unclassified report, the U.S. intelligence community detailed Russia’s most recent efforts to influence the 2016 U.S. presidential election in favor of candidate and eventual president Donald Trump.

The report, crafted by the U.S. National Security Agency (NSA), the CIA, and the FBI, and released by the U.S. Office of the Director of National Intelligence, found that Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the U.S. presidential election.

Putin’s goals, according to the report, were to undermine public faith in the U.S. democratic process, denigrate Democratic candidate...
former U.S. Secretary of State Hillary Clinton, and harm her electability and potential presidency.

“In trying to influence the U.S. election, we assess the Kremlin sought to advance its longstanding desire to undermine the U.S.-led liberal democratic order, the promotion of which Putin and other senior Russian leaders view as a threat to Russia and Putin’s regime,” the report explained.

To carry out this influence campaign, Russia used a messaging strategy that blended covert intelligence operations with overt efforts by Russian government agencies, state-funded media, third-party intermediaries, and paid social media users—known as trolls.

“The Kremlin’s campaign aimed at the U.S. election featured disclosures of data obtained through Russian cyber operations; intrusions into U.S. state and local electoral boards; and overt propaganda,” the report added. “Russian intelligence collection both informed and enabled the influence campaign.”

For instance, in July 2015 Russian intelligence organizations gained access to the U.S. Democratic National Committee’s (DNC’s) networks and maintained access to them until June 2016. Using this access, Russia’s General Staff Main Intelligence Directorate (GRU) compromised the personal email accounts of Democratic Party officials and political figures, including Clinton’s campaign chair, John Podesta.

Then, under the alias Guccifer 2.0, the GRU leaked those emails to DCLeaks.com and WikiLeaks, which shared information with RT—the Kremlin’s principal international propaganda outlet, which has more than 4 million Likes on Facebook and 2 million followers on Twitter.

“Russia’s state-run propaganda machine... contributed to the influence campaign by serving as a platform for Kremlin messaging to Russian and international audiences,” according to the report. “State-owned Russian media made increasingly favorable comments about President-elect Trump as the 2016 U.S. general and primary election campaigns progressed, while consistently offering negative coverage of Secretary Clinton.”

For instance, Russian media began to call Trump’s impending victory a “vindication of Putin’s advocacy of global populist movements” and the “latest example of Western liberalism’s collapse.”

Millions of people viewed these articles and shared them on social media, spreading them among U.S. voters. The U.S. intelligence community did not conduct opinion polls to see how Russian propaganda influenced voting behavior, said former Director of National Intelligence James Clapper in a Senate hearing. But he did reinforce...
the report’s assessment that Russia will apply lessons it learned from the campaign to future efforts to influence the United States and its allies.

And, because Americans elected Trump in the 2016 election, Russia is likely to view its influence campaign as a success and continue using similar methods to influence future elections.

“Putin’s public views of the disclosures suggest the Kremlin and the intelligence services will continue to consider using cyber-enabled disclosure operations because of their belief that these can accomplish Russian goals relatively easily without significant damage to Russian interests,” the report said.

Putin may hold this view because the United States responded to the influence campaign through targeted sanctions. One week before the U.S. intelligence community’s report was released, former U.S. President Barack Obama sanctioned two Russian intelligence services, four individual intelligence service officers, and three companies that provided material support to the Russian intelligence service’s cyber operations.

The U.S. Department of the Treasury also sanctioned two Russian individuals for using cyber-enabled means to misappropriate funds and steal personal identifying information. The U.S. Department of State also shut down two Russian compounds in Maryland and New York that were used by Russia for intelligence purposes, and declared 35 Russian intelligence operatives “persona non-grata.”

“These actions are not the sum total of our response to Russia’s aggressive activities,” Obama said in a statement. “We will continue to take a variety of actions at a time and place of our choosing, some of which will not be publicized.”

While some experts are not surprised by Russia’s actions, one expert has said he was surprised at Russia’s willingness to engage in a disruptive cyberattack against U.S. institutions.

Adam Segal, Ira A. Lipman chair in emerging technologies and national security and director of the Digital and Cyberspace Policy Program at the Council on Foreign Relations, published The Hacked World Order at the beginning of 2016, saying that he thought states on the periphery—Estonia, Georgia, and Ukraine—would conduct disruptive attacks on each other, but that major nation-states would not.

“Clearly, I underestimated the willingness of Russia to use disruptive attacks on the United States,” Segal said at an event hosted by the American Bar Association in January. “I never considered disruptive attacks on the United States focused on institutions, even though I thought those might be the most vulnerable to attacks in the future.”

Disruptive attacks, like the Russian influence campaign, will be a difficult area for the Trump administration moving forward, especially based on the U.S. response to the activity.

Segal, who had just returned from China before speaking at the event, said that the Chinese “seem to see no deterrent value” in the U.S. response to Russia and that the response needed to be stronger to send a clear message not just to Russia, but to other adversaries who might try something similar.

That message was further muddled when just weeks into Trump’s presidency, the U.S. Department of the Treasury eased sanctions to end a ban on selling information technology products to Russia. The ban was originally put in place by Obama in 2015 in response to alleged “malicious cyber-enabled activities” by Russia’s security service in the U.S. electoral process.

Despite the deficient response to the disruptive attack, however, Segal said he still thinks that Russia and China are unlikely to use destructive cyberattacks against the United States—such as targeting critical infrastructure and causing damage—unless their national interests are threatened.

“The Chinese definition of core interests is unfortunately expanding,” Segal said. “But the Chinese know that the United States is going to attribute an attack to them, so they have to be ready for escalation.”

An escalation of destructive cyberattacks is something Leo Taddeo, former special agent in charge of the FBI’s New York Cybercrime Office and current CSO of Cryptzone, says he sees happening in 2017. In an interview with Security Management, Taddeo says he sees nation-states—including the United States—taking a more aggressive position on international
cybersecurity, leading to a cyber escalation between nation-states. The U.S. public has an “appetite for more aggressive cyberactivity” and for “striking back” against those who conduct cyberattacks against American interests, according to Taddeo.

However, Taddeo says he is concerned that the U.S. private sector will be caught in the crossfire of this escalation involving the United States, Russia, China, and possibly Iran, when banks, power companies, and other critical infrastructure—largely controlled by the private sector in the United States—are targeted.

“The Russians don’t have that problem as much as the United States does because Russia is more autocratic,” Taddeo adds. “The private sector there doesn’t complain without permission from the regime and can tolerate more in a crisis.”

Those attack methods are also likely to trickle down to regional conflicts between nation-states with less cyber prowess, such as India and Pakistan. For instance, Taddeo says to look at the attack on the Bank of Bangladesh in 2016 when hackers stole $81 million.

“That type of attack may have been committed by a nation-state to obtain much needed cash resources or to embarrass a smaller state,” Taddeo says. “I think we’ll see more types of cyber conflict...some adopted by nation-states, some by super powers, but with all of these different tools becoming part of the arsenal.”

Taddeo adds that, with today’s technological advances and hacking services for hire, it doesn’t take a great deal of expertise to steal information and share it with organizations like WikiLeaks. Either way, Taddeo says the “genie is out of the bottle” and actors and nation-states are now using cyber methods to conduct influence campaigns for strategic goals.

For the Kremlin, this includes gathering information and attempting to influence public—and government—opinion via social media in favor of Russia. “Immediately after Election Day, we assess Russian intelligence began a spearphishing campaign targeting U.S. government employees and individuals associated with U.S. think tanks and NGOs in national security, defense, and foreign policy fields,” the U.S. intelligence report said. “This campaign could provide material for future influence efforts, as well as foreign intelligence collection on the incoming administration’s goals and plans.”

To read the full U.S. intelligence report, visit SM Online.

SMARTER DESIGN, TIGHTER SECURITY

Optical Turnstiles enhance lobby security and improve pedestrian traffic flow. DSI offers a complete line of products designed to improve access control at entrances to commercial, institutional, educational and government facilities.

OPTICAL TURNSTILE

High Throughput Detects Tailgaters Sleek Architectural Styling

WWW.DSIGO.COM - 800-272-3555

For product info #22 securitymgmt.hotims.com
A study finds the term “shrinkage” outdated and advocates new terminology to better understand and more accurately reflect retail losses.

Redefining LOSS

THE WORLD OF RETAIL has relied on the word “shrinkage” for more than 100 years to describe the losses companies experience as they go about their business. Shrinkage, however, is almost a euphemistic term describing a simple contraction in the size of the stock held by a company, without offering any real sense of what the cause might be.

In this way, the term is similar to “shoplifting”—a rather benign term often used by the industry to describe people actively engaging in criminal acts of theft in stores. For comparison’s sake, you rarely see burglars or robbers described as houselifters or purselifters.

Four buckets of loss tend to be included in survey descriptions of what shrinkage is: external theft, internal theft, administrative or process errors, and vendor fraud. The term “administrative error or process failures” is particularly vague; depending upon the type of retailer and the types of
products sold, it can potentially cover an enormous array of types of loss, including damage, spoilage, product going out of date, and incorrect price adjustments.

A retailer selling food and using a shrinkage definition that includes food spoilage will have a different level of loss compared to a retailer selling clothing or auto parts; yet, many shrinkage surveys continue to combine this data together to generate an overall figure for the industry.

To date, there is no consistent, detailed definition or typology of shrinkage. It is a term that is used throughout the industry, but interpreted in different ways depending on the retail environment and the prevailing organizational culture and practices.

There is a constant desire to understand what the root causes of shrinkage are: Is it mainly external thieves? Is it the staff employed by retailers helping themselves to the stock? Is it due to organizational inefficiencies? Or is it caused by retail suppliers wrongly delivering on purpose or through error?

Surveys will often provide numbers that supposedly apportion the total shrinkage losses to each of these types of losses, with external theft frequently—but not exclusively—seen as causing the largest amount.

The reality is that what these reported shrinkage numbers are actually measuring is what respondents think the causes of shrinkage might be. They are much more a gauge of how the loss prevention industry is feeling than any true measure of the breakdown of losses within the retail industry.

This is because the vast majority of current shrinkage data collected by retailers is based on periodic audit data collected in stores and sometimes in parts of the distribution network. This data captures the difference between the value of stock retailers think they have and the amount that can be physically counted. The difference between the two is how most companies measure their shrinkage.

But all this data does is provide a value of how much stock is not there. What it does not do is offer an explanation as to why it has gone missing: Was the stock delivered to the retailer? Did a customer steal it? Was it damaged or stolen in the supply chain? Did an employee steal it?

The causes could be many and varied, but what is clear is that audit data is rarely good at explaining why discrepancies exist; it simply captures the value of losses where the cause is unknown. Attempts to apportion causes to this data will always involve a high degree of guesswork and personal prejudice.

Retailing has gone through some profound changes since shrinkage was first used back in the 19th century, not least the introduction of open displays, the growth of branding, greater consumer choice, introduction of credit cards and debit cards, the rise of online shopping, and the widespread use of various types of self-service checkout systems, to name a few.

Yet, throughout this time of enormous change, the retail industry has continued to use a term that vaguely captures the difference between expected and actual values as the core measure of loss in their businesses.

Given this, it’s time to reconsider how retail companies understand and measure the losses they experience and to develop a more consistent approach to enable future benchmarking activities to offer more meaningful and applicable information.

For comparison’s sake, you rarely see burglars or robbers described as houselifters or purselifters.
Enterprise-wide integration

ROI acceleration

You call. We answer in person. Every time. 855–WM–SECURE / 855 967 3287

$$$wmssi.com

Enterprise-class security should protect your physical assets and fiscal future. Learn more at wmssi.com.
considerably in how they interpreted the difference, although many made a key distinction between the value of the outcome and how this differentiated costs from losses.

"Costs—they bring value to the business; they are incurred because there is a perceived positive purpose in having them. They are part of the revenue generation process and without them, profits would be negatively impacted," one respondent said.

"Losses are things which, if they didn’t happen, there would be no negative impact upon profitability. They do not offer any real value to the business and simply act as a drain on profitability.”

It was also instructive to hear how some respondents adopted a process of normalizing what some considered to be losses into costs. One respondent explained that “we plan a lot of those costs [possible types of losses], so when we’re looking at it from a planning perspective, we have that built in—anything that we can account for and process and know what it is, we take more so as a cost rather than a loss when we’re defining it.”

Another respondent talked about how the planning and budgeting process enabled many losses to be redefined as costs. “If it goes above budget, then it becomes a loss; otherwise it is a cost,” the individual explained, while another respondent was blunter: “We try and convert as much of [losses] to costs; it’s then not on my agenda anymore. I deal with shrink.”

**Definition.** From the interviews with senior U.S. retail executives and feedback from the roundtables held in Europe, definitions of costs and losses were eventually developed.

Costs were defined as “expenditure on activities and investments that are considered to make some form of...
recognizable contribution to generating current or future retail income.”

Losses were defined as “events and outcomes that negatively impact retail profitability and make no positive, identifiable and intrinsic contribution to generating income.”

Using these definitions, various types of events and activities could then begin to be categorized accordingly.

For example, incidents of customer theft can be considered a loss—the event and outcome play no intrinsic role in generating retail profits—because it makes no identifiable contribution and were it not to happen, the business would only benefit.

Alternatively, incidents of customer compensation, such as providing a disgruntled shopper with a discounted price, can be seen as a cost. In this case, the business is incurring the cost because it believes compensating the aggrieved consumer makes the individual more likely to shop with the business in the future. The policy of compensating is an investment in future profit generation and is categorized as a cost—not a loss.

Another example of a loss is workers’ compensation, where a retailer will cover the legal, medical, and other costs associated with an accident at work, such as falling off a ladder. There is no intrinsic value to the business if an employee is injured at work; if it had not happened, the business would only benefit by not having to pay for the consequences of the event. Therefore, workers’ compensation is a loss.

While some respondents to this research argued that workers’ compensation is a predictable problem that can be—and is—budgeted for, it still remains an event that the retailer would prefer not happen because it negatively impacts overall profitability.

In contrast, expenditure on loss prevention activities and approaches, such as employing security officers or installing tagging systems, can be seen as a cost. The retailer has committed to this expenditure because it feels there will be some form of payback from the investment: lower levels of loss, which in turn will boost profits. Whether this payback is measured or achieved is open to debate.

What these examples focus on is not whether an activity or event can be controlled or whether the incurred cost was planned, but its fundamental role in generating current or future retail income. If a clearly identifiable link can be made between an activity and the generation of retail income, then it should be regarded as a cost; all those activities and events where no link can be found should be viewed as a loss.

Categorizing losses. In developing the categories of the Total Retail Loss Typology, it was important to draw a
distinction between the types of loss that can be measured in a way that is manageable for modern retail business, and those that cannot.

Additionally, it was important to consider the value of collecting data on a given loss indicator. Is it meaningful for the business to monitor a category of loss? Will its analysis offer potentially actionable outcomes that may help the business meet its objectives?

There is little point in developing a typology made up of a series of categories that are either impossible or implausibly difficult to measure or once measured offer little benefit to the business undertaking the exercise.

For example, most retailers would be keen to understand how often items are not scanned at a checkout. While it is theoretically possible to measure this, the reality for most retailers is that the ongoing cost would probably be prohibitive.

Determining whether proposed loss categories met the three M’s test (manageable, measurable, and meaningful) was an important part of creating a typology likely to achieve any form of adoption across a broad range of retail formats.

Typology. The research identified 31 types of known loss that are included in the Total Retail Loss Typology covering a wide range of losses across the retail enterprise and incorporating events and outcomes beyond just the loss of merchandise. The typology is broken down into four locations of loss: store, retail supply chain, e-commerce, and corporate. Each location then has a variety of subcategories divided between malicious and nonmalicious.

