FRANK ARGENBRIGHT, SECURITY GUARD WANNABE
OUR GOAL: Recruit Quicker, Faster, Smarter People

As we grow and expand, I have been working to bring in the best and brightest people. Our Chief Executive Officer, Tom Marano, started with SecurAmerica in May of 2017. This is the third time Tom and I have joined forces, Tom having worked with me previously at AHL Services and AirServ. In 1995, I was $100 million in revenue with a goal to reach $1 billion in 10 years. So I used a national search firm to find someone who was quicker, faster, smarter than me. Tom helped exceed my goal when we reached $1 billion in revenue with 52,000 employees by 2000. Just bragging a little bit!

Tom worked at Apple Computer in the 1980s during its reorganization, working closely with both Steve Jobs and John Sculley. He aided in the corporate restructuring, the repositioning of the Macintosh Computer line, and eventually helped return Apple to profitability. During this time, Tom became a Silicon Valley insider, implementing innovative products and new marketing strategies that solidified Apple as a leader in the technology field. Prior to Apple, Tom served in a variety of operation and management positions at the Pepsi-Cola Company and Procter & Gamble.

Following Tom’s role at Apple, he was the Vice President of Sales and Marketing for the Coca-Cola Company during its global expansion in the 1990s. Tom received a BS in Research from the University of Virginia and an MS in Systems Management from the University of Southern California. Tom also is a US Army veteran, having served in the 25th Infantry Division for three years. Ever since I recruited Tom from the Coca-Cola Company in 1995, we have worked together to build several billion dollar businesses by delivering legendary service to our customers.

With Tom’s background, we can integrate new technology to disrupt the security industry and change the paradigm. We want to build a global security company by recruiting quicker, faster, smarter people. And remember, we want to be the best security company you have ever worked with!

Call me and let’s talk; my office line is 404-926-4202.
In today’s complex world, connections are more critical than ever.

Visit ASSA ABLOY to learn how you can connect to more of what matters most.

#connecttomore | IntelligentOpenings.com
“The cyber threat landscape is shifting in real-time, and we have reached a historic turning point.”

U.S. Homeland Security Secretary Kirstjen Nielsen about her department’s new cybersecurity strategy. PAGE 30

$850,000

Settlement paid by Goodwill Industries of the East Bay Area and an affiliate in a sexual harassment lawsuit brought by the U.S. Equal Employment Opportunity Commission. PAGE 64

151 yrs

Projected wait time for Indian immigrants with advanced degrees to receive a U.S. green card. PAGE 22

60+

Institutions that operate in the Texas Medical Center, the largest medical complex in the world. PAGE 42

“Our data suggests that the recreational use of marijuana is spilling into the workforce.”

Barry Sample, senior director of science and technology for Quest Diagnostics. PAGE 50

“We have townhall meetings and we do surveys, and the number one priority for parents is the safety of our schools.”

Mike Sholl, director of operations for Catoosa County Public Schools. PAGE 26
Quantum Secure’s SAFE software suite is now HID SAFE™ Enterprise.

The leading physical identity and access management software is now part of the HID Global family. HID SAFE™ Enterprise streamlines and automates identity management and compliance while providing operational analytics across multiple sites and systems in a single platform. Find out how to lower your risk profile and operational costs by visiting hidglobal.com/piam

NOW YOU’LL KNOW.

See us at GSX Booth 1737

For product info #3 securitymgmt.hotims.com
COVER STORY

34
FIVE NOT-SO-EASY PIECES
Project management requires foresight to anticipate future snafus. Breaking it down into systematic stages can help.

By Nicholas D’Agostino, PSP

HEALTHCARE
ORGANIZATIONAL HEALTH, INDIVIDUAL WELLNESS
A combined police and security department uses business practices and data visualization to protect two healthcare facilities.

By Lilly Chapa

PREEMPLOYMENT SCREENING
A SCREENING MINEFIELD
More and more job candidates in the United States are testing positive for marijuana. Should employers reconsider their hiring practices?

By Lilly Chapa

ESRM
HOW TO IMPLEMENT ESRM
A global corporation knew it needed to take a more proactive approach to security. Here’s how it did, using enterprise security risk management.

By Art Fierro, CPP

TRAVEL SAFETY
STREET SMAR T S
A personal travel security program empowers individuals to make quick, smart decisions in high-risk environments.

By Charles Goslin, CPP
A world of vital security news delivered to your inbox.

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

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

Check out the *Security Management* newsletters’ new features and design. To subscribe or resubscribe, e-mail ASIS International: [asis@asisonline.org](mailto:asis@asisonline.org).
10 CONTRIBUTING AUTHORS

12 SM DIGITAL
News and online resources.

14 EDITOR’S NOTE
Planning pays.

16 NEWS & TRENDS
Occupational fraud can be perpetrated by anyone from a line employee to a C-suite executive. Whoever the culprit, it is quite costly.
By Mark Tarallo

22 NATIONAL SECURITY
The green card application process is prone to delays and is lacking in technological functionality.
By Lilly Chapa

26 CASE STUDY
A Georgia School District uses an incident reporting tool to enhance situational awareness.
By Holly Gilbert Stowell

60 ASIS NEWS
GSX keynotes announced.

61 ASIS BOARD OF DIRECTORS

64 LEGAL REPORT
A university did not have a duty to prevent a student’s suicide.
By Megan Gates

68 INDUSTRY NEWS
By Flora Szatkowski

72 MARKETPLACE

73 ADVERTISER INDEX

74 SNAPSHOT
Terror attacks in Europe.

X30

CYBERSECURITY
By Megan Gates

EDITORIAL STAFF
Teresa Anderson
editor-in-chief
Teresa.Anderson@asisonline.org

Mark Tarallo
senior editor
Mark.Tarallo@asisonline.org

Megan Gates
associate editor
Megan.Gates@asisonline.org

Holly Gilbert Stowell
associate editor
Holly.Stowell@asisonline.org

Lilly Chapa
associate editor
Lilly.Chapa@asisonline.org

Flora Szatkowski
editorial assistant/staff writer
Flora.Szatkowski@asisonline.org

PRODUCTION & CREATIVE SERVICES STAFF
Tyler Stone
art director
Tyler.Stone@asisonline.org

Keith Schilling
manager, publishing production
Keith.Schilling@asisonline.org

Caitlin Donohue
graphic designer
Caitlin.Donohue@asisonline.org

Molly Fu
graphic designer
Molly.Fu@asisonline.org

Mariah Bartz
graphic designer
Mariah.Bartz@asisonline.org

Matthew Kreider
publishing specialist
Matthew.Kreider@asisonline.org

Pam Fischer
advertising production specialist
pam.fischer@asisonline.org

EDITORIAL OFFICES
1625 Prince Street
Alexandria, VA 22314
703/519-6200
fax 703/519-6299

EDITORIAL MISSION STATEMENT
Security Management is written primarily for security professionals. It also makes vital security information understandable to a general business audience, helping ASIS International advance security worldwide. Readers receive timely information on emerging security threats and practical solutions, which they can use to protect people, property, and information.

CHECK OUT MORE ONLINE at
www.securitymanagement.com
NICHOLAS D’AGOSTINO, PSP
SENIOR MANAGER
OF SYSTEM DESIGN
D’AGOSTINO & ASSOCIATES, LLC

Nick D’Agostino, PSP, designs physical security and technology systems for D’Agostino & Associates, an independent technology consulting firm. He is responsible for project management for the firm and is an expert in documenting and optimizing security, technology, and audio-visual systems for project owners, architects, and engineers.

His work includes spearheading system design and project management across many verticals, including K-12 schools, higher education, and city and municipality multifacility deployments.

D’Agostino is a member of ASIS and a board-certified Physical Security Professional® (PSP); he is also a Project Management Professional (PMP), a designation awarded by the Project Management Institute.

“Five Not-So-Easy Pieces”

PAGE 34

ART FIERRO, CPP
CHIEF SECURITY OFFICER
INTERNATIONAL PAPER

Art Fierro, CPP, is International Paper’s chief security officer, responsible for global enterprise security risk management. Formerly, he served as CEO of Ronin Cyber; executive vice president, security and safety, at Resilient Integrated Systems; vice president of global security at 20th Century Fox Film Corporation; and supervisory special agent for the FBI, where he worked in the fields of violent crime, white collar crime, cybercrime, counterintelligence, and counterterrorism over a 21-year career.

Fierro has been a member of ASIS International for 10 years and is a a member of the ASIS CSO Center. He also served on the ASIS Global Terrorism, Political Instability, and International Crime Council.

“How to Implement ESRM”

PAGE 48

CHARLES GOSLIN, CPP
PRINCIPAL AND OWNER
CG SECURITY ASSOCIATES, LLC

Charles Goslin, CPP, is a retired CIA operations officer and veteran of U.S. Army Intelligence. He has more than 35 years of experience in field intelligence operations, security and risk, and international business. He has worked and lived throughout Southwest Asia, Africa, Central and South America, the Middle East, and Europe.

Goslin provides program management and training on matters of intelligence and geopolitical risk, security, and threat. His book, Understanding Personal Security and Risk: A Guide for Business Travelers, was published last year by CRC Press. He is a member of the Houston Chapter of ASIS International.

“Street Smarts”

PAGE 54
DSI®
DESIGNED SECURITY, INC.
A Detex Company

Protecting Your Most Valuable Assets

Visit Designed Security, Inc.
Booth 2851
At GSX 2018 - Sept 24 - 27
Las Vegas, NEVADA

Turnstiles
Door Alarms
Tailgate Detection

WWW.DSIGO.COM - 800-272-3555

For product info #5 securitymgmt.hotims.com
EUROPEAN TERRORISM

INFORMATION SECURITY
The U.S. Department of Commerce’s National Institute of Standards and Technology issued a draft update to its Risk Management Framework to help organizations integrate information security principles and practices into enterprise risk management programs.

CYBER STRATEGY
The U.S. Department of Homeland Security released its cybersecurity strategy for the next five years.

SCHOOL SECURITY PLANS
A report from the U.S. Government Accountability Office evaluates the number of schools requiring hazard-specific plans, such as active shooter, suicide threat or incident, and bomb threats, among others.

GLOBAL FRAUD
Report to the Nations from the Association of Certified Fraud Examiners looks at 2,690 cases of fraud in 125 countries. It explores the costs, schemes, victims, and perpetrators.