For example, a malicious corporate retail loss would be fraud; a nonmalicious corporate retail loss would be workers’ compensation, regulatory fines, or bad debt. (See chart, page 38.)

However, the term does not encompass every form of loss that a retailer could conceivably experience. The word “total” is being used in this context to represent a much broader and more detailed interpretation of what can be regarded as a retail loss, rather than necessarily claiming to reflect the entirety of events and activities that could constitute a loss. In the future, the scope and range of the Total Retail Loss Typology will change to accommodate new forms of loss, and this is welcomed.

The typology is designed to enable the calculation of the value of retail losses, not necessarily the number of events; where an associated value cannot be calculated or there is no loss of value associated with an incident, it should not be included.

For instance, if shop thieves are apprehended leaving a retail store and the goods they were attempting to steal are successfully recovered and can be sold at full value at a later date, there is no financial loss associated with the incident. The retailer may still want to record that the attempted theft took place and was successfully dealt with, but that it would not be recorded in the Total Retail Loss Typology.

Potential

The proposed Total Retail Loss Typology is a radical departure from how most retail companies have understood and defined the problem of loss within their companies, moving away from a definition focused primarily on unknown stock loss to one that encompasses a broader range of risks across a wider spectrum of locations.

While there is a simple elegance about the approach adopted in the past, based upon the four traditional buckets of shrinkage, it is increasingly recognized that these broad brush and ambiguously defined categories are no longer capable of accurately capturing the increasingly complex risk picture now found in modern retailing. Instead, the Total Retail Loss Typology has the potential to benefit retail organizations by managing complexity, encouraging transparency, creating opportunities, and maximizing loss prevention.

Managing complexity. The retail landscape in which shrinkage was first described has been transformed by innovation and change. Simply relying upon the traditional four buckets of estimated losses to fully reflect and properly convey the scale, nature, and impact of retail losses is no longer
appropriate, particularly as the retail environment becomes more dynamic and fast changing.

**Encouraging transparency.** The ambiguous nature of most shrinkage calculations and the difficulty of understanding its root causes generate a lack of accountability, particularly within retail stores.

Store managers question the reliability of the number, especially where there is a pervasive sense that the supply chain may be foisting losses upon stores that are actually caused by inefficiencies. Unknown store losses can conveniently be blamed upon short shipments or roaming bands of organized thieves, rather than being apportioned to actual events taking place in the store.

Losses can also be moved between different categories, depending upon the performance measures in place—wastage can quickly become shrinkage if the former is identified as a key performance indicator.

By measuring a broader range of categories of loss, it becomes much more difficult to play this game; most losses will be measured somewhere, improving transparency and accountability throughout the organization.

**Creating opportunities.** A recurring theme from the research was the lack of prioritization and urgency associated with categories of loss that had already been measured or for which a budget had been allocated.

Many respondents were quick to view these factors as a cost; therefore, not requiring any remedial action by the business. In effect, the process of capturing the loss or planning for it through budget allocation rendered them immune from concern over the actual loss.

By adopting a systematic approach and agreeing on the definition of a retail loss and bringing these together under a single typology, opportunities may arise to minimize the overall impact of loss upon the business.

**Maximizing loss prevention.** Dealing with an unknown loss, which is what most loss prevention practitioners typically focus on, is probably one of the hardest challenges faced by a management team in retail. This requires the team to develop a
high level of analytical and problem solving capacity. Trying to solve problems where the cause is typically unknown is also at the hard end of the management spectrum. It requires creative thinking, imaginative use of data, and considerable experience. Imagine if these capabilities were used on the broader range of known problems encapsulated in the Total Retail Loss Typology. The impact could be profound. **Using resources.** By generating a broader, more detailed understanding of how losses are impacting a retail organization, it may be possible to take a more strategic approach to the allocation and use of existing resources. The Total Retail Loss Typology could offer value in how businesses not only respond to existing loss-related challenges, but also use it to review the implication of any future business decisions. The interplay between sales and losses needs to be viewed in the round and not as a series of cross-functional trade-offs where losses and profits are allocated separately, driving behaviors that are unlikely to benefit the business. It’s within this context that the Total Retail Loss Typology has been developed—to enable retail organizations to better understand the nature, scale, and extent of losses across the entire business, and to use this information to make more informed choices about how to grow profits and improve customer satisfaction. As the pace of change in retail continues to intensify, it’s time for the loss prevention industry to begin to move away from a notion of loss developed in the 19th century to one that better reflects and recognizes the complexities and challenges found in the 21st century.

**ADRIAN BECK** is a Professor of Criminology in the Department of Criminology at the University of Leicester in Leicester, United Kingdom. Beck undertook the study Beyond Shrinkage: Introducing Total Retail Loss Commissioned by the Retail Industry Leaders Association’s Asset Protection Leaders Council and is an academic advisor to the ECR Community Shrinkage and On-Shelf Availability Group.
Altronix’s new NetWay Spectrum series takes fiber and power to a new level. Indoor and outdoor models include hardened Ethernet PoE switches and multi-port media converters with or without integral power. Units can be deployed with conventional single or multi-mode fiber...or composite cable which combines fiber with copper to simultaneously deliver power and data. Go further with NetWay Spectrum from Altronix.

VISIT US AT ISC WEST – BOOTH # 11073
Surveillance and Stereotypes

Through original research, these authors found that criminal stereotypes impact the surveillance and sanctions of juvenile shoplifters.

Juveniles make up 40 percent of the shoplifters in the United States. Shoplifters, in total, contribute to billions of dollars of loss each year, according to the National Association for Shoplifting Prevention’s 2014 report *Shoplifting Statistics*. To combat adolescent shoplifting, according to the report, retailers depend on private security officers combined with other security measures, including security cameras, observation mirrors, and radio-frequency identification (RFID) tags.

The key to apprehending juveniles during or after shoplifting, however, is to correctly determine whom to surveil. Security personnel often rely on a combination of common underlying physical characteristics—race, gender, and age—and behavioral indices—glancing at clerks nervously, assessing security measures, and loitering—to distinguish shoppers from potential shoplifters.

Are these surveillance decisions a result of bias? To find out, the authors conducted original academic research funded by the John Jay College of Criminal Justice of the City University of New York on how stereotypes play into who is suspected of shoplifting, how that suspect is dealt with, and what private security can do to limit discriminatory practices.
EXISTING DATA
A 2003 *Journal of Experimental Psychology* article, “The Influence of Schemas, Stimulus Ambiguity, and Interview Schedule on Eyewitness Memory Over Time,” which discussed research findings and lawsuits against retailers, concluded that stereotypes of juvenile shoplifters may unduly influence security officers to target juveniles on the basis of their physical characteristics, rather than their behaviors.

Over the past 20 years, the media has reported on cases in which the retail industry engaged in discriminatory practices. This is known as consumer racial profiling (CRP), “the use of race and or ethnicity to profile customers.” According to a 2011 study in the *Criminal Justice Review*, “Public Opinion on the Use of Consumer Racial Profiling to Identify Shoplifters: An Exploratory Study,” officers sometimes use CRP to determine which juvenile shoppers are potential or actual thieves.

Most people develop negative stereotypes about juvenile thieves through exposure to various types of media, particularly when they reside in areas that contain few minorities. The media has the unique ability to both shape and perpetuate society’s beliefs about which juveniles typically commit offenses through its selective coverage of crimes.

It is also common for the media to portray adolescents—particularly boys—as criminals. Biases are then used, whether consciously or unconsciously, in the private sector by retailers and security officers to target shoppers, and in the public sector by those in the legal system, including law enforcement officers, prosecutors, judges, and even legislators, to arrest and prosecute thieves.

The consequences of applying discriminatory practices can be seen in the private sector through lawsuits against retailers. Ethnic minority shoppers purport that they were targeted through excessive surveillance—and even through false arrests.

Researchers have shown that this automated bias occurs even when observers were trained to focus on behavioral cues, and it persists despite findings that shoplifting occurs across racial and ethnic groups, according to the 2004 *Justice Quarterly* article “Who Actually Steals? A Study of Covertly Observed Shoplifters.”

Stereotypes also affect retailers’ decisions on how to handle shoplifters, either formally by involving the police, or informally. The results of accumulated discrimination, accrued during each step in the legal process—initial involvement of police, decision to prosecute, conviction, and
sentencing—continue in the legal system. This is evidenced by the disproportionate number of African- and Latin-American boys shown in the apprehension and arrest statistics of juvenile thieves, compared to their representation in the population, according to Our Children, Their Children: Confronting Racial and Ethnic Differences in American Juvenile Justice, a book published by the Chicago University Press.

CURRENT RESEARCH
To test the premise that there is a widespread stereotype of the typical juvenile thief and shoplifter, our research team obtained information from young adults in two diverse areas: 97 psychology-major college students in a small city in the U.S. state of Kansas, and 156 security and emergency management majors at a college in a large city in New York state.

**Shoplifter profile.** The psychology-major students were 83 percent European American. The rest of the students were represented as follows: 5 percent African American, 2 percent Asian American, 1 percent Latin American, and 9 percent of mixed or unknown descent.

The security and emergency management major students—72 percent of whom were male—came from a variety of backgrounds: 31 percent European American, 37 percent Latin American, 19 percent African American, 9 percent Asian American, and 2 percent Middle Eastern American.

Participants in both locations were asked to guess the common physical characteristics of a typical juvenile shoplifter—age, gender, ethnicity or race, and socioeconomic status.

The stereotypical juvenile shoplifters described by both the Kansas and New York respondents were remarkably similar: male, aged 14 to 17, and from lower- to middle-class families of African-American, Latin-American, or European-American descent. The two samples also indicated that the stereotypical thief was likely to have short or medium length brown or black hair and an identifying mark—such as a piercing.

These findings show commonality in the prevalence of certain physical characteristics, despite the diversity of the two groups of respondents, and demonstrate that American society has a well-developed juvenile shoplifter stereotype.

**Decision processes.** After determining the stereotype, the research team considered whether juvenile shoplifter stereotypes affected respondents’ decisions. The goal was to determine the degree to which the respondents believed that physical characteristics influenced the security guards’ decisions regarding whom to surveil, and what consequences to apply when a youth was caught stealing.

The New York respondents read a brief scenario describing a juvenile shoplifter as either male or female and from one of five backgrounds: European American, African American, Asian American, Latin American, or Middle Eastern American. However, the description of the overt behaviors by the juvenile was the same for every scenario—selecting and returning shirts in a rack, glancing around the store, and stuffing a shirt into a backpack.

Respondents provided their opinions about the degree to which the security officer in the scenario relied on physical characteristics in surveilling a juvenile, and whether the retail manager and security officer should impose informal or formal sanctions on the shoplifter. Researchers reasoned that respondents should draw identical conclusions for surveillance and sanctions if they were simply evaluating the juvenile shoplifters’ behaviors, but that students would have different recommendations for these choices if their racial or ethnic stereotypes were activated.

Respondents who indicated a preference for applying informal sanctions did so more frequently for girls of African-American and Middle Eastern-American descent. These respondents also assessed that the officer described in the scenario based his or her surveillance decisions on physical characteristics. No other gender differences for race or ethnicity were notable when considering reliance on physical characteristics.

Stereotypes also affected decisions on how to sanction the shoplifter. Respondents were given the option of implementing one of four informal sanctions: speak to the juvenile, call parents to pick up the juvenile, get restitution, or ban the youth from the store. Their selection of the least severe sanction—talk to

![Retail Theft | By Lauren R. Shapiro and Marie-Helen Maras](Image 459x734 to 494x771)
the juvenile—was doled out at a higher rate for boys than for girls of each ethnicity except European Americans, which did not differ.

The moderate level sanction—call the youth’s parents—was selected more for girls than for boys of African and Latin descent. The most severe level sanction—ban the youth from the store—was selected more for boys than for girls of African descent. However, it was selected more for girls than for boys of Asian, European, and Middle Eastern descent.

Respondents who indicated a preference for applying formal sanctions attributed physical characteristics to the guards’ surveillance decision for girls more than for boys of Latin descent; gender differences were not apparent for the other ethnicities.

Respondents were also given five formal sanctions for the youths: involve the police, prosecute the theft as larceny, impose a fine, give the youth diversion or community service, or put the incident on the youth’s criminal record. Their selection of the least severe sanction—involves the police—was endorsed more for boys than for girls of Asian, European, and Latin descent, but more for girls than for boys of African descent. No gender difference was apparent for youths of Middle Eastern descent.

The most severe sanction—diversion or community service—was preferred more for boys than for girls of African descent. A small percentage of respondents endorsed a criminal record for the theft of a shirt, but only for girls of African and European descent and for boys of Middle Eastern descent.

Finally, a comparison of our data revealed that respondents believed informal—rather than formal—consequences should be imposed for girls rather than for boys of Asian and European descent, and for boys rather than for girls of Latin descent.

LESSONS LEARNED
Our findings clearly demonstrate that people have stereotypes about juvenile shoplifters. They also showed that people unconsciously use the typical physical characteristics of gender and race or ethnicity associated with their criminal stereotypes to make decisions and recommendations, such as whom to surveil and how to handle a shoplifting incident. Otherwise, there would not have been a difference in how the juvenile shoplifter was processed or punished, because the behaviors exhibited by all of the juveniles were identical across scenarios.

Consumer racial profiling is a defective filtering system that may direct private security officers’ attention to characteristics that are not reflective of actual shoplifting conduct. Our data suggests
that CRP not only hurts retail businesses by discouraging minority consumers from shopping in their stores, but also simultaneously prevents security officers from apprehending shoplifters.

Other research, such as from “Juvenile Shoplifting Delinquency: Findings from an Austrian Study” published in the 2014 *Journal for Police Science and Practice,* shows that only 10 percent of juveniles are caught shoplifting. Even more disconcerting, the typical shoplifter steals on average 48 to 150 times before being apprehended. Clearly, retailers need a better strategy if they are to reduce loss due to shoplifting.

Another issue that was addressed was the decision to involve the legal system. Many businesses, despite having posted prosecution warnings, reported only about half of the adolescent shoplifters they caught to the police. Retailers instead focus on minimizing loss and negative publicity, and may rationalize against reporting the offense to the police because they do not want to stigmatize the adolescent or because they consider it a one-time incident, particularly when the juvenile admits to the theft and then pays for or returns the items, according to the U.S. Department of Justice’s (DOJ) Community Oriented Policing Services.

These beliefs, however, may be misguided. Though current research is scarce, a 1992 study—*The Sociology of Shoplifting: Boosters and Snitches Today*—indicated that 40 to 50 percent of apprehended adolescent shoplifters reported that they continued shoplifting.

There are benefits for retailers who involve the legal system, especially for informal police sanctions. First, criminal justice diversion programs and psychological treatment and educational programs treatment may reduce recidivism. For example, shoplifters who attended and completed a diversion program had significantly fewer re-arrests compared to those who failed to complete or did not attend, a DOJ study found.

Second, the private sector needs the support of the public sector to reduce shoplifting. Shoplifters can be given an opportunity to participate in first offender programs and, upon completion of classes on the effects of shoplifting, have their charges dismissed or even erased.

**RECOMMENDATIONS**

Retailers and private security officers need training to make them aware of their own biases and how their stereotypes affect their choices. They also need training to learn which behavioral indices are most effective in distinguishing shoppers from shoplifters.

If retailers do not make significant changes in guiding their employees—particularly security officers—towards objective measures of vigilance to prevent
INFORMAL SANCTIONS: CALL PARENTS

Researchers asked participants if they would call the suspects’ parents in shoplifting incidents involving juveniles of different races, ethnicities, and genders. Responses varied widely.

<table>
<thead>
<tr>
<th>Race/Ethnicity</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>African</td>
<td>63%</td>
</tr>
<tr>
<td>Asian</td>
<td>54%</td>
</tr>
<tr>
<td>European</td>
<td>50%</td>
</tr>
<tr>
<td>Latin</td>
<td>33%</td>
</tr>
<tr>
<td>Middle Eastern</td>
<td>25%</td>
</tr>
</tbody>
</table>

SOURCE: Impact of Criminal Stereotypes on Surveillance and Sanctions of Juvenile Shoplifters, Lauren R. Shapiro and Marie-Helen Maras

shoplifting, their financial loss will continue to be in the billions of dollars.

Private security officers must be taught how to treat all potential shoplifters, regardless of their gender, in the same way to prevent making mistakes and subjecting retailers to lawsuits for discriminatory security practices.

Overcoming unconscious biases is difficult. Prior to specialized training in bias identification and behavioral profiling, it is important to determine the biases of security officers. Self-assessment measures similar to the ones the researchers used in their study can be administered.

The officers should also keep records that specify each incident of shoplifting, what behaviors drew their attention to warrant surveillance, what act occurred to provoke them to approach the juvenile shoplifter, the items that were taken, the method used, the shoplifter’s demographics, how the situation was handled, who made the decision, and reasons for the decision. The officers should then review these records with their retail managers.

Retailers should also implement a mandatory training program to provide private security officers with the tools needed to identify shoplifting behaviors to increase detection and reduce shrink.

The incident records could be introduced and used to help identify the impact biases have on private security professionals’ decisionmaking about juvenile shoplifters. It would also help security guards learn the various types of suspicious behaviors that shoplifters exhibit, such as juveniles who make quick glances at staff, examine items in remote aisles, monitor security cameras and mirrors, and purposefully draw employees’ attention away from others.

Additionally, a practical component would be to show surveillance videos of the behaviors exhibited by juvenile shoplifters of different gender and race or ethnicity. In this way, the findings of past studies showing the insignificance of race, ethnicity, or gender can be learned through real-world examples.

DR. LAUREN R. SHAPIRO IS AN ASSOCIATE PROFESSOR IN THE DEPARTMENT OF SECURITY, FIRE, AND EMERGENCY MANAGEMENT AT JOHN JAY COLLEGE OF CRIMINAL JUSTICE. SHE HAS PUBLISHED SEVERAL JOURNAL ARTICLES AND CHAPTERS ON THE ROLE OF STEREOTYPES IN PERCEPTION AND MEMORY FOR CRIME AND CRIMINALS. DR. MARIE-HELEN (MARIA) MARAS IS AN ASSOCIATE PROFESSOR AT THE DEPARTMENT OF SECURITY, FIRE, AND EMERGENCY MANAGEMENT AT JOHN JAY COLLEGE OF CRIMINAL JUSTICE. SHE IS THE AUTHOR OF SEVERAL BOOKS, INCLUDING CYBERCRIMINOLOGY; COMPUTER FORENSICS: CYBERCRIMINALS, LAWS, AND EVIDENCE; COUNTERTERRORISM; AND TRANSNATIONAL SECURITY.
Low employee engagement is a widespread challenge. But there’s a host of best practices security managers—and organizations—can employ to address the issue.

Each day, pollsters at the Gallup company monitor the upicks and downticks of America’s pulse. They track large-scale indicators like the country’s unemployment rate, the citizenry’s economic confidence, and the president’s approval rating. But among these tracked statistics at Gallup.com Daily lies a less publicized marker: what percentage of U.S. workers say they are engaged at their jobs? For managers, the answer may be discouraging: only about one-third of American workers are engaged on the job, Gallup now finds. The employee engagement rate has stayed in that low range for the last 15 years—from 26 percent (on a yearly average basis) in 2000 to 33 percent in 2016, according to Jim Harter, chief scientist of Gallup’s international workplace management and well-being practices. Actively disengaged employees cost the United States $450 billion to $550 billion per year, according to Gallup’s research. Employee disengagement can increase turnover, pollute office culture, and lead to more mistakes in the workplace—the last of which can be dangerous in the security industry, where oversights and errors can result in damaging breaches.

Conversely, Gallup researchers found that organizations that successfully sustain high employee engagement reap serious benefits. On average, profitability is 22 percent higher; productivity, 21 percent higher; absenteeism, 37 percent lower; and there are 48 percent fewer staff safety incidents.

Moreover, experts say there are many best practices that organizations and managers can follow to maximize employee engagement. From strength building to safe-space dialogue to stronger mission connection, a security manager’s approach and an organization’s leadership can make all the difference.

Energy and Flow

Employee engagement is not a new workplace concept; it has been discussed and studied for more than 25 years. But with more and more recent research illustrating its benefits, and the hazards
of disengagement, the concept of employee engagement is now “much more integrated into how we look at work,” says management expert David Zinger, a Canada-based consultant who runs The Employee Engagement Network, an online resource.

Zinger and other experts argue that Gallup’s methodology (a 12-question survey that poses core value questions such as “at work, do I have the opportunity to do what I do best every day”), leads to exceedingly low engagement scores. Other methodologies put the U.S. employee engagement rate at about 50 percent, these experts say. Still, almost all agree that whatever metric is used, the rate is still too low.

By definition, employees who are engaged are usually involved in and enthusiastic about their work, and are making valuable contributions to their organization. Bob Kelleher, an expert who runs The Employee Engagement Group consultancy, says he thinks of engagement as a successful partnership between an employer and employee. “The employer is helping the employee reach his or her potential, while the employee is helping the employer reach its potential,” he explains. “It’s the ultimate win–win. The byproduct is this partnership is a discretionary effort.”

And that discretionary effort from the employee often comes naturally, because of the positive energy generated by simply being engaged.

“When an employee is engaged, they experience a state of flow. They are energized. They are learning. They have fun,” says Pi Wen Looi, a workplace expert who heads the Novacrea consulting firm. “As a result, they are more likely to recommend their company as a great place to work, stay longer with the company, and go above and beyond their role.”

How Organizations Prompt Different Levels of Engagement

GEORGE BRADT, management expert and leadership columnist for Forbes magazine, divides the engagement continuum into four levels: disengaged, compliance engagement, contributing engagement, and committed engagement.

Most organizations, he argues, get the level of employee engagement that they deserve—they provoke it by the way they treat employees.

How can an organization prompt disengagement? Bradt offers the following example. In the current U.S. workplace, reorganizations are very common. Often under an “evolve or die” ethos, companies feel they need to change to compete more successfully. These reorganizations can include various types of changes, including layoffs, amended job responsibilities, rearranged chains of commands, expanded or streamlined work processes, and altered goals and objectives.

However, these changes often leave employees confused and uncertain. “Then [company leaders] are surprised when people start becoming disengaged,” he says with a laugh. This disengagement often leads to more turnover. “People don’t know what they are supposed to be doing,” he explains. “So they find happiness elsewhere.”

The next level up is compliance engagement. In this state, employees stay engaged with their work just enough to fulfill their responsibilities and keep their jobs. For some organizations, this level of engagement works; the U.S. Navy and Air Force often operate along these lines, because both have strict command-and-control structures in which people are prompted to do exactly as ordered.

Natural Selection

Managers play a crucial role in maximizing employee engagement in the workplace—and that management effort should start with the hiring process, experts say.

Looi mentions recent research she was involved in that was aimed at identifying employees’ sense of purpose to help them find jobs that were in tune with their personal values. The research showed how an employee-employer values alignment at the start led to greater engagement.

“If you want to have engaged employees, you’ll need to make sure you are recruiting the right talent—a passion and value match, a culture fit, and with the right skills,” she says.

In part, that’s because high salaries are ultimately not enough to ensure high engagement, she adds. “What motivates employees comes from their own heart. You may have market competitive pay and benefits, but these extrinsic motivators are not sufficient to propel employees forward,” she explains. “It’s the intrinsic motivators such as pursuing their values and passion, continual learning, and building
good relationships with peers that will keep a person going and thriving.”

Kelleher illustrates this by using the acronym BEST. Employers tend to hire for the middle two letters, education (E) and skills (S), in hopes that they will be the most reflective of performance. But it is the first and last letters, behaviors (B) and traits (T), that best reflect employees’ values.

Since a values alignment is key to engagement, employers should also focus on behaviors and traits in the hiring process. Sometimes, disengagement is the result of the fact that the values of the company and the employee were never a match. “I often tell clients, ‘You don’t have an engagement issue, you have a selection issue,’” Kelleher says.

The importance of the hiring and selection process also applies to managers, Gallup’s Harter says. Many who become managers don’t yet have the skills and training to be effective.

“A lot of people are put into the role because they are successful in a previous position, but that position was not a managerial one,” he says. “Or, they are selected because they have been around a long time in the organization, so it becomes a rite of passage.”

Indeed, based on his decades-long study of engagement and the U.S. workplace, Harter says that sound manager selection is one of the three most effective ways an organization can increase engagement. The other two ways are managerial practices—a focus on building employee strengths, and a sustained two-way coaching dialogue between managers and employees.

These last two ways are effective in part because they are being driven from below, Harter explains. Newer workers, the 20- and early 30-somethings who are members of the millennial generation, “want a coach type of manager who focuses on strength-based development, as opposed to a manager who is an expert in their weaknesses,” he says.

In a strengths-based workplace culture, employees often learn their roles more quickly, produce better work, and are more engaged, he adds.

In its own recent research, Gallup found that 67 percent of employees who say that their manager focuses on their strengths are engaged, compared with only 31 percent of the employees who say that their manager focuses on their weaknesses.

**Continual Conversation**

Besides a strength-based approach, younger workers are also asking for a managerial approach that does not focus on a once-a-year performance review, but features a continuous two-way conversation in a coaching manner, Harter says.

Other experts agree. Zinger, who consults on employee engagement around the world, says that one commonality he has noticed is that employees in virtually every country want their managers to care about them. Kelleher also stresses this.

“Empathy is a significant leadership competency—especially in 2017,”
Kelleher says, “Employees who think their employers care about them as people are more likely to give above and beyond.” A 2016 Gallup report, *What Great Managers Do to Engage Employees*, drew the same conclusion.

“A productive workplace is one in which people feel safe...enough to experiment, to challenge, to share information, and to support one another,” the study finds. “In this type of workplace, team members are prepared to give the manager and their organization the benefit of the doubt. But none of this can happen if employees do not feel cared about.”

This feeling of being cared about is built through regular conversation, during which the manager learns about the values, goals, and passions of the employee.

“Conversations are in many ways the lifeblood of the organization,” Zinger says. But they do not have to take up hours and hours every week. Some days, brief check-ins are fine, and help maintain engagement.

“Some managers may think, ‘Oh my gosh, I have so much on my plate. Now you want me to have these conversations?’ But it can be as quick as 45 seconds,” Zinger explains. Even a short text or email can be productive, he adds.

Gallup’s *Great Managers* study confirmed this link. It found that consistent communication—whether it occurs in person, over the phone, or electronically—is linked to higher engagement. Employees who have regular meetings with their managers are almost three times as likely to be engaged, compared with workers who don’t, the report found.

Moreover, these conversations are a good opportunity for managers to draw attention to employees’ accomplishments. Here, Kelleher’s advice to managers is simple: “Recognize, recognize, and recognize.”

“Recognition is a significant engagement driver. It is almost always free, has lasting impact, and managers tend to see a replication of the positive results that they are looking to recognize,” he says. “There is simply no downside.”

In addition to conversation, a manager’s behavior is also important because it can have a mirroring effect, Zinger says. Based on that behavior, it’s easy for employees to see how connected a manager is to his or her own work, and the organization at large. A manager who encourages engagement, but is cynical or uncaring in his or her own work relationship will be quickly seen as inauthentic.

And the mirroring effect can work both ways, he adds. Let’s say a security manager has a staff of 10, and two of the 10 workers seem disengaged. Out of frustration, the manager may start avoiding and minimizing his or her conversations and interactions with them. In effect, the manager is following the employee’s lead; from the employee’s point of view, the manager is becoming disengaged.

Finally, Kelleher advises managers to establish what he calls “a line of sight” between an employee’s work and the mission of the organization. To do this, managers need to explain where the company is going and its vision for the future; the strategy for how the company intends to get there; and how the employee’s work is a part of that.
“Line of sight is critically important to engagement. Employees should not be working in a vacuum,” he explains.

What Organizations Can Do
Managers are not the only ones who influence employee engagement. Organizations as a whole, through both their policies and executive leadership, can also have a significant effect, experts say.

For example, a company may want to consider reworking its performance review process so that engagement is discussed during reviews. These should be two-way, safe-space conversations, in which employees are comfortable talking about when they feel disengaged, for what reasons, and what could be done differently.

“Frame performance conversations as a way to look forward and help employees grow, not as a backward-looking, punitive means,” Looi says.

Some organizations may even want to consider replacing annual performance reviews with robust monthly check-in conversations that focus on the development of the employee.

“Get rid of the intimidating phrase ‘performance appraisals’ and replace it with a new forward-looking phrase—the employee development planning process,” Kelleher says.

The organization’s executive leadership, not just middle managers and human resources staff, should also be focused on engagement. Successful companies, experts say, are often proactive on engagement; their leaders are focused on making their firm more attractive in the eyes of the employees, so that more workers will be committed to their jobs.

Some of these successful companies conduct informal stay interviews with staff. Instead of an exit interview, in which managers try to find out why employees are leaving, managers conducting stay interviews try to find out what it would take for an employee to stay.

The Future Is Now
While Gallup’s U.S. engagement rate has been at or below 33 percent for most of the last 15 years, some experts do see signs that employment engagement may improve in upcoming years.

Looi points to research advances in behavior economics and nudge theory, which can be used to improve workplace cultures so that greater engagement is inherently encouraged.

“When applied appropriately and ethically, you can use nudges to increase employee learning, performance, and engagement,” she says.

(For more details on nudge theory see “Management Trends,” by Sean Benson, CPP, in the September 2016 issue of Security Management.)

Zinger explains that Fitbit-like devices that measure engagement, by way of physical indicators that signal when employees are holding their phones or sitting in a chair, may become more commonplace.

And Harter, who describes himself as “hopeful,” sees new workers continuing to transform the U.S. workplace. The millennial generation, which has been driving an increased focus on engagement, will make up three-quarters of the nation’s workforce in just over a decade, according to demographic projections. This generation is keen on being engaged with work that has a purpose, and that is a positive reflection on their values. Studies show, for example, that recent MBAs with high earning power will work for a significantly lower salary if they truly believe in their jobs.

“There’s not as much separation between work and life. People want their work to be representations of who they are,” Harter says.

10th Annual CSO Summit
The premier event for senior security executives.

23-25 April 2017 | WASHINGTON • DC

www.csocenter.org/summit

CONTACT SENIOR EDITOR MARK TARALLO AT MARK.TARALLO@ASISONLINE.ORG. CONNECT WITH HIM ON LINKEDIN.
The bustling Brussels Airport in Zaventem, Belgium, handles more than 500 flights a day, bringing more than 27,000 passengers into the facility with approximately the same number departing. Mornings are particularly busy at the airport, and amid the flurry of activity, it is little wonder that on March 22, 2016, three men emerging from a taxi outside of the departures hall passed through unnoticed.