“Go to SM Online for these and other links mentioned throughout this issue.”
NOTHING ESCAPES our customer service technicians. Not unique security problems. Not tricky installations. Certainly not inventory out your back door. Whether you need guidance with a challenging installation, are inquiring about training or want help making a hardware decision, you can access a team with nearly five decades of combined experience. A sharp mind will promptly help you secure a smart solution. Just call 800-729-3839.

LISTEN • DESIGN • BUILD • SUPPORT

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

DETEx.COM/MAx9

See us at GSX Booth 2851

For product info #6 securitymgmt.hotims.com
In December 1998, the U.S. National Aeronautics and Space Administration (NASA) launched the *Mars Climate Orbiter*. The unit was designed to land on Mars and undertake a scientific mission, including looking for water, monitoring the weather, and recording atmospheric effects. Once the mission was underway, however, NASA scientists discovered that a piece of software tasked with gathering critical information to guide the craft’s thrusters was recording and transmitting data in metric units. Ground control was using imperial measurements.

The unit entered the Martian atmosphere much lower than anticipated, and the $125 million project disintegrated.

In 2005, the United Kingdom announced that it would spend £285 million to build an airport on the small Atlantic island of St. Helena, roughly 2,500 miles east of Rio de Janeiro. However, when the airport opened in 2016, no commercial planes could take off or land from the facility. The volcanic mountain that dominates the island creates dangerous wind shear, making conditions treacherous for aircraft.

A 2017 House of Commons report on the airport noted that “while the airport has since handled a small number of flights, the wind conditions have precluded operation of the planned commercial service.”

In 2015, the U.S. city of Flint, Michigan, decided to change its water source from Lake Huron and the Detroit River to the Flint River to save $5 million. By January 2016, it became clear that the city’s residents were being poisoned by lead contamination. An investigation revealed that city officials failed to mandate the use of chemicals known as corrosion inhibitors. These chemicals keep lead and other heavy metals from leaching out of old pipes into the water supply.

While the full cost of the contamination has not been tallied, victims have filed lawsuits against city officials for the poisoning of thousands of children, and the city’s entire water system must be replaced.

Each of these costly mistakes could have been discovered and mitigated by implementing a thorough project management program. Though the process is not glamorous, it is effective at uncovering risks to the project, identifying a schedule, and organizing tasks and deliverables. All of these issues can be critical to a security project.

In this month’s cover story, “Five Not-So-Easy Pieces,” Nicholas D’Agostino, PSP, goes into detail about how security professionals can use project management techniques to ensure that a project is completed correctly, on time, and on budget. Using the example of a company replacing various legacy products with a new, unified security system, D’Agostino emphasizes: “In hopes of avoiding pitfalls, many organizations will hire project managers and consultants to spearhead alignment projects. This type of management, however, is usually complex and unpredictable work. Thus, one of the most useful attributes a security practitioner can have is experience in project management.”
INTEGRITY. QUALITY. RELIABILITY.

DSX SECURITY AT YOUR COMMAND... AND IN YOUR HAND.

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

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

DSX STANDARD SYSTEMS FEATURES INCLUDE:

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

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

See us at GSX Booth 1345
For product info #7 securitymgmt.hotims.com
The methods used by the culprits vary. Some skim cash from the reserves or walk away with inventory. Some alter numbers on payroll checks. And some pull off various embezzlement schemes, such as reporting false expenses or changing financial statements. The one commonality is that it is the organization’s own employees who are perpetuating the misdeeds. Sometimes they act in collusion with each other, and sometimes they act alone.

The findings come from Report to the Nations, an extensive study issued in April by the Association of Certified Fraud Examiners (ACFE). The study looked at 2,690 cases of fraud spanning 23 industries in 125 countries between January 2016 and October 2017. It is the tenth edition of the report, which ACFE issues every two years.

All told, the 2,690 cases of fraud resulted in losses that exceeded $7.1 billion. But the “true global cost of fraud is likely magnitudes higher,” the report’s authors write. ACFE estimates that 5 percent of worldwide business revenue is lost to fraud, which would come out to roughly $4 trillion annually.

“It’s safe to say the problem remains huge,” says John Warren, vice president and general counsel of ACFE and one of the authors of the report.

Given the magnitude of the losses, it’s not surprising that another report, this one focused on the United Kingdom and issued last year by Bottomline Technologies, finds that executive concern about internal fraud spiked in just one year’s time. In the Bottomline report, UK Business Payments Barometer 2017, the percentage of study respondents...
It’s not the person who looks sketchy. It could be the person who comes over to your house for dinner.

“Equally as concerning is that almost 60 percent of financial decisionmakers simply did not know whether they had been impacted by [internal] fraud or not.”

Occupational fraud, experts say, is an egalitarian crime; the culprit is just as likely to be a top executive as an obscure low-level employee.

“A fraudster doesn’t look like a fraudster,” Warren explains. “They look like everybody else. It legitimately could be anyone. It’s not the person who looks sketchy. It could be the person who comes over to your house for dinner on the weekend.”

When a fraudster is caught, coworkers are frequently shocked.

Historically, occupational fraud has been looked at as an accounting problem—numbers that don’t add up tip off company leaders that something is wrong, Warren says. But ACFE’s report shows otherwise.

“Part of our message is that it’s not really an accounting problem, it’s a behavior problem,” Warren says.

In every edition of the report, ACFE has surveyed 17 different “red flag” behavioral indicators that tend to be associated with fraudsters. “What’s fascinating is, every time we do the study, the same six rank highest,” Warren says.

Those six red flag behavioral indicators are: living beyond one’s means, financial difficulties, unusually close association with a vendor or customer, control issues and an unwillingness to share duties, divorce or other family problems, and a “wheeler-dealer” attitude or cultivated self-image. In at least 85 percent of the cases examined in the report, the fraudster displayed at least one of these red flags; in 50 percent of cases, he or she displayed multiple red flags.

Both male and female fraudsters exhibit these behavioral indicators, but often in different proportions, experts say.

“Studies in the past have shown that male perpetrators were more likely to be the wheeler-dealer-living-beyond-their-means type, whereas the women found themselves in some sort of financial distress and decided this was their easiest, or only, path for relief,” says Shannon Walker, a fraud expert who is founder and CEO of WhistleBlower Security Inc.

ACFE’s report bears out Walker’s view. For female fraudsters, the most common red flag by far is financial difficulties; it occurs in 40 percent of cases, compared with only 24 percent of cases for males. And for males, the wheeler-dealer red flag was present in 16 percent of cases, compared with only 6 percent of cases for females.

“It does look like there are differences in the reasons why women steal, as opposed to men,” Warren says. In addition, on average women commit smaller frauds than men do; losses tend to be 80 to 100 percent greater with men, he adds.

Experts also say that security efforts to prevent occupational fraud can turn helps the security community build more precise and effective countermeasures.

Soufan’s account is useful to the security community that is interested in gaining a more nuanced perspective of al Qaeda’s organizational development and the personalities behind it. He draws the reader in, using vivid, occasionally flowery, language, and makes characters out of al Qaeda members, such as “wily security chief” Saif al-Adel and “cold bureaucrat” Ayman al-Zawahiri. This approach makes the book an easy, engaging, and interesting read.

What compromises the book’s utility, at least in an academic sense, is that it is difficult for the reader to know where fact ends and fiction begins. Despite its “Note on Sources” and “Notes” sections, which are indeed helpful, Soufan provides few citations for direct quotations and perceptions of al Qaeda’s key players. The result is an interesting tale that requires the reader to conduct additional research to fact-check its contents.

REVIEWER: Margaret D.M. Barber is a national security researcher in the Joint Advanced Warfighting Division at the Institute for Defense Analyses.
benefit from an understanding of the motivations and conditions underlying the crimes. “Very few wake up in the morning and decide to rob their organization,” Walker says. “Many have pressures to perform at work, pressures at home, or are suffering from various addictions that inform their decisionmaking processes.”

Warren uses the “fraud triangle” model to explain the three conditions that are often present in occupational fraud incidents. First, the employee is under financial pressure. Second, he or she is given an opportunity to commit fraud, such as access to company resources. Third, the employee rationalizes the theft to him or herself. “They may think, ‘I was borrowing it, I was going to pay it back,’” Warren says. Or, employees may feel the company owes them because they deserved a promotion and never received it.

And if employees are on the verge of stealing, poor internal controls can help push them over the edge, Walker explains. “Certainly, lack of controls or oversight contribute to the opportunity for those at risk to take that first step and steal,” she says. “Once that wedge has been crossed, it becomes much easier for the fraudster to escalate.”

In fact, the ACFE study found that nearly half of frauds examined in the report occurred because of internal control weaknesses. For organizations that want to strengthen internal controls, Walker recommends maintaining consistent employee background checks before hiring; ensuring that sensitive duties are entrusted to more than one employee; implementing spot audit programs and conducting random audits on particularly vulnerable areas; and training employees about fraud prevention and the red flags they should be aware of.

The other key to occupational fraud prevention lies in organizational culture, experts say. Here, the tone is set at the top, Warren says. Organizational managers who always act ethically and treat all employees respectfully are leading by example; employees will often follow suit. “But if leadership is pushing the boundaries, and wading into that ethical grey area, people will take cues from that,” Warren says.

Walker agrees and says that some organizational leaders are taking steps to preempt bad situations by openly supporting a company code of conduct and ethics. “Complacency and lack of a strong tone from the top are two of the most key indicators as to whether you are at risk,” she says. “When management is seen as unengaged, unappreciative or apathetic, it creates an opportunity for a fraudster or potential fraudster to strike.”

CRITICAL RISK MANAGEMENT

PRIVATE SECTOR companies are not the only organizations that are embracing enterprise risk management. The U.S. government continues to do so too, albeit slowly. And recently, one U.S. federal agency released new draft guidelines on how risk management principles can be applied to critical infrastructure’s information systems. The proposed guidelines come from the U.S. Department of Commerce’s National Institute of Standards and Technology (NIST). For the last few years, NIST has worked on refining its Risk Management Framework (RMF), which is aimed at helping organizations integrate information security

SOURCE: A Study of the Pre-Attack Behaviors of Active Shooters in the United States Between 2000 and 2013, U.S. Department of Justice, June 2018
Canopies provide additional security by deterring attempts to climb over the turnstile and when integrating LED lighting units with twilight switch options.

Set your boundaries.

Our full height turnstiles with automatic bicycle door are electronically controlled in both directions and feature power assist operation.

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

Setting boundaries makes access in life smart and secure.

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

DORMA and KABA are now dormakaba. Visit dormakaba.us/PAS-SMMag

See us at GSX Booth 2525 For product info #9 securitymgmt.hotims.com
principles and practices into enterprise risk management programs. The RMF includes, among other components, a structured process for valuing organizational assets for selecting, implementing, and assessing security controls; and for monitoring security controls. Government officials say this RMF is especially necessary because threats to U.S. critical infrastructure are outpacing efforts to reduce vulnerabilities.

“There is an urgent need to further strengthen the underlying information systems, component products, and services that we depend on in every sector of the critical infrastructure,” writes Ron Ross, a NIST computer scientist, in the foreword of the new guidelines. The guidelines have seven objectives:

- strengthen the links between high-level risk management efforts and lower-level operational activities;
- institutionalize risk management preparatory activities; demonstrate how the RMF can be aligned with NIST’s Cybersecurity Framework; integrate privacy concepts into the RMF; promote the development of secure software systems; integrate supply chain risk management principles into the RMF; and provide an alternative approach to selecting security controls.

In addition, the new guidelines include instructions for tasks that will help prepare organizations to use the RMF for their information systems and programs. These tasks are divided into separate categories—organization level and system level.

On the organization level, these tasks include assigning risk management roles to employees, establishing an overall risk management strategy, assessing organization-wide risks, establishing and documenting baselines for stakeholder protection needs, categorizing the comparative impact levels of different information systems, and developing an organization-wide strategy for continuous monitoring.

On the systems level, the tasks include identifying the business mission that the system supports, identifying stakeholders that have an interest in the system, categorizing the types of information the system uses, conducting a system-level risk assessment, identifying the system’s protection and privacy requirements, and registering the system for purposes of management and oversight.

“Given the significant and ever-increasing danger of the threats, it is imperative that organizations remain vigilant and that leaders and managers at all organizational levels understand their responsibilities and are accountable for protecting organizational assets and for managing security risks,” NIST says in the guidelines.
If you are facing risk, we’d like to introduce you to something we call G4S Humanware. It’s a security principle that puts your interests first, and designs around you. We’ll help you identify risks, then utilize our software and hardware to design and implement security strategies to meet your needs. And we’ll back it up with the world’s most formidable guard force who are field tested, deployed in your environment, and keeping an eye on your business. By adding G4S Humanware to your security, we provide the most advanced defense against risk. One that’s made just for you.
NATIONAL SECURITY | IMMIGRATION

A recent series of federal reports reveals that the process for granting permanent residence to foreign nationals—commonly known as issuing a green card—is inefficient and stuck in the 20th century. The largely paper-based application process is riddled with inaccurate information, and the time it takes for an application to be processed is more than twice the U.S. Department of Homeland Security’s (DHS’s) stated goal time.

U.S. Citizenship and Immigration Services (USCIS), which operates under DHS, oversees the processing of more than 50 types of foreign national benefits, including green cards. An April 2018 USCIS report documenting the issuance of green cards to legal immigrant workers sponsored by their employers paints a grim picture: immigrants from India with advanced degrees, for example, have a projected wait of 151 years to receive their green cards.

Not all waits for green cards are so long—several factors affect the quantity and frequency of green card dispersion, including the category of visa through which immigrants apply, their country of origin, their family, employment or education status, and more. According to a March 2018 DHS Office of the Inspector General (OIG) report, USCIS field offices have an average completion time of more than...
A goal that does not reflect operational realities contributes to unmet customer expectations and reduces trust in USCIS.

seven months. The department’s goal completion time is four months, which is achieved in fewer than 3 percent of cases, according to the OIG report.

“Lawmakers, immigration advocates, and the public have raised concerns about how long USCIS takes to adjudicate green card applications,” the OIG report notes.

In addition, USCIS posts inaccurate green card application completion times on its website, which causes confusion for applicants and within the department itself. The OIG report found that the calculated date of when a decision will be made on an application is already six weeks out of date once it is posted on the website because it takes time to collect internal data.

“The information is confusing, unhelpful, and makes it very difficult to determine how long applicants can realistically wait for a decision,” the OIG report states.

The website can also skew a field office’s perceived rate of productivity. If a field office’s number of pending applications rises suddenly, it can move the calculated decision date backwards.

“This apparent lengthening in processing time may make a field office appear inefficient when the reality may be quite different,” the report states.

One example cited involved the Reno, Nevada, field office, which on the USCIS website appeared to have slow processing times—but was actually completing applications more quickly than the national average. Due to the office’s efficiency, USCIS shifted more applications from other offices to Reno, which caused the website processing time to spike and display an inaccurate calculation—for a while, Reno was showed to take an average of 518 days to complete applications, when it actually completed them in about 184 days.

The overall delay in processing applications may be a matter of perception as well, according to the OIG. Because the application process consistently takes twice as long as the USCIS goal time, the report states that it is unrealistic and should be reassessed. In efforts
to meet the current goal processing time, the department has spent $42.5 million in a five-year span for inspection service officers to work overtime to clear the backlog.

“USCIS has used temporary staffing assignments and overtime to keep processing times low, but it currently takes, on average, more than twice the amount of time,” the OIG report notes. “We believe USCIS is not meeting its 120-day goal because the goal itself is unrealistic given the complexity of adjudications and factors beyond USCIS’ control that affect the timeline. A goal that does not reflect operational realities contributes to unmet customer expectations and reduces trust in USCIS.”

THE COMING STORM

BY THE FBI. Video available on YouTube; youtube.com/watch?v=s9g5jB3Zxu4.

THE FBI RELEASED a short training video for law enforcement personnel titled The Coming Storm, which explores the sensitive and growing threat of school shootings. This video offers realistic images of a campus shooting along with timely warnings and advice from FBI experts. School administrators, security officers, and law enforcement personnel are just a few of the groups that will benefit from watching this video.

The video opens with a self-made video depicting a young student who feels victimized by others at his school. The scene shifts to a meeting where a group of school, FBI, and law enforcement personnel discuss the potential meaning of this video. The discussion presents a dilemma for law enforcement and school officials—how to protect individual rights while at the same time providing optimum security for the wider population.

During this talk, an actual shooting occurs at a local university. The FBI special agent and law enforcement officers rush to the scene, and the video depicts a realistic, though softened, account of a mass shooting.

The OIG wasn’t the only federal entity to investigate the green card application process. In a 2017 report, the U.S. Government Accountability Office (GAO) investigated just what is taking so long when it comes to processing green card applications—and whether the system ensures the integrity of the immigration process.

USCIS has been trying since 2006 to transform its current paper-based system into an electronic one but has faced management and development challenges—GAO notes that over the last 10 years, it has made 30 recommendations to address weaknesses in the program, 18 of which USCIS has complied with.

The so-called transformation program to create a software platform to process green card applications has experienced “significant cost increases and schedule delays,” GAO reports. The program’s most recent baseline indicates that it will cost up to $3.1 billion and be fully deployed by March 2019—that’s an increase of $1 billion and four years longer than previously thought. The program has been operating in breach—without a DHS-approved acquisition strategy and baseline due to exceeding a previous baseline—off and on since 2013.

“The program did not complete deployment of system functionality associated with its Citizenship line of business by its September 2016 deadline, resulting in another schedule breach,” says Carol Harris, director of information technology acquisition management issues at GAO. “Since then, we have reported that the program remains in breach. Until the program re-baselines, it is unclear whether USCIS still intends to fully deploy by March 2019.”

After the September 2016 breach, USCIS had planned to re-baseline the program in February 2017, but GAO reports that in December 2016, DHS leadership instructed the department to stop development on the project and instead develop a remediation plan. “DHS leadership elected to continue with the program’s pause in new development following program reviews in March 2017, July 2017, and October 2017,” GAO noted in a recent update. The program’s office also underwent a reorganization in January 2017. When asked if the pause in development was due to the new White House administration, Harris says that GAO did not investigate or report on the reason for revising the remediation plan.

The continual delays in deploying a fully electronic application system are impacting the ability of USCIS to realize the cost savings and benefits of the eventual transformation, GAO notes. Currently, legacy systems must remain operational until the electronic system is fully deployed. Even in 2014, GAO notes, it cost USCIS an extra $71 million to maintain both systems. And a previous software system that the
DISPLACED REFUGEES

Last year, 86.5 million people were forcibly displaced by war, violence, and persecution, reaching a record high for the fifth year in a row.

Where world refugees come from

- **Syria**: 6.3 M
- **Afghanistan**: 2.6 M
- **South Sudan**: 2.4 M
- **Myanmar**: 1.2 M
- **Somalia**: <1 M

**SOURCE:** United Nations High Commissioner for Refugees, June 2018

department spent eight years and $475 million to develop was decommissioned in 2016 due to its instability.

There are still serious questions about whether the new software—if or when it’s fully deployed—will solve the department’s backlog woes. GAO notes that by operating in breach status for so long and not addressing key practices for software development, USCIS risks deploying a system that does not meet its cost, schedule, or performance needs.

“It is more important than ever that USCIS consistently follow key practices associated with software development, systems integration and testing, and contract management and execute effective program oversight and governance,” the GAO report states.

OIG notes that a larger percentage of foreign nationals may be subject to interviews in the future, further lengthening the amount of time it will take to complete the green card application process. That report recommended that USCIS update its website to more accurately reflect the length of the application process and to reassess the current goal of 120 days, and the department concurred, noting that it will monitor processing times over the next year and consider a new goal time.

“The integrity of the citizenship process depends on careful adjudication of green card applications,” the OIG report states. “Given their responsibility and the consequences of their decisions, [information service officers] should continue to be given time to thoroughly vet applicants, especially if adjudicating green card applications becomes more complex.”

To view the reports mentioned in this article, visit SM Online.

CRITICAL INFRASTRUCTURE PROTECTION (CIP)

Secure – Cost Effective
Government CIP compliance, key connected with audits and time functions.

- IP68
- ISO 9001
- ISO 14001
- ISO 27001
- UL437
- ATEX

**SOURCE:** National Security C.indd 25 08/17/2018 1:33:22 PM
The public funding effort has helped further an environment of safety and security at local schools, says Mike Sholl, director of operations for the Catoosa County Public Schools. Catoosa County Public Schools, made up of 17 elementary, middle, and high schools, plus a performance learning center, is currently in the fifth phase of the ESPLOST funding. Sholl explains that community members were polled on how they would like to see the public education dollars spent.