The trio loaded their heavy suitcases onto baggage carts and entered the flow of people heading through the doors toward the ticket desks. Shortly after they entered the departures hall, the three split up to take their places in separate ticket lines.

Three minutes later, one of the men detonated his suitcase bomb, which had been packed with nails, as he stood in one of the check-in lanes. Approximately nine seconds after that, the second man detonated his suitcase bomb in another lane. The third suitcase bomb did not detonate immediately; surveillance camera footage showed that after being thrown to the ground by the second blast, the third man, Mohamed Abrini, simply got up and walked away from the airport toward the city center.

It is unknown whether he left because he got cold feet or because his device failed to detonate, but he was later arrested and charged with participation in the attack. Police bomb technicians destroyed Abrini’s bomb-filled suitcase, which they report may have been the largest of the three, in a controlled explosion.

The attack at Zaventem resulted in 17 deaths. Another 14 victims were killed when a fourth suicide bomb was detonated an hour later in a subway train at the Maalbeek metro station in Brussels. The coordinated attack was the deadliest in Belgian history. It was also a lethal reminder of the continuing threat to the soft parts of airports outside security checkpoints.

THE EVOLUTION OF AIRPORT ATTACKS

Terrorists have been targeting airports since the 1960s in a continual game of cat-and-mouse with security professionals.
EVOLVING TACTICS

The air transit system has been considered a prime target since the beginning of the modern era of terrorism. From a terrorist’s perspective, hundreds of people trapped inside a pressurized metal tube at 30,000 feet are ideal targets not only because the victims are so vulnerable, but because of the heavy media coverage such attacks generate.

For example, the photos of TWA 847 pilot John Testrake in the plane’s cockpit window being held at gunpoint by a Hezbollah hijacker became some of the most iconic images of 1980s terrorism. Terrorist threats to aircraft spurred a series of security improvements, which were in turn answered by changes in terrorist weapons and tactics. The evolutionary—and deadly—game of cat-and-mouse between terrorist planners and aviation security officials has been occurring since the 1960s.

Initially there was very little security provided to the air transportation system, but a sharp increase in commercial airline hijackings in the 1960s and early 1970s led to enhanced airline security in the United States and Europe. High-profile hijackings led to greater and more widespread improvements to aviation security worldwide.

As hijackings became more difficult to conduct, terrorists began to direct their attention to aircraft bombings. Palestinian bombmakers created plastic explosives to look like everyday items in increasingly elaborate efforts to bring them onto aircraft undetected. The result was a number of airline bombing plots in the 1980s using concealed devices.

In 1987, North Korean agents destroyed a plane using a device hidden inside a radio to set off liquid explosives hidden in a liquor bottle. In another incident in 1986, explosives and the detonating device were hidden in a suitcase under a false bottom and a pocket calculator. Security detected the device before it could be taken aboard the plane.

Perhaps the most famous of these bombings was Pan Am Flight 103 in 1988, when a bomb hidden in a suitcase detonated on board, killing all 259 on board and 11 people on the ground.

A BRIEF HISTORY OF TERRORIST ATTACKS ON THE AIRLINE INDUSTRY

- 1961: The first attempted ‘skyjacking’ of an airline on American soil
- 1969: The longest hijacking in history thus far, covering 6,900 miles, by a 19-year-old U.S. Marine
- 1985: TWA Flight 847 hijacked for more than two weeks by members of Hezbollah and Islamic Jihad
- 1988: A timed bomb hidden in a suitcase detonated on Pan Am Flight 103, killing all 259 on board and 11 people on the ground
- 1994: Philippine Airlines Flight 434 was damaged by a bomb assembled on the plane from separate components and left on board
- 2001: Four U.S. planes were hijacked and turned into human-guided cruise missiles to attack New York City and Washington, D.C.
- 2011: A suicide bombing in the international arrival hall of Moscow’s Domodedovo International Airport killed 37 people
- 2016: Three coordinated suicide bombings took place in Belgium at the Brussels Airport and Maalbeek metro station, killing 32 people
1988, a bombing that killed 243 passengers, including two of my colleagues, U.S. Diplomatic Security Service Special Agents Dan O’Connor and Ron Lariviire.

Despite security improvements, terrorists continued to focus on attacking aircraft. In 1994, an attacker assembled a bomb in the aircraft lavatory and left it on board when he deplaned at an intermediate stop on the flight’s course. The bombing was a dry run for a more complex strike against multiple airlines.

When security measures were improved in the 1990s to defend against this style of attack, terrorists adapted once again. While planning the 9/11 attack, hijackers used permissible carry-on items—like box cutters—to hijack planes and turn them into human-guided cruise missiles.

In response to post-2001 security crackdowns to protect against that type of attack, jihadists again shifted their tactics toward onboard suicide attacks with hidden bombs. The first of these was the failed December 2001 shoe bomb attack. When security officers began screening shoes routinely, aspiring airline bombers then shifted to a plot to fill camouflaged toiletry containers in carry-on baggage with liquid explosives.

The U.S. Transportation Security Administration subsequently introduced restrictions on the quantity of liquids that passengers could bring aboard an aircraft, and, in turn, a jihadist attempted an attack with a device that was sewn disguised in a laptop, was smuggled aboard a flight in Somalia. Fortunately, that bomb only killed the suicide operative when it detonated and the aircraft

A bomb concealed in a soda can was smuggled onto an airliner in Egypt, killing 217.
was able to return to the airport for an emergency landing.

However, not all attacks on aviation involve hijacking or smuggling bombs aboard aircraft. Just as terrorists adjusted for heightened security at embassies by targeting traveling diplomats, attackers have found ways to attack airline passengers even as it has become more difficult to attack aircraft.

Back in the mid-1980s, terrorists attacked crowds of airline passengers beyond the confines of airport security at ticket counters in Rome and Vienna. In November 2002, al Qaeda operatives attempted to attack an Israeli airliner in Kenya with a surface-to-air missile. A 2011 attack at Moscow’s Domodedovo airport took advantage of the facility’s soft areas, as did the Brussels attack.

In the wake of the Rome and Vienna attacks, perimeter security at airports in Europe was temporarily increased, but due to the cost and effort involved, soon reverted to business as usual.

Similar short-term increases in security posture at airports across the globe were seen in the wake of the 9/11 attacks and to a lesser extent following Domodedovo.

In that attack, three operatives armed with his suicide bomb. Fortunately, the second attacker was shot and immobilized before he could do so. The third attacker was pursued by the authorities and detonated his device in a parking lot, causing minimal damage like the second bomber. Between the gunfire and the first bomb, however, 45 victims were killed—nearly three times more than in Brussels. The bulk of the victims were outside the security checkpoint at the door to the departure hall.

The targeting of the soft side of airports is especially attractive to grassroots groups and individuals who lack the ability to construct bombs sophisticated enough to be smuggled through security.

The July 4, 2002, armed assault against a ticket counter at Los Angeles International Airport and the June 2007 attack against the Glasgow Airport using a poorly constructed vehicle bomb are examples of attacks against the soft side of airports by poorly trained grassroots jihadists.

**EXPANDING DANGER**

In response to recent attacks in Brussels and Istanbul against the soft side of airports, security has again been increased. However, in many places this increased security is not much more than a show of force intended to reassure the traveling public and to perhaps deter poorly trained would-be terrorists. Without names or bag checks, it is difficult to keep a professional terrorist—especially one who has a ticket—away from the facility.

In some places, more thorough checkpoints have been established away from the airport to conduct initial screening. This tactic can be quite effective at smaller airports, but cumbersome at larger, busier airports where the heavy volume of travelers causes a backlog at the inspection point, thus effectively pushing the target away from the building to the crowd of people awaiting screening.

It is important to remember that the objective of terrorist planners is to create a high body count and a large amount of publicity. This means that an attack against the soft side of an airport can be almost as good as an attack against an aircraft, and a successful attack against an airport is better than a failed or thwarted attack against a harder target.

As the security at airports is pushed outward in response to attacks against the soft sides of airports, and checkpoints are established away from the building, this merely moves the real target—the vulnerable group of people awaiting screening from inside the building—to an area outside of it.

This principle was demonstrated during the June 28, 2016, attack against Istanbul’s Ataturk International Airport. In that attack, three operatives armed with AK-47s and suicide vests launched an attack on the soft side of the airport. Coming in the wake of the Brussels attack, and due to the overall high terrorist threat inside of Turkey, security was increased at Turkish airports, and armed security checkpoints were established at the entrances to the departure hall to prevent terrorists from entering the hall like they did in Brussels.

Shortly after the three attackers exited their cab outside the departure hall, they were confronted by police and a firefight erupted between the police and the attackers. The first operative was able to approach the security checkpoint and detonate his device amid the crowd. This device shattered a large window that permitted the second attacker to enter the building and begin searching for a crowd of people to target with his suicide bomb.

**STAYING AHEAD OF THE GAME**

Moving the security checkpoint outward from the airport simply moves the chokepoint outward, and the crowd of people waiting to get through that checkpoint remains vulnerable. This principle applies to many circumstances and locations beyond airports as well, posing a significant challenge to security professionals. While not an easy problem to address, some methods exist to mitigate the threat.

First, static security checkpoints themselves are not enough. It is necessary to establish outward-looking protective surveillance that extends beyond the property line. This surveillance also needs to focus on preoperational surveillance rather than just attack recognition. Once the attackers start shooting or detonating bombs, it can be helpful to quickly counter them and limit their access to additional victims, but it is far better
Built on the foundation and legacy of the highly regarded Wisenet line of network cameras, Hanwha makes across the board enhancements to deliver its most robust line to date. Based on Hanwha’s new proprietary Wisenet 5 chipset, Wisenet X series cameras feature WiseStream II advanced compression, industry leading 150dB WDR, USB for easy installation, dual SD card slot for high capacity on-board recording, and new intelligent video analytics and audio classification. Explore the innovation in Wisenet X and see how we can go further, together.

hanwhasecurity.com
to catch them at an earlier phase of the terrorist attack cycle.

Many large international airports are using surveillance technology that identifies suspicious behavior and alerts operators. The information collected by these programs can be shared with nearby airports, allowing them to keep an eye out for similar activity on their premises.

Terrorists often follow an attack planning cycle and are vulnerable to detection as they conduct the surveillance they require to carry out an attack. Terrorist operatives generally possess poor surveillance tradecraft and are not difficult to spot if people are looking for them.

But cops or soldiers manning a checkpoint at a door are not normally well positioned to spot such activity. This, ideally, needs to be accomplished by specialized units that have been trained in the craft of detecting surveillance and who are not tasked with manning checkpoints. Teams such as these will patrol parking areas and other spaces further away from the airport to identify potential threats.

This type of technology and information sharing between airports is imperative because attackers may scope out multiple facilities in a region. It is important for security teams at different airports to foster information sharing by alerting their counterparts to anomalous behavior.

Surveillance must also go beyond the use of cameras and should use a combination of human agents and cameras integrated with analytic software that can be used to help expand and direct the efforts of the humans. Cameras with nobody watching them are little better than no cameras at all. They may be useful for investigating an attack after the fact, but will be of little help in preventing an attack.

Even in a case where the preoperational surveillance is missed and an attack is underway, personnel located beyond checkpoints can help to see problems as they are developing rather than allowing attackers to gain tactical surprise by permitting them to have free rein in areas where they can assemble and coordinate their attack.

Furthermore, undercover operators can enjoy tactical surprise themselves and are in a great position to turn the tables on the attackers. Action is always faster than reaction, and if the attackers are permitted to draw and shoot first, it gives them a significant advantage over security forces.

A failed attack against a soft target venue in Garland, Texas, in May 2015, showed that security personnel manning the door of a facility can gain a life-or-death advantage in a firefight if they have advanced warning and a description of a potential threat.

In the Garland case, the FBI alerted local authorities of a potential threat to the event and provided the suspect’s vehicle description. This passing of critical intelligence prepared local officers for an impending attack. It also highlights the importance of intelligence sharing both horizontally and vertically within the law enforcement and security communities as they seek to secure airports and other soft targets.

SCOTT STEWART is vice president of tactical analysis at STRATFOR. Com and lead analyst for STRATFOR Threat Lens.
MOVING FORWARD
WITH HASSLE-FREE SECURITY

Developed specifically for airport applications, the Horton ControlFlow™ One-Way Revolving Door protects against security breaches in high-volume traffic areas. Horton’s patented Object Detection Technology uses a light curtain and photo-reflective sensors to scan for objects that could be left or passed to the secure area. Engineered for purpose, the new hassle-free security door is designed to last.

hortondoors.com

Visit us at ASIS, Booth #1033 / September 25 - 28, 2017
For product info #36 securitymgmt.hotims.com
PRODUCT SHOWCASE

EMPLOYEE SAFETY
Employers that have a mobile workforce, distributed teams, or large campuses may have difficulty tracking employees’ locations, schedules, and travel in case of location-based critical incidents. Everbridge of Burlington, Massachusetts, introduced the Everbridge Safety Connection to help businesses and organizations quickly locate and communicate with their people. The solution aggregates geo-location data from multiple systems so that administrators can reach out to those who are potentially at risk, including employees, contractors, and visitors. Booth 3040, Circle 422

MOBILE ACCESS
DSX Mobile Command from Dallas-based DSX Access Systems, Inc., brings the power of the DSX workstation program to the convenience of a smartphone. The mobile command feature allows the activation of custom predefined commands, locking and unlocking of doors, control of alarm points, and monitoring of system events from a mobile but secure application. Apple- and Android-compatible, it enables global functions such as building and campus lockdown, incident response reconfiguration, and more. Repetitive chores like momentarily unlocking a door or granting access to a gate can be programmed into command buttons for easy activation. Booth 7103, Circle 423

VIDEO MANAGEMENT
The Blazer Express from Hikvision of Zhejiang, China, is an intelligent video management station that manages Hikvision IP cameras with three primary functions. It’s a Windows-based NVR with a solid-state-drive operating system. It accommodates 16 or 32 cameras with 16 built-in PoE inputs for IP cameras, and up to 24 terabytes of onboard storage. The Blazer Express manages live video and playback from up to 15 remote NVRs. It offers powerful video analytic searches and point-of-sale integration. Booth 18037, Circle 424

DOOR OPERATOR
The Auto EntryControl Swinging Door Operator from Security Door Controls of Camarillo, California, provides hands-free, low-power, point-of-entry door control to help meet ADA requirements for door installations in storefronts, office buildings, campuses, and healthcare facilities. With its safe and reliable electro-mechanical drive and slim-line design, the microprocessor-based unit is self-tuning and self-learning. It offers non-handed operation, full mechanical stops, and a variety of interface options for sensors, push-plates, fire alarms, and electrified locks. It meets the ANSI standard for compliance with the Americans with Disabilities Act. Booth 21009, Circle 426

INTEGRATED SECURITY
G4S Secure Solutions of Jupiter, Florida, has a 100-year legacy of innovation in the security business. New processes assess and thwart security risks, while new technologies help security personnel execute their jobs more efficiently. Integrated Security Solutions address today’s security challenges in four steps: ASSESS and evaluate risks; EQUIP personnel with technology for efficient and effective protection; INTEGRATE solutions with the customer’s company, technology, and environment; and STAFF the solution with the correct trained personnel in the right roles and numbers. Booth 10053, Circle 425
PORTABLE DETECTOR
The Walkthrough Caster Set from Garrett Metal Detectors of Garland, Texas, is ideal for stadiums, special events, and school use. The casters, which can be permanently attached, allow full mobility of a Garrett PD 6500i walkthrough metal detector by one person. Detectors can be moved to a secure location when they are not in use and provide an unimpeached exit at the close of an event. The caster assembly is constructed of durable, powder-coated steel for use in all types of environmental conditions. Booth 16127, Circle 427