“We have townhall meetings and we do surveys, and the number one priority for parents is the safety of our schools,” he tells Security Management. “So when we started ESPLOST V, that led us to implement all the safety initiatives we have.”

Those initiatives include collaborating with local law enforcement to prepare for emergency response, and a variety of technological solutions to support security. “We have door buzzing systems, we’ve added cameras to our schools, so we’ve spent a lot of time and money on making our schools as safe as we possibly can,” Sholl says.

The local sheriff’s office works closely with the district. There are plans to add live monitoring capabilities for police, allowing them to view events as they happen via campus cameras and provide dispatch. In addition, the district employs several school resource officers who either work full-time on a campus or divide their time among the schools.

Among Catoosa County’s top concerns is the possibility of an active assailant situation at its schools. It wanted to be able to quickly notify law enforcement and provide teachers and students with the ability to quickly react, all while following pol-
policies and procedures. The district knew investing in this type of solution would aid in all types of hazardous situations, including medical emergencies, natural disasters, and other incidents.

At a regional school safety conference in 2015, Catoosa discovered SIELOX CLASS (crisis lockdown alert status system), a daily incident and crisis reporting tool. The district chose Tiger Creek Elementary, one of its 10 elementary schools, as its test case for the product, and installed it in early 2016.

SIELOX CLASS operates via a Web or mobile interface that provides teachers or administrators with several customized options for sending different alerts, so it can be pulled up on any mobile device or computer. A dashboard with customized alerts allows teachers and administrators to perform a variety of tasks. Colored buttons make it easy to distinguish what type of incident is being reported, from a medical alert for the nurse’s office to a 911 call in a life-threatening situation.

“Our playgrounds are a good distance away from the school building. So—say a child gets injured on the playground, and could break a leg or an arm or hit his head or her head—that teacher can initiate the blue medical alert and get someone on the way out there,” Sholl notes.

Teachers use CLASS daily for their morning check-in to let administrators know that they and their students are in the building. In the event of an incident, a chat box will pop up for all CLASS users where communication can take place.

“An important part of bringing in SIELOX was communication, and the ability to check-in,” says David Beard, principal at Tiger Creek. “Each of the individual classrooms is represented by a different color and a different square, and we know the status of those rooms based on the color system that SIELOX uses.”

CLASS also gives first responders and administrators a clear picture of where students and teachers are at any given moment. “If teachers leave the building or take students off campus, they will use SIELOX CLASS to let us know that they are no longer on the premises,” says Braden Moreland, assistant principal at Ringgold Elementary, adding that...
it would help responders to know that they are not on campus in the event of an emergency.

The district also tied SIELOX CLASS to its cameras throughout the building, setting up an alert that would notify users of motion detection in a lockdown situation.

“We decided that we would like to use CLASS to detect motion in the building, so that if we did go into a hard lockdown there would be no traffic in the halls,” Beard says. “If everybody else is locked down and out of the building, the sheriff’s office has a good idea of where that perpetrator would be.”

The district regularly conducts drills for all types of hazardous scenarios, including its dangerous situation protocol, known as “Run, Hide, Survive.” With a panic button on the app, any teacher can initiate a lockdown at the school.

For enhanced situational awareness, the district incorporated camera views into the lockdown feature of CLASS.

“The teacher gets the popup that says ‘lockdown’ and gets a bullet list of instructions on what to do, as well as two camera views of the hallway outside their classroom,” Beard explains. “So, if he or she wants to do the run part of Run, Hide, Survive, he or she can see if there’s any danger outside the doorway, and then make that decision to run with the children. So that’s another layer we’ve added with SIELOX, and it works very well.”

The district notes that, thankfully, no lockdown procedure has ever been necessary outside of a drill. However, an accidental activation of the lockdown feature by a receptionist at an elementary school proved the value of the product.

“She was trying to log out and she accidentally hit the lockdown icon, and of course I immediately received a text and I was on the phone calling the principal,” Sholl says. “He went and found out that it was a false alarm, and within two minutes, the sheriff’s deputy had pulled into the campus, because he had been notified and dispatched to that school.”

The district plans to have SIELOX CLASS deployed at all 17 schools by the end of the 2017–2018 school year.

“CLASS provides a very quick response and gets the word out very quickly to lots of people,” Sholl says. “The accidental lockdown just proved to us that it’s very efficient and works how we want it to work.”

FOR MORE INFORMATION:
Karen Evans, karen.evans@sielox.com, www.sielox.com, 856.861.4568

### STATS

**NUMBER OF U.S. STATES THAT REPORTED REQUIRING HAZARD-SPECIFIC PLANS**

<table>
<thead>
<tr>
<th>District-Led Plans</th>
<th>School-Led Plans</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bombs or bomb threats</td>
<td>17</td>
</tr>
<tr>
<td>Chemical, biological, or radiological threats or incidents</td>
<td>17</td>
</tr>
<tr>
<td>Active shooter</td>
<td>15</td>
</tr>
<tr>
<td>School bus accident</td>
<td>15</td>
</tr>
<tr>
<td>Suicide threat or incident</td>
<td>14</td>
</tr>
</tbody>
</table>

**SOURCE:** Analysis of State Educational Agencies Survey, Government Accountability Office, March 2016
FREE Expo-Only Pass!

XPERIENCE
the next generation of exhibits

• 550+ Exhibitors
• X Learning Stages
• D3 Xperience
• Career HQ
• Headshot Studio
• NEW! Career Fair
• ASIS Hub
• Con-X-tions Lounge
• Innovative Product Awards
• International Trade Center

THURSDAY BONUS: Get special access to the keynote and enjoy lunch in the exhibit hall

REGISTER FOR YOUR FREE EXPO-ONLY PASS ➤ GSX.org/Expo
Promo Code GP41
#GSX18
The cyber threat landscape is shifting in real-time, and we have reached a historic turning point,” said DHS Secretary Kirstjen Nielsen in a statement on the strategy’s release. “Digital security is now converging with personal and physical security, and it is clear that our cyber adversaries can now threaten the very fabric of our republic itself.”

Between 2006 and 2015, the number of cyber incidents on U.S. federal government systems that were reported to DHS increased more than tenfold—including the massive Office of Personnel Management breach that compromised the records of more than 4 million U.S. federal employees and affected 22 million people.

“The growing interconnection of cyber and physical systems within critical infrastructure also creates the potential risk for malicious cyber activity to result in direct physical consequences,” according to DHS. “For example, the December 2015 overriding of controls in the Ukrainian electric grid resulted in widespread loss of power.”

ON MAY 15, 2018, the U.S. Department of Homeland Security (DHS) released its cybersecurity strategy for the next five years.

“The cyber threat landscape is shifting in real-time, and we have reached a historic turning point,” said DHS Secretary Kirstjen Nielsen in a statement on the strategy’s release. “Digital security is now converging with personal and physical security, and it is clear that our cyber adversaries can now threaten the very fabric of our republic itself.”

More recent incidents, such as WannaCry and NotPetya, have also demonstrated the threat of using the Internet of Things to conduct cyberattacks with far-reaching consequences.

Because of this, Nielsen said DHS is “rethinking its approach” to cybersecurity to confront systemic risks by issuing its strategy guide. The guide was a requirement under the National Defense Authorization Act of 2017 and lays out a five-part approach to manage national cyber risk: identifying risk, reducing vulnerability, reducing threat, mitigating consequences, and enabling cybersecurity outcomes.

“Through our efforts to accomplish seven identified goals across these
five pillars, we work to ensure the availability of critical national functions and to foster efficiency, innovation, trustworthy communication, and economic prosperity in ways consistent with our national values and that protect privacy and civil liberties,” DHS said.

To understand the cybersecurity landscape and its risks, and address vulnerabilities, threats, and consequences of DHS’s cybersecurity activities, the department must first be able to identify risks.

The department’s first goal in its pillar of its strategy is to assess cybersecurity risks so it understands the “evolving national cybersecurity risk posture to inform and prioritize risk management activities,” according to the strategy.

To do this, DHS said it plans to work with stakeholders—sector-specific agencies, nonfederal cybersecurity firms, and others—to understand trends in threats, vulnerabilities, interdependencies, and potential consequences so the department can prioritize its activities and budget accordingly.

“DHS must also take stock of gaps in national analytic capabilities and risk management efforts to ensure a robust understanding of the effectiveness of cybersecurity efforts,” the strategy explained. “We must anticipate the changes that future technological innovation will bring, ensure long-term preparedness, and prevent a ‘failure of imagination.’”

As part of this goal, DHS has set specific objectives, including identifying evolving cybersecurity risks that affect economic security, public health, and national security; identifying and creating plans to address gaps in analytic capabilities; and developing plans and scenarios for future technology deployments that could be disruptive.

Another pillar of DHS’s strategy is to reduce the vulnerability of U.S. federal agencies across the board.

“DHS leads the effort to secure the federal enterprise and must use all available mechanisms to ensure that every agency maintains an adequate level of cybersecurity, commensurate with its own risks and with those of the larger enterprise,” according to the strategy.

To assist the rest of the U.S. federal government, DHS will work with the Office of Management and Budget (OMB) to address systemic risks and interdependencies between agencies.

“DHS must also support agency efforts to reduce their vulnerabilities to cyber threats by providing tailored capabilities, tools, and services to protect legacy systems, as well as cloud and shared infrastructure,” the strategy explained. “Within its own systems, DHS must continue to adopt new technologies and serve as a model for other agencies in the implementation of cybersecurity best practices.”

As part of this pillar, DHS laid out sub-objectives to more clearly define how it will achieve this goal. These include developing and implementing a clear governance model for U.S. federal cybersecurity; issuing new or revised policies and recommendations to ensure adequate cybersecurity across the enterprise; and providing agencies with integrated and operationally relevant information necessary to understand and manage their cyber risk.

One example of this in action prior to the release of the strategy was DHS’s binding operational directive 18-01, which required U.S. federal agencies to increase their email and Web security. Specifically, DHS mandated that agencies implement Domain-based Message Authentication, Reporting,

FINANCIAL INVESTIGATIONS

BY RONALD L. MENDELL.
Charles C. Thomas; ccthomas.com; 242 pages; $35.95.