COUNTERSURVEILLANCE
Research Electronics International (REI) of Algood, Tennessee, introduced the ANDRE Near-field Detection Receiver, a handheld broadband receiver that detects known, unknown, illegal, disruptive, or interfering transmissions. The ANDRE locates nearby RF, infrared, visible light, carrier current, and other types of transmitters. The ANDRE Advanced Kit includes a wide range of accessories specifically designed to receive transmissions across a 1 kHz to 6 GHz frequency range. It presents signal responses on a touchscreen display in the form of a histogram that shows signal strength over time. The device’s frequency counter generates an automatic signal list and detailed frequency band classification. Audio mode accesses analog audio demodulation, playback, and recording. Booth 19124, Circle 429

SECURITY MANAGEMENT
AMAG Technology, Inc., of Torrance, California, offers a security solution that manages access control, video surveillance, intrusion detection, identity management, visitor management, and incident management. Powered by a robust, policy-based platform, it helps security managers reduce risk, reduce cost, and maintain compliance. The Symmetry Security Management System provides intelligent networked solutions scaled to manage security challenges from small, remote facilities to multinational organizations around the world. Booth 11053, Circle 431

DOME CAMERA
The AXIS Q6155-E PTZ Dome Network Camera from Axis Communications of Chelmsford, Massachusetts, is a pan-tilt-zoom model with laser focus, offering much faster and more accurate autofocus even in the most challenging lighting conditions. The new laser focus technology combined with high image quality allows people and objects to be identified quickly and precisely. The camera offers HDTV 1080p resolution and 30x optical zoom. The camera also has Axis’ Zipstream technology, which lowers bandwidth and storage requirements while keeping necessary forensic details. Booth 14051, Circle 428

SECURE STORAGE
The VUE Locker from Chicago-based LossPreventionSolution.com features an open mesh design and a welded-on hardened steel hasp that resists cutting and hammering, keeping items safe and untouched. The welded construction of expanded metal and the heavy-duty, powder-coated finish hold up in the harshest industrial settings. The company’s aesthetically pleasing, custom-designed solutions allow quick visual inspection of stored goods, ventilation, and peace of mind. Booth 22150, Circle 430
SECURITY BOOTHS
Par-Kut International, Inc., of Harrison Township, Michigan, manufactures bullet-resistant security booths for high-security locations. The enclosures meet protective levels UL8, NIJ4, and higher and can be engineered to meet blast load requirements. In addition to HVAC, options include reflective glass, gun ports, anti-fatigue floor mats, dimmable interior lighting, and generators. They can be built on trailers or on top of towers. Bullet-resistant guard booths can have a very basic appearance or incorporate design enhancements to blend with surroundings. Circle 436

GLOBAL INTELLIGENCE
NC4 Risk Center provides security professionals with timely, comprehensive global threat and incident information about physical hazards that may have an adverse effect on physical security, personnel, supply chains, and other mission critical infrastructure within the organization. NC4 of El Segundo, California, has a dedicated team of skilled analysts working to create situational awareness by monitoring, gathering, analyzing, reporting, escalating, and responding to incidents and events that threaten an organization’s resilience. NC4 Risk Center aggregates and integrates information from public and private sources to bring users a highly configurable presentation of relevant information for operational risk management. Booth 33096, Circle 433

VIDEO SEARCH
FaceVACS-VideoScan video screening and analytics technology from Cognitec Systems Corporation of Dresden, Germany, now allows users to perform complex searches on persons appearing in camera streams and stored media files. Users can upload videos recorded at a specific location and time to track possible participants in a crime. They can find a person enrolled in an image database or search for an unknown person and locate their appearances in multiple videos. Person searches can be filtered by age ranges, gender, ethnicity, and glasses. A special IP video camera with built-in face detection and tracking technology is a component of the system. Booth 17127, Circle 432

TAILGATE DETECTION
Detex Corporation of New Braunfels, Texas, offers dependable panic hardware for restricted secure areas, where unauthorized entry must be controlled and authorized entry must be quick and reliable. The Tailgate Detection System ensures that only one person enters a door for each authorized card read. It is compatible with most access control technologies, is easy to retrofit, and has an integrated door prop alarm for extra security. Booth 19109, Circle 435

RUGGED PHONES
GAI-Tronics of Mohnton, Pennsylvania, announced a new line of Behavioral Health Telephones, which meet the stringent standards set forth by the U.S. Department of Veterans Affairs and the Design Guide for the Built Environment of Behavioral Health Facilities. Designed with the safety of both staff and tenants in mind, the phones come in a variety of styles. They feature stainless steel construction and an armored 12-inch cord for handset models. They can be mounted in robust surface mount enclosures. The phones are available in both analog and VoIP configurations and some models can be used indoors or outdoors. Booth 2037, Circle 434
not only a life was lost
an empire fell
only if caesar had somebody watching his back
grey mustn't exceed white®

The Company
SECURITY 2000 license holder, registered with the Government of Pakistan in 1996, provides complete private security services. In 2001 opened a full licensed office in Dubai. 20 years later 2000 is a brand of professional security spread from Kel to Gwadar headquartered in Karachi, 10 local offices in country and 1 each overseas in UAE and London taking care of client needs. Has partnered with leading security companies like Pinkerton and Global Source. It provides service to 7 top Fortune 50 companies and 12 top 25 companies of Pakistan. Multinationals getting services include Standard Chartered, ICI, Nokia, Pepsi, YKK, Nestle, Abbott, PPL, L'Oreal, Syngenta, Sanofi, BAH, HBL, DIB and now Metrobus. There are 90 others.

The Leadership

The Future
Every business must be based on white or black inputs of information. The space in between is grey. While black or grey may exceed each other, your business may still run but the moment grey exceeds white you are in trouble. To adopt a zero risk policy only proceed where white clearly exceeds grey. If not ask, We will provide you information you need obtained from anywhere in the world in under 30 days. Starting 2017 we have begun providing this service to clients in Pakistan and worldwide. Ask ANY question confidentially about any prospective client, partner or any defaulter or any other issue. We will trace the perpetrator, provide answers and recommendations, which will help your life, your business. No one can hide. Security is about reducing the grey.® And we will do it for you.

Winner International and other Security Awards
crc@security2000.com

ISO 9001 Certified

ask a question
20 offices affiliates 100 countries

Your Protection Executive Protection Assets Protection Brand Protection Diligence Protection Survey Protection

Global due diligence
Global asset search
Corporate mergers
Corporate checks

For product info #37 securitymgmt.hotims.com

Your Protection Executive Protection Assets Protection Brand Protection Diligence Protection Survey Protection

Global due diligence
Global asset search
Corporate mergers
Corporate checks

For product info #37 securitymgmt.hotims.com
PERSONAL SAFETY

Verint of Melville, New York, introduced the Mobile Reporter phone application, which enables users to immediately alert security to a potential security issue—regardless of their location. The app will send critical updates to the command center in a wide variety of formats, such as a simple SOS alert, text message, detailed report form, photo, and live audio and video. The technology can be leveraged for a wide variety of applications, including executive travel, remote employees, outside contractors, and visitor safety. When alerted, the command center gets a single view of users, their locations, and their current status. The system offers a variety of mechanisms to initiate active or passive tracking of people through their devices and bi-directional communication with the device. Booth 2097, Circle 437

IDENTITY ACCESS

The SAFE Sports and Events Access Manager from San Jose–based Quantum Secure—part of HID Global—enables secure and rapid entry to stadiums and other venues, providing security for temporary or limited-engagement events. The mobile app solution removes the need to rely on clipboards and lists to manage contractors, vendors, volunteers, and other nonticketed individuals who need temporary access to a venue. The solution also integrates with IT systems and multiple handheld devices for swift, accurate real-time validation and immediate onboarding and provisioning for a variety of identity types based on access permissions. The solution also records identity access logs to track key operational and security metrics and streamline compliance processes. Booth 11063, Circle 438

IP CAMERAS

Honeywell of Northford, Connecticut, expanded its Performance Series IP Family to include new, affordable, easy-to-install 1080p and 4MP wide dynamic range IP cameras. The new cameras deliver high-quality video, a superior user experience, easy video integration with other solutions, and improved user account security with enhanced risk reduction, lowering installation, operation, and maintenance costs. The range includes 15 new IP cameras in mini dome, micro dome, ball, and bullet designs. Select cameras include motorized focal zoom technology, which autofocuses the lens after zooming. Booth 14025, Circle 439

INTERCOM ACCESS

The Complete IP Door Intercom System from Talkaphone of Niles, Illinois, is a fully integrated access control package with head-end IP video attendant station and two-way IP call station. The VOIP201C3SYS package includes the VOIP201C3 Call Station that connects with the AVM-1 IP video attendant station to provide a one-stop solution. The AVM-1 can monitor and regulate entry points through the call stations using video and voice communications. Easily install it at any access point to intelligently control customer or employee entry or exit. The included VOIP201C3 surface mounted call station with an ONVIF-compliant wide-angle megapixel IP camera is constructed of IP66-rated, vandal-resistant, marine-grade stainless steel. An additional Ethernet port is provided to support connection to optional Ethernet devices. The call station also allows for remote software upgrades, configuration, and monitoring. Booth 10109, Circle 441

ETHERNET TRANSPORT

ComNet, Communication Networks of Danbury, Connecticut, introduced the ComNet CTS24+2, which offers up to 24 ports of 10/100Mbps Ethernet and two ports of Gigabit uplink using TX or SFP combo ports. Up to three eight-channel modules can be used. These modules are offered in CAT5/6 10/100Mbps Ethernet, optical 100FX SFP, or CopperLine Coax or UTP extending interfaces. Booth 4071, Circle 440
Attend the premier event for security professionals!

Join more than 22,000 security management professionals for best-in-class analyses and insights, the latest technology innovations, and unparalleled opportunities for collaboration and career advancement.

REGISTRATION NOW OPEN

www.securityexpo.org/apr
VIDEO ANALYTICS
Avigilon Appearance Search from Avigilon of Vancouver, British Columbia, Canada, is a sophisticated, deep-learning, artificial intelligence search engine for video data. It easily sorts through hours of footage to quickly locate a specific person of interest across all cameras on an entire site. It can help track a person’s route and identify previous and last-known locations to improve incident response time and enhance forensic investigations. Avigilon Appearance Search technology integrates with Avigilon Control Center 6.0 Enterprise edition software, Avigilon cameras with self-learning video analytics, and select NVRs. Booth 22043, Circle 442

SECURITY REVOLVING DOORS
Facilities requiring controlled access of authorized personnel to sensitive areas can rely on security revolving doors from dormakaba of Winston-Salem, North Carolina. The doors combine convenience with performance, providing a practical and secure solution for any interior access point. Doors are designed to harmonize with traditional or modern environments. All models are available in a wide variety of finishes and can be configured to allow essential and safe passage. A sophisticated sensor system in compliance with current safety standards prevents possible injury. Depending on the security requirements, the door may be equipped with a contact mat, scales, or internal monitoring. Booth 8053, Circle 443

ACCESS SOFTWARE
Keyscan of Whitby, Ontario, Canada, offers Aurora access control management software, which seamlessly integrates with Kaba E-Plex wireless locks to provide a single software platform solution. New features include Microsoft-certified webcam support, plus integrations with video management systems such as Salient Systems, biometric readers from BioConnect and Suprema, and visitor management from EasyLobby. Keyscan networked access control systems are designed for applications in all vertical markets. Booth 8053, Circle 444

ETHERNET OVER COAX
The eBridge800E Managed 8-port EoC Receiver with integral PoE+ switch is the head-end solution for upgrading coax to IP. New from Altronix of Brooklyn, New York, the compact 1U rack unit features two 1GB uplinks, an 8-port PoE+ switch, and CAT-5 to coax media converter. IP devices can be deployed up to 300 meters away, and a built-in battery charger ensures seamless operation. LINQ technology allows users to monitor, control, and report power/diagnostics from anywhere over the network. The unit is made in the United States and has a lifetime warranty. Booth 11073, Circle 445

CONSOLES
Impulse Dual Sit/Stand consoles from Minneapolis-based Winsted Corporation combine ergonomics and operator comfort. Studies show that prolonged sitting can be detrimental to one’s health, and that alternating between sitting and standing can increase energy and reduce fatigue. The consoles provide two independently adjustable, ergonomically curved work surfaces. These surfaces can be raised and lowered to meet the needs of individual operators while offering flexibility to sit or stand. Options include electric-lift legs for adjusting the work surface height from 30 to 46 inches at the push of a button, three programmable height settings, and a load capacity of 520 pounds. Booth 14109, Circle 446
WEATHERPROOF LOCKS
Abloy Security of Irving, Texas, offers a range of tough locks that can withstand severe weather conditions and environmental extremes. ABLOY PROTEC2 CLIQ LED key and interface make it easy to retrofit mechanical locks with electromechanical models. There are no batteries in the locks, because the power comes from the key. CLIQ technology provides audit trails in both the lock and the key, flexible time functions, and immediate removal of lost keys. All padlocks feature case-hardened boron-steel shackles and hardened steel UL-listed cylinders. Patent-protected keys can also open ABLOY door locks, and the keys cannot be duplicated.  
Booth 8061, Circle 448

SECURITY PANELS
Mercury Security Products, LLC, of Long Beach, California, released the new MS Bridge series. New MS Bridge multi-device interface panels are designed to fit the specific physical parameters of Software House Pro Series access systems, and they can be easily installed for a changeover to the Authentic Mercury open platform. The award-winning solution provides a cost-effective and streamlined path to move beyond the limitations of proprietary hardware for feature-rich access control. The Authentic Mercury model also allows customers to choose from industry-leading access control software providers, both at time of product selection and in the future as their needs evolve.  
Circle 452

PROTECTIVE COVERS
STI tough polycarbonate covers from Safety Technology International, Inc., of Waterford, Michigan, help prevent theft and vandalism to larger keypads, access controls, volume and lighting controls, and other similar devices. Molded of clear polycarbonate, which is the same material used in football helmets, each protected unit can be clearly seen and quickly identified. The cover has a strong piano-style hinge, enclosed back box, gasket, and lock. Other models are available.  
Booth 30044, Circle 449

UNDER-VEHICLE INSPECTION
The CPAS enhanced under-vehicle surveillance systems from Comm Port Technologies of Cranbury, New Jersey, has been re-engineered with advanced metal alloys to support up to 78 tons. Security personnel can view the entire length of a vehicle in real time and full color. Full high-definition color is supported even with vehicles moving up to 75 kilometers per hour. As part of the updated package, CPAS now includes a driver image camera, automatic number plate recognition, templates, and automatic comparison software all bundled together.  
Booth 352, Circle 450

ANTI-TAILGATING SYSTEM
Designed Security, Inc., (DSI) of Bastrop, Texas, introduced the Entry Sentry, an optical security device that detects multiple persons entering a doorway on a single valid authorization. It uses proprietary sensing technology to detect direction and tailgating, and it is compatible with all card reader technologies and access control systems. The system mounts easily on standard door frames and hallway walls. Entry Sentry consists of two self-contained, narrow door- or wall-mounted units that provide both local and remote alarm indications.  
Booth 19109, Circle 451
VOLUNTEERS PLAN FOR THE FUTURE

MORE THAN 250 ASIS International volunteer leaders from across the globe gathered in Arlington, Virginia, for the January leadership meetings and strategic planning workshop. The program launched with member awards, followed by an organizational update from CEO Peter J. O’Neil, CAE. He explained the changes taking place to better align staff and technology investments with organizational priorities.