THIS WELL-ORGANIZED publication is a worthwhile resource for anyone who is charged with conducting financial asset investigations. Laid out in a logical fashion, the fifth edition of How to Do Financial Asset Investigations goes into just the right amount of detail for each covered topic.

Information gathering is becoming in many ways more difficult due to privacy concerns and data breaches that occur seemingly daily. Conversely, informational media are rapidly growing, and author Ronald Mendell stresses the need to compare online resources against print sources, human sources, and other available sources to corroborate the information.

This book lists several resources for gathering information, many of which are commonplace and should be known even to the novice investigator. However, some of the sources listed by the author are not so well known and provide excellent repositories of information. Mendell makes a good point regarding consciously using a commonsense approach for natural language searches when using the Internet as a tool. He correctly indicates that the searcher must stay up to date regarding the various websites and other resources. It is imperative for the investigator to think beyond blindly using the same static lists, because websites are constantly changing.

A fictional case study illustrates how to tie together other bits of information with public data. He uses this example to emphasize the numerous sources of information and the added value of link analysis software. The author discusses how the discovery of prior litigation for the targets of investigation may prove invaluable.

In summary, this book is well conceived and accomplishes its stated intent. The experienced investigator will be reminded of many sources that can be used every day. The novice investigator will learn about specific sources of information and how to analyze data. This useful and well-written book will prove to be an excellent resource.

REVIEWER: James E. Whitaker, CPP, PCI, CFE (Certified Fraud Examiner) has more than 45 years of experience in investigations. He serves on the ASIS International Healthcare Council and the PCI Review Course faculty.
and Conformance (DMARC) for their email systems. (See “Spoofing the CEO,” Security Management, October 2016.)

Another goal of this pillar of the strategy is to protect critical infrastructure by partnering with stakeholders to ensure national cybersecurity risks are managed. This partnership is key because a majority of the critical infrastructure in the United States is owned and operated by the private sector.

“DHS must partner with key stakeholders, including sector specific agencies and the private sector, to drive better cybersecurity by promoting the development and adoption of best practices and international standards, by providing services like risk assessments and other technical offerings, and by improving engagement efforts to advance cybersecurity risk management efforts,” the strategy stated.

An example of this in action was DHS’s response to the 2017 WannaCry ransomware attack. During the attack, DHS’s National Protection and Programs Directorate partnered with other agencies and the private sector to help U.S. hospitals—a major target of WannaCry—ensure their systems were not vulnerable to the malware. It also released an unclassified technical alert to help defenders defeat the malware and prevent its spread.

In addition to reducing vulnerability, DHS’s strategy also outlines a goal to reduce threats in cyberspace overall.

“In partnership with other law enforcement agencies, DHS must prevent cyber crime and disrupt criminals and criminal organizations who use cyberspace to carry out their illicit activities and leverage identified threat activity and trends to inform national risk management efforts,” the strategy explained.

To do this, DHS will create investigative priorities related to illicit cyber activity, identify and conduct high-impact investigations of cybercrimes by transnational criminal organizations, disrupt online marketplaces for malicious cyber activity, and develop options to disrupt, counter, and deter transnational criminal organizations.

The final portions of the DHS strategy are to mitigate consequences and enable cybersecurity outcomes.

With the rise of cybercrime and illicit cyberactivity, DHS must have a role in

---

We must anticipate the changes that future technological innovation will bring.
limiting the impact of significant cyber incidents, the department said.

“Many cyber incidents do not require a national response,” the strategy explained. “But when they do, DHS plays a unique role in responding to cyber incidents to mitigate potential consequences by providing technical assistance to affected entities and other assets that are at risk and investigating the underlying crimes.”

DHS took this role, for example, in July 2017 when the U.S. Secret Service—part of DHS—worked with international law enforcement to arrest a Russian national who allegedly operated BTC-e.

“From 2011 to 2017, BTC-e is alleged with facilitating over $4 billion worth of Bitcoin transactions worldwide for cyber criminals engaging in computer hacking, identity theft, ransomware, public corruption, and narcotics distribution,” DHS said. “Researchers estimate approximately 95 percent of ransomware payments were laundered through BTC-e.”

While the strategy is an important framework for the U.S. federal government, it has been met with criticism. Ray DeMeo, chief operating officer of Virsec, says the DHS strategy is high-level and is missing an implementation plan.

“One of the document’s guiding principles is to foster innovation and agility—this is a big ask, where existing time horizons must be reduced from years down to months,” DeMeo says. “We need to dramatically accelerate collaboration with the private sector, where meaningful security innovation is happening daily, if we are going to change the asymmetric nature of today’s threat landscape.”

DeMeo also says he will be looking for more information from DHS—a department with a domestic mandate—about how it intends to address cybersecurity globally.

“The reality is that a large portion of Internet crime is driven from the international Wild West, from areas with lax law enforcement or actional nation-state sponsorship,” he explains. “This problem is as much diplomatic as it is technological.”

Two of the most vocal critics have been U.S. Representative Bennie G. Thompson (D-MS), ranking member of the House Homeland Security Committee, and U.S. Representative Cedric L. Richmond (D-LA), ranking member of the Cybersecurity and Infrastructure Protection Subcommittee and author of the legislation that originally mandated the strategy.

In a joint statement, Thompson and Richmond said the strategy is overly focused on policies and procedures that DHS needs to develop further.

“It also fails to mention—at any point—one of the most pressing cybersecurity challenges of the moment: election security,” they said. “The fact is, because of the department’s failure to adhere to the statutorily-mandated deadline, it lost time and missed opportunities to make progress maturing its cybersecurity posture and capabilities.”

The congressmen added that they hoped to see more information about how DHS plans to implement its strategy in another report, which is due to Congress by August 15, 2018.

“In particular, we expect it will provide greater detail on the roles and responsibilities that components will undertake, a description of any new authorities it needs to fulfill its mission to secure federal networks, as well as an explanation of what resources the department will need,” Thompson and Richmond said.

As of Security Management’s press time, DHS had not submitted an implementation plan to Congress.
Project management requires foresight to anticipate future snafus. Breaking it down into systematic stages can help. Here’s how.

Alignment is in. Many cities, municipalities, corporations, and school systems are taking steps to align their physical security systems so that security programs across locations will be fully integrated.

The benefits of such a move are numerous. Uniformity across systems makes it easier for end users, and converged systems are easier to manage from operation centers. Moreover, having only one system makes maintenance and upgrades easier, and this can help provide long-term stability.

But achieving alignment is no easy feat. Navigating a physical security installation across several facilities can be a difficult undertaking; often, such a project includes wrangling a mish-mash of individual products to get them to function under one cohesive system. Alternatively, some take the approach of completely redesigning the physical security system so that it reflects current best practice design standards. Both paths can be difficult.
In addition, the potential pitfalls of attempting a unification project are numerous. What is the installation environment in each facility? Which key players need to be involved at each facility, and at what level of involvement? What type of network infrastructure must be in place to integrate the systems?

In hopes of avoiding pitfalls, many organizations will hire project managers and consultants to spearhead alignment projects. This type of management, however, is usually complex and unpredictable work. Thus, one of the most useful attributes a security practitioner can have is experience in project management.

Although there is no one roadmap for successful project completion, and despite all the caveats, most projects can be broken down into five stages. The main purpose of this article is to walk the reader through these stages, which experts sometimes refer to as “process groups.” The five process groups are initiating, planning, executing, monitoring and controlling, and closing. For our purposes, the second process, planning, can be considered the design process, and the third process, executing, can be considered the installation process.

Although these stages will remain consistent, the role and scope of a project manager’s responsibilities will change from project to project. And, there may be many project managers on a single project: one for the design team, one representing the owner, one who serves as an installation project manager in the field, and others. Each will have different responsibilities.

Primarily, this article is written from the point of view of the project manager who is outside of the organization and is hired by an owner to design and manage a project that will be installed by a third-party contractor, either through a public bid or the solicitation of proposals. Typically, this type of manager would be a consultant who works on a project-by-project basis with different teams and organizations, for the procurement and installation of a multi-facility physical security system.

However, the concepts and best practice guidance offered here could be applied to almost anyone involved with the management or supervision of physical security projects, whether that person is inside or outside the organization.

Initiating

As a project kicks off, the act of project management is often the act of discovery. The project may be ill-defined, just a blurry picture of the needs and goals of the project’s owner. But an ill-defined project cannot be effectively managed, so it is often the project manager’s task to focus the project with the owner into a clear and actionable roadmap.

For the project manager, one of the main goals of the initiating process is to get up to speed with the requirements, history, and expectations of the project. This includes understanding who the project stakeholders are and determining the project’s requirements, constraints, and assumptions.

Physical security projects can be sponsored by a range of departments in an organization, including security, facilities, IT, finance, and general management. But these departments may have different levels of familiarity with physical security systems, so the project manager must gain an understanding of how well the owner’s team knows physical security. This understanding should then inform the project manager’s general approach, including the process of assembling the design team.

This understanding can be gained during the meetings that take place during the initiating process. For example, the design or project management teams may be akin to experts—they will design and demonstrate how the systems work and function together and explain design best practices. In another
Another key task of the initiating process is to learn the requirements and goals of the project. What is the general scope? What physical protection systems will be affected? Will this be a replacement project, or will it integrate with existing systems? Is there a deadline for installation completion? If grant money is involved, is there a deadline for spending funds? Each answer is part of the roadmap.

Once the initially hazy picture has come into focus, the project manager may take the next steps. These include developing a rough estimate of how many days will need to be spent in the field documenting existing conditions and systems, and how many designers should be hired to create design documents. Other decisions involve who will sit on the project stakeholder’s team, whether the owner will require manufacturer demonstrations, and what a reasonable cost for the project looks like.

During this stage, the project manager may discover that the existing team of stakeholders is inadequate. In this case, the project manager should try to ensure that all decision makers are included, and that, if applicable, teams not directly associated with security are also represented, or at a minimum made aware of the project. Other stakeholders, for example, could include facility directors, senior management, service providers, IT teams, and grant funding representatives. If the project is for a municipal, city, or public organization, the owner may prefer to involve law enforcement in the early stages and throughout the process.

By the end of this first stage, all stakeholders should understand their roles within the project, what will be expected of them, and the type of work that will be performed on their systems or the facilities they manage. Accomplishing this early is important. It is never a good idea to inform an IT director of an IP video surveillance project a week before the network electronics are scheduled to be installed.