The workshop component of the program opened with a discussion on the Society’s new strategic plan. Attendees broke into working groups to provide input on aligning their volunteer areas of work with the new plan. Many innovative ideas emerged and results are being used by ASIS staff and the Board of Directors to shape deliverables and metrics. At the end of the day, attendees and HQ staff came together for fun-filled, sports pub-themed networking.

“The opportunity to collaborate with ASIS staff and the Board of Directors, have concerns heard, and be involved in developing solutions for change was an unparalleled volunteer leadership experience that was on point, transparent, and highly appreciated,” said Senior Regional Vice President Jeffrey A. Slotnick, CPP, PSP. “The Sports Night was a terrific end to a full day of camaraderie and information sharing.”

Day two included the annual business meeting address to the membership from ASIS President Thomas J. Langer, CPP, who noted that the past two years have been “the stage setting and execution years for the Society’s refreshed direction.” He recapped past-year milestones, citing new leadership at headquarters, a renewed focus on member value, new strategic priorities (including ESRM and comprehensive mobile access to Society programs and services), and increased global growth and inclusion so all members can reap the full rewards of their membership. He noted that the board has addressed many tough realities—both financial and structural—and is fully aligned with the Society’s path forward.

“In 2017, expect to see positive changes in member engagement, website design and experience, educational offerings and learning formats, and more responsiveness to chapters, councils, and regions.”

Go to www.asisonline.org/volunteer to listen to Langer’s full address.

The program wrapped up with the Society’s first town hall of 2017, an interactive Q&A between volunteer leaders, board members, and ASIS executive leadership. The positive response from this exchange continued with the launch of bimonthly virtual town halls beginning in March. Share your thoughts on the Society’s new direction via email to asisfuture@asisonline.org.
ASIS 2017: WHAT’S NEW?

Get ready to experience the best in security networking, education, and technology. The ASIS International 63rd Annual Seminar and Exhibits (ASIS 2017) is coming to Dallas, Texas, September 25–28.

The finest global security event in the industry is getting better. Some events will be expanded and new ones will be launched. The calendar is shifting some popular activities to new times. These changes will lay the foundation for what is sure to remain an outstanding event for years to come.

Some of what’s new for 2017 includes:

- **New hours for exhibits.** Expo days will shift from the traditional Monday through Wednesday schedule to Tuesday through Thursday, creating more non-competing hours so attendees can maximize their educational and networking experiences. Tuesday and Wednesday, the exhibit hall will be open from 10:00...
am to 5:30 pm; Thursday’s hours are 10:00 am to 1:00 pm.

**Opening night celebration.** Join peers and colleagues from around the globe and across the profession to kick off ASIS 2017 on Sunday, September 24, with a big Texas welcome. Mechanical bull riding, armadillo races, good food, live music...you’ll find it all at the ASIS 2017 Opening Night Celebration. This event, which will be held from 7:00 pm to 10:00 pm, was formerly known as the Welcome Reception.

**ASIS Happy Hour.** Connect with peers and clients on Tuesday, September 26, from 4:30 pm to 5:30 pm. This gathering, which will be held in the exhibit hall, is designed to help you learn more about a wide range of security solutions and innovations.

**President’s Reception.** This event is moving from Monday night to Wednesday night. It is always one of the most anticipated events at Seminar—and this year will be no different! Be sure to stay in town for this one-of-a-kind experience.

**New educational offerings.** Watch for new learning formats, plus more education on the exhibit hall floor. Visit www.securityexpo.org for the latest announcements and updates. Use #ASIS17 on Facebook and Twitter to connect with ASIS show management staff, exhibitors, and fellow attendees.

**NEW CHAIR OF THE S&G COMMISSION**

For the first time in a decade, the ASIS International Standards and Guidelines (S&G) Commission has a new chairman. Michael Knoke, CPP, takes on the role vacated by F. Mark Geraci, CPP, at the start of 2017. Serving alongside Knoke is Vice Chair Bernard Vendrell. The Commission has a full plate in the year ahead, including the upcoming release of the Security and Resilience in Organizations and their Supply Chain Standard. In addition, work is well underway on a joint ASIS/(ISC)/ISACA Security Awareness Standard and a Private Security Officer Selection and Training Standard. Keep current on S&G news and activities at www.asisonline.org/standards.

**CSO SUMMIT**

Nearly 75 senior security executives from across the globe are expected to attend the 10th Annual CSO Summit April 23–25 at the Ritz Carlton at Pentagon City in Arlington, Virginia. The high-level program features sessions on cyber risk, community stakeholder engagement, and metrics for the C-suite. Attendees will also get a behind-the-scenes tour of the U.S. Capitol and gain insights on public-private partnerships from event keynoter John Walsh, who created the television program America’s Most Wanted and now anchors The Hunt with John Walsh on CNN. Summit updates can be found on the CSO Center website, www.cso.asisonline.org.

**MEMBER BOOK REVIEW**

Managing Critical Incidents and Large-Scale Event Security. By Eloy Nuñez and Ernest G. Vendrell. Published by CRC Press; 314 pages, $89.95.

Examining case studies and after-action reports for valuable lessons, Managing Critical Incidents and Large-Scale Event Security provides a timely resource for understanding effective critical incident management. Effectively conveying their knowledge and experience, the authors use vignettes to provide real-world examples of hurricane response planning and recovery; planning and post-action events for several Super Bowls; and responses to various riots and other incidents from the 1980s to 2015. While walking the reader through known and familiar concepts and practices, Nuñez and Vendrell deliver a fresh perspective on successful critical incident management, explaining how to attain fiscal resources for planning, exercising, executing, and recovering from security events.

The authors challenge Federal Emergency Management Agency (FEMA) precepts of four phases of critical
incident management. Advocating for a three-phase model, Nuñez and Vredell suggest that mitigation is intrinsic throughout all stages and therefore is not a phase in and of itself. Throughout the text, the authors advocate for mitigation during the preparedness, response, and recovery phases of critical incident management.

Written with the critical incident manager in mind, the book delivers sound advice, providing readers with several checklists for effective training and management of such events. Managing Critical Incidents is ideal as a go-to reference for incident managers, as well as a valuable textbook for instructing future practitioners.

**REVIEWER:** Dr. Will Morrison, CPP, is a security management professional with more than 35 years of service in the U.S. federal government that includes work in national and homeland security. He has been a member of ASIS International since 2004.

**LIFETIME MEMBERS**
The ASIS Board of Directors granted life membership to the following individuals:

- Ira M. Weiss, CPP
- Thomas M. Seamon, CPP
- Brian N. Goldsworthy, CPP
- Robert C. Anderton, CPP
- Richard F. Williams, CPP

**LIFETIME CERTIFICANTS**
Congratulations to the following security professionals who have achieved lifetime certification status:

- James V. Clarke, CPP
- John W. Collins, Jr., CPP
- Harold F. Crawford, CPP
- Daniel R. Devine, CPP
- Richard C. Hofmann, CPP
- Lester E. McFarland, CPP
- Margaret Nix, CPP
- Michael J. Pepe, CPP
- Robert W. Riley, CPP
- Fergus P. Ross, CPP
- Dennis J. Urban, CPP
- Jose Luis Zepeda, CPP

In 2016, Timothy McCreight, CPP, made two important changes to his résumé. In March, he joined Above Security, a Hitachi Group Company, as director of advisory services. In September, he was elected to the ASIS Board of Directors.

At Above Security, McCreight leads a team of senior information security professionals as they earn positions of trust with clients and help grow their information security programs. He also helps senior executives understand the risks facing their people, property, and information while demonstrating the positive effect a security program can have for their organizations.

A native of Edmonton, Alberta, Canada, McCreight began his career in hotel security and then joined the provincial telephone company. Both positions gave him opportunities to learn about physical security, but he never lost interest in computers. Returning to college to study computer programming and network design led to his appointment as chief information security officer for the Government of Alberta. Despite starting Alberta’s program from scratch, his team won Best Information Security Team just three years later. “Having exposure to both disciplines provided me with greater insight into concepts such as Enterprise Security Risk Management and the business principles of a holistic security program,” he says.

The importance of paying attention to the “people part of security management” was ingrained in McCreight early in his career. During an investigation, he discovered that an employee was siphoning off money earmarked for charity to support a spouse’s drug habit. Once exposed, the employee was let go. But McCreight provided the employee with counseling and access to a lawyer, which enabled the employee to start a new life. “I focused on the investigation,” McCreight recalls, “but provided hope to someone in a desperate situation.”

As an ASIS member, McCreight has taken advantage of opportunities to expand his security industry knowledge by attending and speaking at conferences, assuming leadership positions, and moving onto the ASIS Board. Impressed with colleagues who had attained the Certified Protection Professional® (CPP), McCreight was motivated to pursue his own certification. “Sitting with these security leaders, hearing their stories, and seeing how they gave new members advice and guidance really drove me to start seeking my CPP,” which he attained in 2002.

He cautions others seeking the CPP to first ask two questions: Are you ready to commit a lot of personal time to prepare for the exam? And why do you want to attain the CPP? An honest answer to the second question is essential. “Attaining the CPP is not a ticket to a CSO or VP role, and it won’t guarantee a raise or promotion,” he asserts. Rather, “the CPP demonstrates a commitment to the security profession that you earn—through study, practice, and experience. This commitment also extends to the values and ethics of ASIS, he adds, and “you need to be able to demonstrate your professionalism as a CPP.”

McCreight values keeping up with trends facing the security industry and learning how new threats may affect clients. Being a CPP “has given me more focus on the work I do and how I present myself to my organization and my clients.”

**PROFILE BY MARY ALICE DAVIDSON, PRINCIPAL, DAVIDSON COMMUNICATIONS**
FRAUD. Volkswagen will plead guilty to three U.S. criminal felony counts and pay a $2.8 billion penalty to resolve a U.S. federal criminal investigation into its cheating on emissions tests. The plea is the result of Volkswagen’s long-running scheme to sell roughly 590,000 diesel vehicles in the United States by using a device designed to cheat emissions tests, which are mandated by the U.S. Environmental Protection Agency (EPA) and the California Air Resources Board (CARB).

Volkswagen, according to the U.S. Department of Justice (DOJ), participated in a conspiracy to defraud the United States and its U.S. customers and to violate the Clean Air Act by misleading regulators and customers about whether its diesel vehicles complied with U.S. emissions standards.

Volkswagen also pleaded guilty to obstruction of justice for destroying documents related to the scheme and to a separate crime of importing vehicles that did not comply with U.S. emissions limits into the country.

CORRUPTION
Brazilian global construction conglomerate Odebrecht S.A. and petrochemical company Braskem pleaded guilty and agreed to pay penalties of at least $3.5 billion to resolve U.S., Brazilian, and Swiss charges of bribery. The two companies used a business unit, dubbed a “Department of Bribery” by the U.S. Department of Justice (DOJ), to systematically pay hundreds of millions of dollars to corrupt government officials in countries around the world to win business. “The criminal conduct was directed by the highest levels of [Odebrecht], with the bribes paid through a complex network of shell companies, off-book transactions, and off-shore bank accounts,” according to the DOJ. (U.S. v. Odebrecht S.A., U.S. District Court for the Eastern District of New York, No. 16-643 (RJD), 2017; U.S. v. Braskem, U.S. District Court for the Eastern District of New York, No. 16-644 (RJD), 2017)

BREAKS
Employees on rest breaks must be relieved of all of their duties, the California Supreme Court ruled, finding that a security firm violated state law by requiring security guards to carry phones and radios and remain on call during rest breaks. “California law requires employers to relieve their employees of all work-related duties and employer control during 10-minute rest periods,” the court wrote. The suit was brought by security guards employed by ABM Security Services, Inc. (Augustus v. ABM Security Services, Inc., Supreme Court of California, No. S224853, 2016)

FIREARMS
A U.S. appeals court found that California’s 10-day waiting period to purchase a firearm is a reasonable safety precaution for all individuals seeking to purchase a gun, regardless of whether they have purchased a gun in the state before. In a lawsuit challenging California’s law that created the waiting period, the appeals court reversed a lower court’s decision, finding that the law does not violate plaintiffs’ Second Amendment rights under the U.S. Constitution because the waiting period is a “reasonable precaution for the purchase of a second or third weapon, as well as for a first purchase.” (Silvester v. Harris, U.S. Court of Appeals for the Ninth Circuit, No. 14-16840, 2016)
Under the terms of the plea agreement, which must be accepted by the court, Volkswagen will plead guilty to all these crimes, will be on probation for three years, will be under an independent corporate compliance monitor who will oversee the company for at least three years, and agrees to fully cooperate in the Justice Department’s ongoing investigation and prosecution of individuals responsible for these crimes,” the DOJ said in a statement.

A federal grand jury also indicted six former Volkswagen executives for their roles in the cheating scheme: Heinz-Jakob Neusser, former head of development; Jens Hadler, former head of engine development; Richard Dorenkamp, former head of engine development after-treatment department; Bernd Gottweis, former supervisor responsible for quality management and product safety; Oliver Schmidt, former general manager in charge of the environment and engineering office; and Jürgen Peter, part of the quality management and product safety group.

Volkswagen engineers began designing a new diesel engine in 2006 to meet U.S. emissions standards that would go into effect in 2007. The engine was marketed as a “clean diesel” engine, but Volkswagen soon realized that it could not design an engine to meet the stricter standards and attract sufficient customer demand in the United States. So, Volkswagen decided to use a software function to cheat U.S. emissions tests.

“Volkswagen engineers working under Dorenkamp and Hadler designed and implemented software to recognize whether a vehicle was undergoing standard U.S. emissions testing on a dynamometer (device for measuring force) or it was being driven on the road under normal driving conditions,” the DOJ said. “If the software detected that the vehicle was not being tested, it operated in a different mode, in which the vehicle’s emissions control systems were reduced substantially, causing the vehicle to emit [mono-nitrogen oxides] up to 40 times higher than U.S. standards.”

This new engine model was installed in Volkswagen vehicles beginning in 2009. The vehicles were then imported to the United States. To legally sell the vehicles in the United States, the coconspirators allegedly lied to the EPA about the existence of the test-cheating software.

In 2014, West Virginia University’s Center for Alternative Fuels, Engines, and Emissions published a study commissioned by the International Council on Clean Transportation. The study found “substantial discrepancies” for Volkswagen vehicles when tested on the road compared to when they were undergoing EPA and other tests on dynamometers.

Instead of telling the truth about the testing, however, Volkswagen employees—including Neusser, Gottweis, Schmidt, and Peter—attempted to disclose as little information as possible to U.S. regulators, customers, and the public.

U.S. regulators followed up with

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

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

To see the full text of selected regulations, bills, and reports, visit www.securitymanagement.com and click on SM Online.
Volkswagen to determine why the discrepancies in testing were occurring. But in “implementing their strategy of disclosing as little as possible, Neusser, Gottweis, Schmidt, Peter, and their co-conspirators” provided regulators with “testing results, data, presentations, and statements in an attempt to make it appear that there were innocent mechanical and technological problems to blame, while secretly knowing that the primary reason for the discrepancy was their cheating software that was installed in every Volkswagen diesel vehicle sold in the United States,” the DOJ explained.

Volkswagen used this strategy with regulators for more than 18 months, successfully obstructing attempts to uncover the truth.