**Design**

The greatest indicator of a well-executed project is a well-executed design process. The overall objective of this process is to create a complete set of project documents that a third-party contractor or integrator can then use to create a proposal or bid.

These documents, typically referred to collectively as the project manual, will typically include plan drawings, wiring diagrams, and riser and elevation drawings. They also include specifications explaining the scope, the installation standards, the configurations of various systems, and other pertinent information. Front-end documents in the manual often describe the nature of the project and any general requirements that the bidding contractor must adhere to.

To create a thorough project manual, it is important for the project manager to assemble a qualified design team. Physical security projects can be derailed by subpar designs that do not consider each facet of each system’s requirements. The design team must be able to accurately document the correct configuration requirements among systems; all installation best practices and requirements; the code requirements and testing parameters; and the closeout tasks such as training.

Once the design team is assembled, the project manager begins the process of creating progressively more detailed designs and reviewing them periodically with the owner. A good guide is to review the design documents at 50 percent completion, 75 percent, 98 percent, and 100 percent. At each review, it should be conveyed to the owner what was refined, changed, omitted, or added from the last review.

The overall cost and the installation schedule should also be reviewed at those junctures. Most likely, the project will have a specific budget and installation schedule that the design team must adhere to. At each design milestone, the project manager must ensure that the owner understands the budget and schedule. Any major design change should be reviewed with the owner.

If the project does not have a predetermined budget, the project manager should have a usable estimated cost range after project initiation. At the halfway point, an estimate within a few percentage points of the actual cost should be completed and reviewed with the owner. It is also important the owner understands how any future requests will affect the budget and installation schedule.

Ideally, the project should leave 10 percent of the total budget in contingency to cover unforeseen costs. For example, for a project with a budget of $1 million, the design team should allocate up to $900,000 and leave $100,000 for contingencies. Aside from this practice, some projects also contain a management contingency designed to cover changes in project scope directed by management. However, this contingency may or may not be shared with the project manager, and it may not be included in the total project budget.

When it comes time to estimate individual costs, the environment and condition of existing facilities should be kept in mind. Areas likely to add surprise costs to the project should be reviewed. Take ceilings, for example. If
the facility has open ceilings, will the low-voltage cabling need to be run in conduit? If so, how much cost will that add? Or, consider data closets. Is there adequate wall space to mount patch panels, switches, and servers? Is there wall space to mount security panels? Other areas that should be reviewed for cost impact include power requirements, configuration fees for integrating systems, and software fees for updating out-of-date systems, among other items.

Taken together, the overall goal of the planning and design process is to create a project manual that is fair to both the owner’s needs for attaining the project goals, as well as the contractor’s needs to correctly price the project.

Many potential headaches that could occur during the installation process can be mitigated by giving the contractor a realistic schedule for procurement and installation of the systems, and by ensuring that the project comes in at or under budget. This is done by informing the owner early and often of the realistic requirements that the scope of the project will require. All cost-saving measures should be considered during the design process when at all possible.

Throughout the design process, the project manager and design team should constantly ask themselves, “If I were a contractor, would I be able to properly price this project based on the project manual documents without adding change orders in the field?” Many projects are soured by an incomplete project manual that puts the contractor in the disadvantaged position of having to constantly submit change orders to correct their fee.

During the executing process, the contractor who was awarded the project proceeds with installing and testing the systems. Sometimes the project manager and design team stay on to manage the schedule and invoices, review the installation and test results, and generally ensure that that the project is being installed to the quality standards documented in the project manual on behalf of the owner.

The relationships among designers, consultants, project managers, and contractors should be built on teamwork and based on the shared goal of providing the owner with a well-executed project and physical security system. The best projects are those where a mutual respect and a spirit of genuine collaboration are exhibited by all parties and where the project manager has the best interest of all parties in mind.

Although, careful initial documentation of exactly what is expected of the installation will help avoid oversights and miscommunications, it is still prudent, and often mandatory, for the project manager to review and approve the work being completed. During this process, the manager’s best strategy for ensuring that the project is executed well is to stay vigilant in correcting all possible holdups.

If the overall budget fails to capture all installation costs, change orders can occur during the installation process, after the project has been awarded to a contractor. A change order is a claim to a change in scope that usually comes with an associated cost. It is used by the contractor to seek fees for the change. Change orders can be owner directed or project directed, and they can be legitimate or illegitimate.

Here’s an example of a legitimate, owner-directed change order. After a project manual went out to bid and the project was awarded to a contractor, the owner requested to add access control hardware to a door. This hardware was not included in the design, so the contractor was not allowed to give a cost associated with it. Seeking a fee to now include that door in the installation was a legitimate change order.

Here’s an example of a legitimate project-directed change order. The contractor discovered that 100 feet of conduit was needed to mount a video surveillance camera in an open-ceiling mechanical space. The project manual did not clearly document that the contractor would need conduit at this location, so the contractor sought to submit a change order for the cost of procuring and installing the conduit.

Illegitimate change orders occur when a contractor seeks fees for a task or product that was clearly documented in the project manual and, therefore, should have been included in the proposal or bid. It should be noted that legitimate or illegitimate status will not determine if the change order will be accepted by the project. Change order acceptance or rejection is determined by
the project manager, owner, and other applicable stakeholders.

One benchmark of success for the project is the number and scope of change orders. In other words, how close was the executed project to the agreed upon budget and original design?

Monitoring and Controlling
If the project manager’s responsibility is to review and sign off on the installation, it is best to do so early and often. The goal is to correct minor issues before they grow into major issues.

For example, let’s assume a contractor completes a 200-door access control project across 20 different facilities, but does not properly secure the cabling above the ceiling grid as designed. The longer the project manager waits to get on site and review the work, the more difficult it will be to fix this mistake. If the cabling contractor is a subcontractor of the prime contractor and is finished with the scope of work, by the time the project manager is on site to review the work, it may be impossible to correct these mistakes.

The project manager should be on site to review, at a minimum, the first few devices that are installed to ensure that the installation is clean and to specification. Indeed, many contractors prefer this method of installation kickoff because it will ensure that the installation is on the right track.

Common installation mistakes found on physical security projects can include sloppy or exposed cabling to devices; installation of sensors, cameras, and other devices that are not plumbed or properly secured; low-voltage cabling strung across the ceiling grid and not on cabling support; failure to firestop applicable penetrations; and poor cable management and cable terminations in the data closets and control panels, among other things.

All site visits, communications between owner and contractor, issuances of work that need to be fixed, and approvals of work done correctly should always be formally documented and distributed to the entire team in field reports and punch lists. In turn, the contractor must document any corrections or installation requirements that are completed.

Requests for information from the field, product submittals, invoice submittals, and general project housekeeping should be reviewed and answered by the project manager in a timely matter to ensure that the project is not delayed due to lack of direction for the contractor or owner.

Sometimes, the biggest roadblocks to completing a project on schedule...
are the tasks that must be completed by the owner. It is important that the project manager also manage this side of the project. He or she should inform the owner early and often when tasks will be due and should sometimes advise them on how they can be best completed. These tasks may include providing IP addresses for cameras, printing and issuing badges for new access control systems in time for system cutovers, providing configuration on network electronics if required, and configuring and relaying information related to VLANs, among other things.

Often, contractors are only allowed to invoice for work completed or for devices that were purchased and delivered to the facility. If the project manager is tasked with reviewing invoices, it should be easy to approve or reject fees based on work completed because the project manager has periodically seen and reviewed the work in person.

Most projects will require that the project hold a retainer against the contractor’s fee until the project is 100 percent complete. This retainer is held until the end of the project, after all the installation and miscellaneous responsibilities of the contractor have been met. Each project may have specific requirements in terms of payment and proof of work for payment that should be reviewed and adhered to by all parties.

Closing

The closing process can be initiated when 10 percent of the project is left to complete. Common tasks to be completed during the closeout process include administering training, delivering operation and maintenance manuals, final testing of systems, reviewing the system test results, reviewing cabling test results, and handing over the systems to the owner.

It is a good idea to start closeout tasks when the project is around 75 percent complete. However, getting the owner and relevant stakeholders together for training and closeout meetings can be a difficult task depending on their schedules. If the project is being completed in a school district, for example, training may need to wait for a professional development day, so it is best to book training as soon as the trainer is available.

Depending on the owner’s level of expertise, it may also be beneficial to include additional training in the project manual two to six months after the project is handed over to the owner. This will allow the owner to schedule refresher training if desired.

Once the project manager and design team accept the final installation; all closeout deliverables are finalized; and all final fees, contingencies, and invoices are paid; the project is handed over to the owner and the project is considered complete.

Successful project completion requires improvisation, teamwork, thoroughness, and foresight. All are skills that are developed over time and through hands-on experience on projects of different sizes and types. The best project managers are those who learn from their mistakes, document their lessons learned, and share those insights with the project management and security management communities.
protect your company with the most advanced
INTEGRATED SECURITY SOLUTIONS.

Mobile Guarding  Auxiliary Services  Electronic Security Systems  Fire Protection
Consultancy  Cybersecurity and SOC  Global Risk Advisory
Manned Guarding  Comprehensive Systems Maintenance  Control Center

prosegur.com  twitter.com/prosegur  linkedin.com/company/prosegur  youtube.com/prosegur

see us at GSX Booth 3317
For product info #22 securitymgmt.hotims.com
The Texas Medical Center is the largest medical complex in the world. More than 60 institutions operate within its 2.1-square-mile footprint in Houston, including The University of Texas Health Science Center, which produces the most healthcare graduates in the state, and the MD Anderson Cancer Center, a joint academic institution and cancer treatment and research center.

It’s up to the University of Texas Police at Houston (UTP-H) to protect the 25,000-plus employees, 5,000 students, and 135,000 patients treated annually at the two institutions and across multiple cities—a Texas-sized job that requires the efforts of sworn officers, public safety officers, and civilians. The unique organization, which combines police and security operations under the same umbrella, serves a disparate community of patients, teachers, students, and healthcare workers. And a few years ago, the need for the ability to adapt and respond to an increasingly complex threat profile became apparent to UTP-H leadership.

“Don’t get me wrong—we really did a great job of responding and mitigating threats, but we were response-oriented,” says UTP-H Chief of Police and Chief Security Officer William Adcox. “Frankly, we weren’t able to take a systematic focus across the entire risk spectrum on an institutionwide basis.”