In a separate civil case, Volkswagen will pay $1.5 billion for violating EPA regulations and for customs fraud. The agreement with the EPA in the civil case also requires injunctive relief to prevent future violations. It also resolves alleged violations of the Financial Institutions Reform, Recovery, and Enforcement Act. (U.S. v. Volkswagen, U.S. District Court for the Eastern District of Michigan, No. 16-CR-20394, 2017)

**SURVEILLANCE.** European Union (EU) member states may not impose general obligations on electronic communications services to retain data, the EU Court of Justice ruled.

The decision was a blow to the recently enacted U.K. Investigatory Powers Law, which allows the U.K. Home Department to require public telecommunications operators to retain all data related to communications for up to 12 months. The U.K. law was enacted in 2016 to replace the expiring Data Retention and Investigatory Powers Act (DRIPA) that was passed in 2014.

U.K. Member of Parliament Tom Watson and Brexit Secretary David Davis filed suit against DRIPA in 2014, and the U.K. High Court found parts of it to be unlawful and incompatible with EU law.

The U.K. government appealed the ruling, which brought the case to the EU Court of Justice. It found that EU law precludes the “general and indiscriminate” retention of electronic communications traffic data and location data.

“The fact that the data is retained without users of electronic communications services being informed of the fact is likely to cause the persons concerned to feel that their private lives are the subject of constant surveillance,” the court wrote. “Consequently, only the objective of fighting serious crime is capable of justifying such interference.”

The court ruled that EU member states can—as a preventive measure—create provisions for targeted retention of electronic communications data to fight serious crime, “provided that such retention is, with respect to the categories of data to be retained, the means of communication affected, the persons concerned, and the chosen duration of retention, limited to what is strictly necessary.”

The court also explained that access to the data by national authorities must be subject to conditions, including being reviewed by an independent authority and being retained within the European Union.

The U.K. law “exceeds the limits of what is strictly necessary and cannot be considered to be justified within a democratic society,” the court added. The U.K. government plans to appeal the ruling to the EU Court of Appeals because it has not completed Brexit and is still subject to EU law. (Secretary of State for the Home Department v. Tom Watson and Others, Court of Justice of the European Union, No. C-698/15, 2016)

**U.S. LEGISLATION**

**EMAIL.** The U.S. House of Representatives passed legislation that would update privacy protections for electronic communications stored by third-party service providers.

The Email Privacy Act (H.R. 387) would update the Electronic Communications Privacy Act (ECPA) to require all U.S. government agencies to obtain a warrant to search Americans’ online communications, regardless of when

---

**LEGAL HIGH-LIGHTS**

**CASE:** United States v. Takata
**VENUE:** U.S. District Court for the Eastern District of Michigan
**STATUS:** Takata pleaded guilty
**SIGNIFICANCE:** Takata pleaded guilty to one count of wire fraud and will pay criminal penalties of $1 billion for lying about its defective airbag inflators.

**CASE:** EEOC v. PJ Utah LLC
**VENUE:** U.S. Dist. Ct. for the Dist. of Utah
**STATUS:** Settled
**SIGNIFICANCE:** The owners of a Papa John’s Pizza franchise will pay $125,000 to settle a disability discrimination lawsuit for allegedly providing a job coach to an employee with Down syndrome.

**CASE:** Fraud
**VENUE:** U.S. District Court for the Central District of Michigan
**STATUS:** Subpoenaed
**SIGNIFICANCE:** The owners of a Papa John’s Pizza franchise will pay $125,000 to settle a disability discrimination lawsuit for allegedly providing a job coach to an employee with Down syndrome.
U.S. REGULATIONS

The U.S. agencies published a final rule that requires contract employees who handle personally identifiable information (PII) or work with a system of records to complete privacy training. The rule was crafted by the U.S. Department of Defense, the General Services Administration, and the National Aeronautics and Space Administration. It requires contract employees who handle PII to receive initial and annual privacy training on working with PII and the contractor’s incident response plan. The privacy training must address the safeguarding of PII or a system of records, and should be “role-based, provide foundational as well as more advanced levels of training, and have measures in place to test the knowledge level of users,” according to the rule.

Contractors are also required to maintain documentation on employees’ privacy training and provide it to the agencies upon request. The rule applies to contractors and subcontractors at or below the simplified acquisition threshold of approximately $150,000 and to contracts and subcontracts for commercial items.

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

AS PART OF THE CELEBRATION of Finland’s 100th anniversary as an independent state, the Centenary World Championships in Lahti were held in February and March. The Lahti2017 FIS Nordic World Ski Championships featured more than 700 athletes from 60 different countries competing in 21 disciplines.

Lahti city’s public transport committee, Lahden Seudun Liikenne, selected Confi dex Ltd. to deliver smart tickets for use by tourists, suppliers, and volunteer staff for transportation and admission during the championships. The smart ticket for the championships could be purchased for one to seven days for both admission and transportation. It facilitated the estimated increase of 8,000 daily trips.

Confi dex previously supplied a Waltti travel card solution to Lippu-ja maksujärjestelmä Oy, the publicly owned company that oversees public transportation throughout Finland. The Waltti travel card system, currently in use in 13 cities and three rural transportation areas in Finland, is compatible with the cards used during the championships and will be used for future special events.

PARTNERSHIPS AND DEALS

Intelligent fire panels from Advanced were chosen to protect the National Theatre in London as part of its renovation. Tri-Management designed and implemented the system.

AMAG Technology and Microstrategy incorporated collaborated on a next-generation physical access control solution combining Microstrategy’s Usher and AMAG Technology’s Symmetry access control.

Dahua Technology USA and PSA Security Network announced a partnership to distribute Dahua’s video surveillance solutions to the security industry.

DataDirect Networks partnered with Synergy Solutions Management to offer organizations access to a facility near Vancouver, Canada, where users can plan, design, and test video surveillance solutions and conduct training.

Generali Global Assistance partnered with The University of Texas at Austin’s Center for Identity for education, research, and advocacy initiatives in the identity protection arena.

Canadian Pacific Railway selected an integrated suite of public safety software from Hexagon Safety & Infrastructure for managing incidents and responses.

Interfocus Technologies formed a partnership with Cylance Inc. to integrate its endpoint management solution and Cylance’s endpoint malware prevention product.

NEC Corporation conducted trials for cashless payment services utilizing NEC facial recognition technology in cooperation with Sumitomo Mitsui Financial Group, Inc.; Sumitomo Mitsui Banking Corporation; and Sumitomo Mitsui Card Co., Ltd.

Netwrix Corporation announced that Tesica Services chose Netwrix Auditor to secure customer data and comply with government requirements.

Ocularis 5.2, OnSSI’s VMS software, now integrates with Software House...
Join more than 2,500 security and law enforcement professionals from the public and private sectors to examine the critical security issues facing organizations and communities.

You’ll find:

- Free Expo admission—showcasing cutting-edge security solutions
- Top-notch education—hear from industry leaders on critical security issues
- Peer-to-peer connections—collaborate with colleagues and strengthen your professional network

Learn more at www.asisonline.org/nycexpo
C•CURE 9000 v2.40 and v2.50 security and event management system from Tyco Security Products.

Princeton Identity implemented an iris recognition system for access control at Brevillier Village residential retirement facility in Erie, Pennsylvania.

Razberi Technologies is partnering with ScanSource Networking and Security; ScanSource resellers in North America will now have access to Razberi ServerSwitchIQ video surveillance appliances.

ShadowDragon and DeliverFund are partnering to track criminals and free victims of sex trafficking.

Siellox LLC today announced a partnership with Milsk Company to serve as its manufacturer’s representative for the Ohio Valley region.

Tyco Security Products announced that Software House C•CURE 9000 now integrates with Guardian Indoor Active Shooter Detection System by Shooter Detection Systems.

GOVERNMENT CONTRACTS

Axon, a business unit of TASER International, announced that it received orders for its Axon Body 2 cameras from the Louisiana State Police, the Chattanooga Police Department (Tennessee), the University of Cincinnati Public Safety Department, and others.

The Office of Military Cooperation at the U.S. Embassy contracted with CH2M to design and deliver infrastructure and facilities enabling Kazakhstan to more effectively combat the illegal drug trade.

Digital Barriers plc, secured a contract with the U.S. Transportation Security Administration to enhance the capability of the Thruvis solution for detecting weapons and explosives concealed under clothing.

Hesco won the tender to become the sole supplier of 1-meter-high temporary flood defenses for the United Kingdom’s Environment Agency.

McMurdo, Inc., won a contract from the U.S. National Oceanic and Atmospheric Administration

National Environmental Satellite, Data and Information Service to provide fourth-generation search and rescue ground stations.

The U.S. Defense Advanced Research Projects Agency awarded Raytheon multiple contracts to research and develop technologies to detect and respond to cyberattacks on the U.S. power grid infrastructure. The U.S. Navy awarded Raytheon a contract for next-generation encryption devices to safeguard military tactical data transmissions.

California Public Utilities Commission approved a San Diego Gas & Electric proposal to construct the South Orange County Reliability Enhancement project that will improve electric reliability to its customers while enhancing public safety.

Utility, Inc., announced that the Fulton County Police Department in Georgia will equip its officers with its BodyWorn body cameras.

The U.S. Department of Homeland Security awarded an interoperability testing support contract to Valytics.

The Columbus Police Department in Ohio is deploying body-worn cameras from WatchGuard.

AWARDS AND CERTIFICATIONS

AMICO Security announced that its ANC fence system received an M5.0 security rating in compliance with the ASTM F2781-10 standard.

Arteco announced that its Open Connector is on the list of the Top 30 Technology Innovations from Security Sales & Integration Magazine because of its excellence in intuitive event management.

Chemimage Sensor Systems received a Platinum 2016 Technology Innovation Award for its VeroVision portable shortwave infrared hyperspectral imaging detection system from Military & Aerospace Electronics and Intelligent Aerospace publications.

Convergint Technologies was named the 2016 National Systems Integrator of the Year by Axis Communications.

EyeLock LLC released test results from Novetta certifying EyeLock performance supporting planned global deployments of its iris technology across IoT market segments.

The Regional Manufacturing Institute of Maryland recognized Galaxy Control Systems as a Champion of Maryland Manufacturing.
**MetricStream** was named Industry Innovator of the Year by *SC Magazine* in the category of Risk Management and Policy Management.

**NC4** was recognized as an Emergency Incident Management Systems champion by *Info-Tech Research Group*.

**NEC Corporation of America** took the honors as the Company of the Year at the *Frost & Sullivan* 2016 Growth, Innovation and Leadership Awards gala.

**SMP Robotics** announced that its S5 Security Robot won awards at *ISC East* in the Tech Tank and Featured New Product contests.

**Tyco Fire Protection Products** was honored by *American Security Today* with two ASTORS Homeland Security Awards. The SIMPLEX ES-Enabled Fire Alarm System was a Platinum winner for Best Fire & Safety System and a Gold winner for Best Mass Notification System.

**Veracity** won a Vision in Business for the Environment of Scotland 2016 Environmental Product or Service Award recognizing the company’s contribution to the environment through its products and approach to product lifecycle management.

**Viakoo** was awarded a U.S. patent for validating retention times of surveillance data.

A new patent for **Virtual StrongBox** recognizes its end-to-end enterprise IT–level security for financial institutions and other high-risk firms.

**ANNOUNCEMENTS**

**Bettafence** announced a rebrand of its corporate name to **PRÆSIDIAD** following its acquisition of **Hesco**.

**Bitdefender** joined the No More Ransom initiative supported by **Europol**, contributing to the global fight against ransomware. Bitdefender is offering free decryption tools to victims.

**Chubb** is offering an expanded suite of cyber loss mitigation services to help its U.S. and Canadian policyholders reduce the impact and likelihood of a cyber incident.

**COPsync, Inc.** launched a new corporate website at www.copsync.com.

Certain Mechanical Security businesses from **Stanley Black & Decker** will be purchased by **dormakaba** under a new agreement.

**The European Commission** is proposing to establish a European Travel Information and Authorisation System (ETIAS) to strengthen security checks on visa-free travellers. The ETIAS will gather information on visa-free travellers to allow for advance irregular migration and security checks.

The **Financial Services Information Sharing and Analysis Center** (FS-ISAC) and the **Monetary Authority of Singapore** (MAS) will collaborate to establish an Asia Pacific Regional Intelligence and Analysis Centre to encourage regional cybersecurity information sharing within the financial services sector.

**HID Global** acquired **Bluvision**, a Bluetooth Low Energy provider in the enterprise Internet of Things market.

**Security Line**, the official publication of the **Metropolitan Burglar & Fire Alarm Association of New York**, is no longer in print but is exclusively an online publication for members.

**Napco Security Technologies** released a new catalog.

**SnapAV** acquired video surveillance company **Visualint**.

**SOS Security LLC** acquired **Total Safety Inc.** to expand into the local patrol, response, and other markets.

**The University of Maryland Francis King Carey School of Law** created two new online master’s degree programs primarily for nonlawyers: a Master of Science in Cybersecurity Law and a Master of Science in Homeland Security and Crisis Management Law.

---

### 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>FLIR SYSTEMS, INC.</td>
<td>ACQUISITION</td>
<td>PROX DYNAMICS AS</td>
<td>The acquisition adds unmanned aerial systems capabilities to FLIR’s portfolio for expanded intelligence, surveillance, and reconnaissance applications.</td>
</tr>
<tr>
<td>INFOBLOX INC</td>
<td>COLLABORATION</td>
<td>QUALYS INC.</td>
<td>The two companies integrated their products to streamline vulnerability management, compliance, and threat remediation for enterprises.</td>
</tr>
<tr>
<td>IJET INTERNATIONAL INC.</td>
<td>ACQUISITION</td>
<td>RED24</td>
<td>Insurance expertise in kidnap and ransom, product safety, investigations, and background screening from RED24 will add to IJET’s risk management solutions.</td>
</tr>
<tr>
<td>TRUTAG TECHNOLOGIES</td>
<td>STRATEGIC PARTNERSHIP</td>
<td>CARSURIN</td>
<td>TruTag’s authentication solution and Carsurin’s network of inspection and certification capabilities in Indonesia will enhance brand and supply chain security.</td>
</tr>
</tbody>
</table>
SECURITY VIEW

S2 Magic Monitor Version 4 from S2 SECURITY of Framingham, Massachusetts, provides a unified security management user experience for access control, video surveillance, forensics, digital signage, and live Internet. New features include third-party video management system support, audio support, and advanced Internet widgets. It supports Milestone and exacqVision video management, in addition to S2 NetVR Series products. Real-time media from Twitter and Everbridge and enhanced weather radar maps bring tailored situational awareness into the security operations center and public areas. This version also enables integrators to monitor system health and control licensing and software updates online. 401

VIDEO EVIDENCE

COBAN TECHNOLOGIES INC. of Houston, Texas, released its new FOCUS Video Evidence Ecosystem and FOCUS X1 Body Camera. The ecosystem includes body cameras, in-car video systems, mobile video applications, and other intelligent devices that work together to deliver perspective and evidentiary value for officer safety and efficiency. The X1 Body Camera captures high-definition video, even in low light. Its battery lasts more than 12 hours between charges, and it offers pre-event recording, automatic wireless triggering, and multiple mounting options. Operation is simple and intuitive. It is compatible with COBAN in-car video systems, Android devices, and laptops for viewing, tagging, and uploading. 402

RFID READER

The XT-Mini RFID UHF Reader from TAGMASTER NORTH AMERICA, INC., of Tacoma, Washington, is an all-in-one vehicle access and security device. Designed to withstand demanding environments, it reads signals from up to 20 feet away. It has an integrated circular, polarized antenna and controller and can be used with an existing access control system using RS232, RS485, or Wiegand. Built-in red and green LEDs provide visual feedback that a tag has been read. UHF tags require no batteries and allow for hands-free access at gated communities, parking areas, and facility entrances. 403

REPEATER

The BE8216POE/REP repeater from BOLIDE TECHNOLOGY GROUP of San Dimas, California, extends Ethernet and power up to 300 feet, or users can cascade three of the devices to extend the connection up to 1,300 feet. The repeater provides real-time transmission without delay. With a built-in splicing slot and magnet hanger, it is designed for easy wall mounting and provides efficient connections between NVRs and cameras. 404

PORTABLE BARRIERS

DELTA SCIENTIFIC of Palmdale, California, upgraded its Portable MP5000 Barrier. A new universal voltage DC power unit allows efficient deployment in remote locations and areas with limited power options. The control circuit in the new Hydraulic Power Unit provides easy integration of various control options, such as keypads, card readers, key fobs, wireless transmitters, and computer networks. A new safety option provides self-contained infrared beams that will stop the barrier plate if a vehicle or pedestrian crosses the sensors. The mobile barriers tow into position and can be deployed in 15 minutes. 405
**GROUND SURVEILLANCE**

The GA1360 short-range sensor is the latest in the GroundAware family of reconfigurable surveillance sensors from San Diego–based DYNETICS. The device has a range of one kilometer and a 360-degree field of view. A single unit provides surveillance coverage of about 750 acres; the longer-range GA4120 senses up to 4 kilometers across a 120-degree field of view to cover about 2,000 acres. Both devices operate via Doppler S-band radar that detects intrusions and generates actionable data on potential ground-based threats. They integrate with cameras, video management systems, access control, and other systems. 408

**MOBILE VIDEO ACCESS**

VICON INDUSTRIES, INC., of Hauppauge, New York, released Vicon Valerus Mobile, an app for Vicon Valerus Video Management Software that allows users to access the VMS system from mobile devices. Users can watch live and recorded video from any device on the system. Flexible screen layouts display up to nine concurrent video streams. Users can also control pan-tilt-zoom cameras, including the presets. The app is available for free download from the Apple App Store and Google Play. 407

**ETHERNET MEDIA CONVERTER**

COMNET, Communication Networks of Danbury, Connecticut, introduced the ComNet RLMCS-FPPOEHO, a substation-rated and industrially hardened Ethernet media converter that supports Universal PoE (Power over Ethernet) powered devices requiring up to 60 watts of operating power. It is designed for deployment in environments with high levels of electromagnetic noise and interference and severe voltage transients and surges, such as electrical utility substations and switchyards. A user-selectable link fault pass-through provides remote indication of a network fault, and a summary fault alarm provides a local or remote indication via a dry contact closure in the event of loss of optical link or operating power. 406

**MOBILE ACCESS**

ISONAS INC. of Boulder, Colorado, launched a new mobile credential for access control. Pure Mobile gives users the ability to use their mobile phones as an authorized and secured credential for entrance to a facility. It works with the ISONAS Pure IP RC-04 hardware, leveraging its Bluetooth Low Energy feature. Pure Mobile provides another level of security to the platform with unique session keys during transactions. Credentials are non-transferable. 410

**ELECTRONIC LOCK**

SOUTHCO, INC., of Concordville, Pennsylvania, expanded its H3-EM Electronic Locking Swing-handle Series. The new H3-EM with Integrated Multiclass RFID Reader provides an integrated HID SE smart card reader and supports multiple readers, providing a high level of security and facilitating the transition to new security technologies used to manage access. It has LED indicators for visual status of equipment and also offers single-hole panel preparation. When connected to an access control system, the unit enables users to track and record access to the locks, providing an audit trail. 411

**BIOMETRIC ACCESS**

ZKACCESS of Fairfield, New Jersey, announced that its ZKBioPack software allows for the integration of ZKAccess biometric readers with Access It! access control software from RS2 TECHNOLOGIES of Munster, Indiana. RS2 customers can launch the ZKBioPack software application from the Access It! software interface when ZKAccess IP-based biometric readers are added. Administrators enroll biometric credentials (fingerprints or faces) using a device attached to the computer. Supported ZKAccess models include the F18 indoor fingerprint reader, TF1700 and TF1600 outdoor fingerprint readers, and the MB700 multi-biometric fingerprint and face reader. 409
MARKETPLACE

**BODY CAMERA ALERT**

**TASER INTERNATIONAL** of Scottsdale, Arizona, released the Signal Performance Power Magazine, a smart battery that works with TASER’s X2 and X26P Smart Weapons. It automatically notifies compatible Axon cameras that a TASER Smart Weapon within signal range is armed, the trigger is pulled, or its arc switch is activated. When cameras sense the status change, they start recording so officers don’t have to remember to start the camera. Axon Signal provides similar alerts from actions in a patrol car, such as light activation. 412

**PTZ CAMERA**

The Illustra Flex 2 MP PTZ camera from **TYCO SECURITY PRODUCTS** of Westford, Massachusetts, offers 20x optical zoom with continuous auto-focus, plus 10x digital zoom for effective video surveillance over long distances. The pan-tilt-zoom camera also features motion detection, wide dynamic range, automatic defogging, backlight control, and noise reduction. Outdoor models use 60-watt PoE+ power for easy installation. Each camera provides multiple streams of H.264 and MJPEG video compression for image clarity and efficient bandwidth management. The camera can be quickly configured via the Illustra Connect software tool. 415

**ATTACK-RESISTANT DOORS**

**ASSA ABLOY** of New Haven, Connecticut, announced that its door brands Ceco Door, Curries, and ASSA ABLOY Wood Doors offer attack-resistant openings that delay or thwart an attacker’s entry to a room. Ideal for classrooms, offices, and public buildings, this product line includes door, frame, and hardware, plus protective glass from School Guard Glass. The systems meet test standards for forced entry and ballistic-resistant levels of protection for various threats. While the door or glass may not stop a bullet from penetrating the opening, the door assembly can withstand an intense four-minute physical attack after being shot 60 times. 416

**KEY CONTROL**

**MORSE WATCHMANS** of Oxford, Connecticut, is improving its KeyWatcher Touch to make it more secure and more useful. For improved cybersecurity, the data between the KeyWatcher Touch and the KeyWatcher Touch server can be encrypted with AES256 technology with a pre-shared key that is definable on a site-by-site basis. The server service can run under a domain user account, and Windows authentication is now supported for SQL. The KeyPro III software was revamped to make it easier to use. Other enhancements include easier replacement of keys from the TrueTouch key tracking software, new notifications, and better control of reports. 415

**VIDEO MOUNT PRODUCTS** of Stevensville, Maryland, introduced a new 27-rack space equipment rack enclosure. The EREN-27ExK 19-inch enclosure features integrated cooling fans and lockable side panels. It houses multiple electronic components while protecting them from thermal damage, as well as vandalism and theft. The fully assembled unit is constructed of welded steel with a reversible tempered glass front door and a double-swing steel rear door. Front and rear rails are adjustable and threaded with standard 10-32 threading. The rack has top and bottom cable-routing knockouts and vents. 417
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 #41 securitymgmt.hotims.com
MARKETPLACE

SOLAR BATTERY PACKS
New solar battery packs from Larson Electronics of Kemp, Texas, help power lights, cameras, and other devices for long periods of time and in remote locations without access to electricity. The units come in different sizes and capacities, from 400 to 1,500 watt-hours. Unlike fueled generators, these cells can be deployed silently. They can be charged via a solar panel array, the electrical grid, or a generator. 418

VISITOR BADGES
Time-expiring visitor badges from Visitor Pass Solutions of Farmington, Connecticut, show security officers and passersby that a visitor’s badge is no longer valid. Over time, the badge changes color and displays a “VOID” message to prevent reuse and reentry. Fabric-friendly adhesive keeps the badge in place. The automatic change, which begins within six to eight hours, means that staff members do not need to collect badges from departing visitors. 419

IDENTIV, INC., of Fremont, California, launched uTrust TS Cards for excellent security at low cost. The high-frequency 13.56 MHz access card product line offers high-assurance identity and access card authenticity to both new and existing physical access control systems. They use new NXP MIFARE DESFire EV1 256B technology, which is specifically designed for physical access cards. TS Standard Cards are intended for new installations, while TS Migration Cards include 125 kHz proximity technology and support commonly used Wiegand card data formats. The uTrust TS Universal Enrollment station automates card number reading and enters cards into the access control system software. 420

PSIM SOLUTION
VISUAL MANAGEMENT SYSTEMS LTD. of Glasgow, Scotland, launched the newest addition to the TITAN VISION portfolio. Flexible, scalable, and secure, TITAN SIGMA provides all the elements of a physical security information management (PSIM) solution with emphasis on the detection and verification requirements of the installation and the command-and-control elements of a situational awareness application. It was specifically developed for sensitive, high-security, and mission-critical environments. It offers access to sophisticated analytical tools and intelligent self-learning technology, which further increases system efficiency and effectiveness. It integrates with nonsecurity applications such as point-of-sale, energy management, messaging, and HVAC to provide a fully tailored management tool. 421

EARN CPEs ANYTIME...ANYWHERE
UPCOMING WEBINARS
April 5  PREPARING YOUR HEALTHCARE FACILITY FOR ALL HAZARDS
April 19  ADA COMPLIANCE FOR SECURITY PROFESSIONALS
April 26  IDENTIFY AND RESEARCH THREATS VIA OPEN SOURCE INTELLIGENCE
May 3  FINANCE 101 FOR SECURITY PROFESSIONALS
May 17  BEHAVIOR DETECTION AND ASSESSMENT: PROTECTING MALL OF AMERICA
www.asisonline.org/webinars
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 #
--- | ---
15 | Abloy Security, Inc. 24
05 | Altronix Corp. 43
03 | Avigilon 08
03 | B.I.G. Enterprises 04
29 | Brownyard Group 48
20 | CEIA USA 31
28 | Cognitec 47
12 | Comport Technologies 21
13 | Comnet 23
01 | Dahua 02
08 | Detex Corporation 17
11 | dormakaba 19
22 | DSI (Designed Security Inc.) 33
43 | DSX Access Systems, Inc. 91
07 | G4S 13
19 | GAI-Tronics Corporation 29
33 | Garrett Metal Detectors 59
06 | Genetec 11
34 | Hanwha Techwin America 61
04 | Hikvision USA 06
36 | Horton Automatics 63
30 | LossPreventionSolution.com 49
44 | Mercury Security 92
41 | Mission 500 87
25 | NC4 41
09 | Par-Kut International, Inc. 18
17 | Quantum Secure 27
14 | Research Electronics, Int’l 24
18 | Safety Technology International, Inc. 28
37 | Security 2000 67
16 | Special Response Corporation 25
02 | Talkaphone 03
10 | TSCM America 18
23 | WM Security Services, Inc. (WMSSI) 37

ADVERTISERS ONLINE

Abloy Security, Inc. www.abloyusa.com
Altronix Corp. www.altronix.com
Avigilon www.avigilon.com
B.I.G. Enterprises www.bigbooth.com
Brownyard Group www.brownyard.com
CEIA USA www.ceia-usa.com
Cognitec www.cognitec.com
Comport Technologies www.comport.com
Comnet www.comnet.net
Dahua www.dahuasecurity.com
Detex Corporation www.detex.com
dormakaba www.dormakaba.com
DSI (Designed Security Inc.) www.dsigoa.com
DSX Access Systems, Inc. www.dsxinc.com
G4S www.g4sus
GAI-Tronics Corporation www.gatrincs.com
Garrett Metal Detectors www.garbrett.com
Genetec www.genetec.com
Hanwha Techwin America www.hanwhasecurity.com
Hikvision USA www.hikvision.com
Horton Automatics www.hortondoor.com
LossPreventionSolution.com www.losspreventionso.com
Mercury Security www.mercury-security.com
Mission 500 www.mission500.org
NC4 www.nc4.com
Par-Kut International, Inc. www.parkut.com
Quantum Secure www.quantumsecure.com
Research Electronics, Int’l www.reiusa.net
Safety Technology International, Inc. www.sti-usa.com
Special Response Corporation www.specialresponse.com
Talkaphone www.talkaphone.com
TSCM America www.tscmamerica.com
WM Security Services, Inc. (WMSSI) www.wmssi.com
THE FUTURE OF BACKGROUND CHECKS


Q. YOU WERE APPOINTED BY U.S. PRESIDENT BARACK OBAMA TO LEAD THE NBIB WHEN IT WAS CREATED IN OCTOBER 2016, AND THEN ASKED TO STAY ON BY PRESIDENT DONALD TRUMP. WHAT WERE THE MAIN ISSUES FOR YOU GOING INTO YOUR ROLE?
A. There were two big issues. One is, there is this backlog of background investigations that everybody refers to—it’s significant. That number is interesting, but it’s not the real number. The real number is how long does it take us to turn out an investigation? If we had a backlog of 5 billion cases, nobody would care as long as we were turning out the investigations on a timely basis. We aren’t, so we have an immediate problem to deal with which is to reduce the time it takes to get somebody a national security clearance.

The other piece is, what does the future look like? We’re operating with legacy IT systems; we’re operating with a process that dates back to before I was born. We have a good chance to reexamine that process of how do you initially determine whether somebody is trustworthy and...how do you continue to maintain that trust?

Q. THE NBIB WAS CREATED AFTER THE MASSIVE U.S. OFFICE OF PERSONNEL MANAGEMENT CYBER BREACH IN 2015. HOW IMPORTANT IS REBUILDING TRUST IN YOUR ABILITY TO KEEP THEIR DATA SAFE?
A. The worst thing I could do is lose any more data. The second worst thing I could do is make promises I can’t keep, so we have worked extensively with the chief information officer and other outside organizations—including the U.S. Department of Defense—to look at our system, as it is. A lot of work was done immediately after the breach—a lot of strengthening of the system—and I am comfortable that it is protected to a high degree.

But having said that, how do I convince the world? I don’t have a good answer for that right now other than we have to prove to them that we can protect it...Putting out a poster that says, “Trust Me.” I don’t know that that works. Our record’s going to reflect that.

Q. WHAT DO YOU SEE AS THE MAJOR CHALLENGES FOR NBIB IN 2017?
A. Related to the Trump administration, I don’t see any major challenges. There is a common thread that no administration wants people to betray trust, and administrations want us to have people who are cleared and trustworthy.

The real issue with anything is are things funded? This has been a perennial issue in security in general, ensuring that the amount of funding is there to make sure that the investigations can be done and that [the government agencies] can fund them.

And again, it’s not just what we’re trying to do at NBIB. The whole issue of protecting information globally by the government is absolutely critical. The last administration got it; I expect this one will get it.

I also don’t see any roadblocks to continuing the progress towards streamlining the process. I have every reason to believe that [Trump] will follow suit like every other administration. They want us to do this right, and we’ll get an opportunity to do it right.
CREATING THE FUTURE OF SECURITY... TODAY

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

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

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

**DSX Access Systems, Inc.**

**www.dsxinc.com**

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


For product info #43 securitymgmt.hotims.com
We’ve Done Vegas a Solid.

Open and easy to upgrade without locking you into a proprietary system. The tried and true standard where security is more than a requirement, it’s mission-critical.

Things move fast in Las Vegas, and securing your infrastructure shouldn’t run on luck. That’s why enterprises looking to maintain control, competitiveness, and peace of mind build their systems on the rock-solid, Authentic Mercury Access Control Platform.

Learn more. www.mercury-security.com