To do so, UTP-H took inspiration from the industry it serves. “Prevention has always been a major tenet of healthcare, and we wanted to look at opportunities where we could contribute to the prevention piece within security,” Adcox explains. “We saw the organizational value in shifting to looking at prevention, integration, and near-miss opportunities, to the point where we even looked at our traditional planning cycle and how we could become more agile and adaptive to the threats.”

The department embarked on a three-year process to overhaul its operations to become a more adaptable, responsive force with a shared purpose of prevention, protection, and preparedness.

“We wanted to try and get upstream of harm—prevent incidents before they occur, and be prepared to deal
with what is occurring,” says Raymond Gerwitz, director of risk strategy and operational excellence at UTP-H. “We created a shared purpose around prevention, preparedness, and protection and are engaging everyone in the idea. It’s no longer enough to protect and serve—we want to prevent too.”

Building an Operations Center
When approaching the department’s overhaul, leaders adopted a business state of mind. Most of UTP-H’s senior leaders hold MBAs and have been trained in business principles, and Gerwitz says that mindset—an unusual one for security organizations—has gone a long way to inform the department’s operational strategy.

“We ask, ‘How can we operate more like a business rather than a security group?’” Gerwitz says. “We looked at the strategies of communities we serve, took those principles, and adapted them to our environment. You won’t find many police departments or security groups that have a strategy map—it’s not a thing they think about. We took that from corporate America and blended it into how we do things.”

UTP-H began its overhaul with an internal value analysis that assessed operations at a day-to-day level to determine whether they aligned with the department’s updated goals.

“We look at different groupings of employees, every single task that they perform—how much time does it take, and what resources, and why they do it. Because there’s a law or regulation? Or because there’s an organizational policy? Or because it’s historically done? Or because there’s an executive directive?” Adcox says. “You break it out and that gives you a good picture of your internal value analysis so that you can look at those tasks that you can effectively quit doing and see what bandwidth you can pick up.”

One result of the analysis was the transition from a traditional police and security dispatch center into a more forward-facing risk operations center. “In the call center’s case, there were opportunities there to retire some misaligned tasks and insert new responsibilities that bring the value we’re looking to provide to the organization,” Gerwitz explains. “In essence it becomes a mathematical formula—I can retire tasks that are limited in value and repurpose the staff to increase value without adding headcount.”

Adcox says that it is important for employees to have both security training and a business mindset. “We really started placing priority on identifying members of our organization and people we would be bringing in that had a business acumen and were able to help lead us in new directions,” he says. “We’ve been fortunate and able to recruit capable individuals who bought into the vision. It all starts with your people, and that’s what’s critical. Getting the right people in the right roles and then ensuring that there’s a shared purpose—that’s how we approached it.”

The new department structure includes five service lines—healthcare security, investigative services, police services, risk management, and threat management—which often work together to respond to an incident.

“For the longest time, the face of the department was police services—the individual who wore the uniform, but now we have these five major service lines—the groups that set us on this journey of prevention,” Gerwitz explains. “A big part of being engaged is understanding everyone’s contribution—everyone has a role to play, even if it’s in the background.”

Gerwitz notes that the approach has paid off. Thanks to a combination of training and monitoring how calls are addressed, the percentage of calls handled by a single team member
has increased. These percentages are tracked monthly and shared with staff, encouraging open conversations about how calls are managed and keeping team members engaged.

Data-Informed Operations

The switch in response protocol illustrates how UTP-H is achieving its goal of predictive policing by focusing more on analyzing calls and encounters. Adcox says that previously, as in many organizations, analysts would log the data of the encounter but not use it.

“That was our response—we’d handle it, log it, and move on,” Adcox says. “We didn’t know the basis for the suspicious person—what’s the story? Now, we analyze and take data that comes in from multiple calls and visualize the data, and that better informs our officers of any trends, repeat offenders, potential threats that were averted, and what to look for. We now have an extended prevention opportunity on behalf of the communities we serve.”

For example, the operations center team is now encouraged to handle calls on their own without passing them along to another section to streamline the process.

“If they take care of a call on their own, they receive credit from a performance perspective on that,” Gerwitz says. “If they hand it off to someone else downstream, then they don’t. We monitor the percentage of things they are doing on their own on behalf of the organization without handing it off, because that generates efficiencies for us. And it empowers that group to try to handle things without having to go to others to get it done.”

If a call comes in about a suspicious person on campus, the operator can look at surveillance footage and recognize that person as an employee. Operators may reach out to that employee’s manager and ask why that person is in that area, but they don’t send a resource out to respond because they know it’s an authorized person who is perhaps in that area for a reason.

Gerwitz emphasizes how data visualization informs all aspects of the combined protection model.

“How do we want to go about creating a new shared purpose and engage the shift towards prevention? Let’s find data we need,” Gerwitz says. “We know the narrative, so what’s the data that supports it? Now we have that data, so we create visuals to enlighten our staff and get them engaged in what we’re all trying to do. For a long time, this information was kept in databases and didn’t resonate with our managers.”

Shared Purpose

Part of any organizational restructuring often includes developing a strategic plan, but once changes become the new normal it can be hard to measure whether operations are still true to that plan. Adcox and Gerwitz say the department constantly checks whether the department’s efforts point to its guiding principles.

“Three years ago, when we started this process, strategic planning was viewed as a necessary evil,” Gerwitz says. “There’s this perception that our efforts were a waste of time because we wouldn’t really use it. We had to change that mindset and educate everyone that some of what we’re trying to do will be unrealized, some will be impacted by emergent needs, or executive mandates, or in response to particular threats. It’s okay not to do everything as planned, but there is value in planning.”

Data analysis and visualization play a big part in both sticking to the plan and adapting where needed. UTP-H does not shy away from recalibrating or retiring components in the department if they do not show added value.

“Putting all these things in place is good but validating and proving that they are providing value intended is the most significant piece,” Gerwitz says. “How do you show people that you’re doing the things you say? Or, if you need to, how do you recalibrate your organization to do something more valuable? In today’s security field you have to adapt to threats coming, you can’t lay back and rely on the same strategies. We don’t spend a lot of time on traditional analysis. We let the current predict the future.”

All calls, incidents, and interactions are meticulously documented in a robust, interactive database that can be used for predictive policing by focusing more on analyzing calls and encounters.
that occurred in May—27 instances—and in a few clicks could drill down and view when and where the incidents occurred, who was the responding officer, and the final outcome.

“To be able to see this type of detail is very powerful for supervisors and managers, we ask them to go in and conduct management by visualization,” Gerwitz explains. “It’s easy for them to see what’s going on in their teams, and they can adapt their strategies based on what they’re hearing from the outside—if there are lots of vehicle and pedestrian hazards in a certain area, they can look and see whether we’re in those areas or we need to adapt our patrol tactics.”

Near misses are of particular interest to the department, because they signal both a looming threat and an area where predictive policing can be used.

“We’re almost fanatical about failure or near misses,” Adcox explains. “We’re not interested in numbers—how many doors we check that have to be secured, that kind of thing. What we are interested in are the doors that should have been secured that were found unsecured, or individuals in a certain part of the hospital who don’t belong or are lost—those are near misses. We’ll see how often that’s occurring or if it’s the same individuals. We have got to get in front of something happening.”

UTP-H relies on metrics to inform its tactics and mitigate negative trends before they affect the community.

“It might be how we view and put together video feeds, or we might put together a specific covert operation or put cameras in certain areas,” Adcox explains. “It might be working within a specific group of employees, asking them to watch for certain activity and report a certain way. It’s very proactive.”

Empowering Employees

All employees have access to performance and value visualization tools in the spirit of transparency and to understand the operations of the entire department and the impact their teams have in keeping the institutions safe. Gerwitz says that most employees don’t view the information every day, but they are alerted when new resources are added. There has been a lot of thought put into how the data is accessed—the department is on its second iteration of the visualization tool, he notes.

“It’s now much more graphic and in line with how people want to consume information,” Gerwitz says.

Managers will also put together visualization boards specific to their teams, and in the case of groups like security officers who aren’t often in front of computers, they will print them off and review them during meetings.

“It has been helpful in allowing people to straightforwardly show their value,” Gerwitz explains. “Before we put this in place, it was hard for people when they were stopped to tell me how your team benefits what we’re trying to do—it was hard for them to articulate that in a way that made sense to people. This program makes it easy. I think that’s the biggest benefit to the department—now managers are able to adapt and show value at any moment based on what teams are doing. From an organizational perspective, the feedback we get from senior executives who use these processes themselves brings a lot of credibility to our team.”

Connecting with Communities

Adcox has worked with UT Health and MD Anderson for 14 years and is aware of the challenges of protecting the esteemed educational and healthcare facilities. Part of UTP-H’s transition included opening more dialogue between the department and the institutions to ensure they are working towards the same goals.

“We bring in leaders from the institutions and walk them through our process and spend time on things they value,” Gerwitz says. “If we bring in the clinical team, we’ll spend a lot more time on issues they deal with in the clinics and how we adapt our training, versus meeting with the finance folks, where we validate our programs and show value.”

One example of partnership between UTP-H and the institutions it serves is
the approach to people experiencing a mental crisis. Beyond developing a trusted response protocol, the UTP-H threat management team strives to work with the school and hospital to predict potential personnel issues before they come to fruition.

“You bring all these pieces of information together, so they can present to you a real picture of what the situation is,” Adcox explains. “You’re able to get people help in advance of losing their jobs or harming themselves or someone else. It’s been very effective, and we have progressive data and use data visualization to show that.”

If an employee, patient, or visitor is actively in mental crisis, the threat management team is trained on how to respond and follow up, Gerwitz says. That 98 percent of UTP-H responders are certified mental health officers due to the unique stresses of the joint education and healthcare environment—most other law enforcement departments in Texas provide less than 10 percent of their officers such training, he says.

“That employee in crisis will be assessed using tools we have been trained on to screen for the person’s mental state,” Gerwitz explains. “So, say on a scale of one to 10, I’m an eight—I’m in a bad place, and the responders apply a strategy to bring me down. Following that event, through peer review or interacting with me as they continue to monitor my status, they reassess me, and now I’m a five—they measure that delta.”

The team has a calculated goal for an average reduction of the intervention score and, using data visualization tools, can track how successful different intervention methods are and adapt intervention tactics based on those statistics across a variety of populations.

“It’s a team effort across the institutions—there are others participating in this effort, such as human resources, employee health programs, supervisors, and we can track who all handled each case and its outcome,” Gerwitz explains.

Being able to map out the outcomes of police interactions with people in crisis has been impactful in promoting relations between the institutions and UTP-H, Gerwitz adds. Of the 98 threat intervention cases he mapped out, only two resulted in arrest. This statistic goes a long way in garnering trust with hospital employees who might be wary of involving police in a mental crisis.

“For a long time while implementing this, we had to break down the walls of thought that if you call the police, someone is going to get arrested,” Gerwitz says, adding that the outcome statistic was well received by clinicians. “To me, this is the more high-level analytical, value-driven style, compared to performance monitoring that goes on in typical security operations.”

Adcox agrees, noting that such data illustrates UTP-H’s thoughtful approach to conflict in such a sensitive environment.

“In our business, our whole approach is an organizational health, individual wellness method,” Adcox says. “It is not in any way a prosecutorial or criminal justice approach. Because we have a police component, you have that extra tool in your toolbelt if you need to bring a situation under control.”

**Partners in Business and Purpose**

Gerwitz says that another important culture shift has been thinking about the business success of the organizations UTP-H serves, not just its own success.

“Not only are these healthcare institutions and educators, they are also businesses,” he says. “Part of the value we’ve been able to distill from all of this is that if you act like a business partner and are treated like a business partner, you can do better with your allocated resources and meeting the goals of the organization.”

Adcox explains that UTP-H has assessed where its operations overlap with UT Health and MD Anderson and partners with them to share knowledge and training. In areas such as investigations and crisis training, the department can step in and share its own resources for the benefit of the entire organization.

“I cannot stress enough the importance of going into each of these places that perform these critical functions for these organizations and working with them,” Adcox says. “Have a joint training, let us explain what we do and what our expertise is, and they’ll teach you what’s important to them, and then you have the trust factor and can start talking about how to integrate and help each other.”

Since UTP-H is known for its high level of conflict resolution training, it has partnered with UT Health to train nursing students on handling people in mental crisis—everything from body language in the hospital room to handling a patient’s family to deescalating conflict. Adcox says UTP-H also trains clinicians, physicians, and nurses working at the facilities in the same practices.

“We’re able to bring that into play because of the expertise we’ve had to develop in being effective in our organization,” Adcox says. “We also have an immersive simulation center so that you actually have practical, holistic experiences and not just the classroom. This technology is for the entire organization, not just us.”

By aligning UTP-H with UT Health and MD Anderson’s enterprise goals and overarching missions, the department is now seen as an equal and valuable partner—in business and protection alike.

“The struggle we have on the security and law enforcement side is that we’re not accepted as legitimate business partners, we’re a cost center that’s a necessary evil,” Gerwitz says. “You have to hold yourself to the same accountability and integrity and commitment to the organization as any other business unit. You’re no different from the other teams working on behalf of the organization. This business approach is aimed at making sure we’re being good stewards of the resources provided. When people believe you’re doing that, they’ll support you.”

**Contact Associate Editor Lilly Chapa** at LillyChapa@ASISOnline.org. Follow her on Twitter: @LILLYCHAPA
How to Implement ESRM

International Paper (IP) is one of the world’s leading producers of fiber-based packaging, pulp, and paper. Headquartered in Memphis, Tennessee, IP employs approximately 52,000 people worldwide and has operations in more than 24 countries serving customers around the globe.

The Challenge
When IP’s director of security announced his retirement, the IP team—Deon Vaughan, vice president, deputy general counsel, chief ethics and compliance officer; Casey Yanero, HR manager, corporate staff groups; and Jennifer Carsley, director, legal operations—recognized it was time to transform corporate security to an enterprise level function.

The ever-changing threat landscape and IP’s core values of “Safety, Ethics and Stewardship” underscored the need for IP to transition to a proactive security posture. To lead this transition, IP hired Art Fierro, CPP, in February 2017 to fill the newly created chief security officer (CSO) role.

ESRM Solution
Enterprise security risk management (ESRM) links security activities to an enterprise’s mission and business goals through risk management methods.

The CSO’s role in ESRM is to manage risks to enterprise people and assets in partnership with the business leaders. ESRM involves collaborating with business leaders on the realistic impacts of identified risks, presenting potential strategies to mitigate those impacts, and then implementing the strategy in line with accepted levels of business risk tolerance.

Fierro’s background is rooted in ESRM in both the government (FBI) and the corporate space. To move IP from a traditional security organization to an ESRM enterprise model, Fierro conducted an extensive security analysis to identify where the organization excelled and where the data showed opportunities for improvement.

A global corporation knew it needed to take a more proactive approach to security. Here’s how it did, using enterprise security risk management.
The analysis included conversations across business groups and corporate partners. It served as the foundation for IP’s ESRM strategy and helped create its vision statement: “To protect IP people, information, products, and the corporate brand in support of business objectives and enterprise success.”

IP’s new enterprise security strategy is grounded in the principles of security mitigation steps based on risk and using cost-benefit analysis to ensure a return on security investment. The strategy also aligned with IP business operations and is designed to help achieve business objectives—meaning security would not just be a cost center but also a business enabler.

Outcomes
With the endorsement of ESRM at the leadership level, Fierro was able to work with partners to create a risk-based security program to focus security resources on identified risks. The program also provides the operating manual for vulnerability and risk assessments, so IP can make informed business decisions about its risk tolerance.

Enterprise Security Management created a new concept, a virtual operations center, which produces a global threat picture that helps it identify and address emerging global threats to IP employees and facilities. The virtual operations center is outsourced to leverage economies of scale, leading edge technology, and professional threat analysts and operators, while providing an excellent return on security spend.

Over the past year, Enterprise Security Management focused on a number of strategic initiatives. One is the geospatial traveler-tracking program for IP’s traveling employees.

Another initiative is the corporate campus security capital improvement project. Enterprise Security Management is leading a security improvement project for IP’s corporate headquarters based on ASIS International physical security standards and guidelines, as well as geographic risk demographics and the return on security spend.

Enterprise Security Management also launched its first national security guard force contract to consolidate and standardize guard force operations across certain U.S.-based facilities. The consolidated operations agreement helps ensure consistency and reduce cost.

Enterprise Security Management is also working with EHS to add a security aspect to the current field assessment process to identify actual risk at IP’s global locations. Assessment results will be used to develop security recommendations, including leveraging security technology.

Additionally, Enterprise Security Management created a new active shooter response training program for employees. The training included Virginia Tech shooting survivor Kristina Anderson, who shared a survivor’s perspective, as well as the Memphis Police Department, which provided training for employees on Run, Hide, Fight. The active shooter plan is also available on IP’s internal website for employees to reference.

Working across business groups and with critical internal partners, Enterprise Security Management developed new crisis communications reporting, dissemination, and functional requirements that include mass communications features for a unified enterprise response to man-made or natural disasters.

ART FIERRO, CPP, IS CSO AT INTERNATIONAL PAPER. HE FORMERLY SERVED AS CEO OF RONIN OPTION-CYBER, EXECUTIVE VICE PRESIDENT AT RESILIENT INTEGRATED SYSTEMS; AND VICE PRESIDENT AT 20TH CENTURY FOX FILM CORPORATION. HE IS A MEMBER OF ASIS INTERNATIONAL.

Partnerships
Sharon Ryan, senior vice president, general counsel, and corporate secretary, embraced ESRM as IP’s new enterprise security strategy, because the strategy was aligned with IP’s core values and business strategy.

“We recognize that by adopting the latest risk management strategies in enterprise security and bringing on experienced security professionals, not only are we helping protect our people and property, we are also reducing the risk of negative exposure related to our brand and reputation,” she says.

Ryan supported the strategy by rebranding IP Corporate Security to Enterprise Security Management and creating three new positions reporting to Fierro and designed to address IP’s enterprise risks: global threat manager, global physical security manager, and global investigations manager. The three functional roles cover the spectrum of enterprise risk and each has a deployment roadmap, which ties into the larger Enterprise Security Management global strategy.

Vaughan also supported the effort by endorsing a campaign for Enterprise Security Management to build partnerships across business lines, such as IP’s Environmental Health and Safety (EHS) department, and to partner on initiatives to protect IP’s employees—one of Enterprise Security Management’s strategic objectives.
A Screening Minefield

More and more job candidates in the United States are testing positive for marijuana. Should employers reconsider their hiring practices?

**DRUG USE BY AMERICAN WORKERS** is the highest it’s been in more than a decade, and some companies and states are changing their preemployment screening processes to account for the shift. More than half of U.S. states have legalized the use of cannabis either medically or recreationally. This shift, combined with a strong economy that makes finding quality job candidates more challenging, is compelling some organizations to adapt.

**Nationwide Trends**

Quest Diagnostics, a leading provider of drug screening services, recently released its annual Drug Testing Index, an analysis of national workplace drug positivity trends derived from its lab analysis. Its 2017 statistics show that 4.2 percent of employees screened for drug use tested positive last year—the highest positivity rate in more than a decade. Rates of cocaine use among tested employees rose, as did methamphetamine use in the Midwest and South United States.

One statistic is sure to catch the attention of employers—the rate of employees testing positive for marijuana has continued a five-year increase, but increases were most striking in states that have legalized the recreational use of marijuana. This is true for both the general U.S. workforce, as well as the federally mandated, safety-sensitive workforce—rail, bus, and truck drivers; pilots; and workers in nuclear power plants, as mandated by the U.S. Department of Transportation (DOT).

“These increases are similar to the increases we observed after recreational marijuana use statutes were passed in Washington and Colorado,” said Barry Sample, senior director of science and technology for Quest Diagnostics, in a statement. “While it is too early to tell if this is a trend, our data suggests that the recreational use of marijuana is spilling into the workforce, including among individuals most responsible for keeping our communities safe. We encourage policy analysts to track these trends closely to determine whether a correlation between the state legalization of marijuana and increased workforce drug use, as suggested by our data, bears out in other research.”

As the legalization of medical and recreational cannabis continues to spread throughout the United States, it’s becoming clear that the employment challenges it poses are not going away any time soon. In 2017, researchers saw a slight decline in testing for marijuana in the workplace—98.4 percent of tests screened for marijuana, compared to 99 percent in 2016. About 70 percent of drug tests in the workplace are for preemployment screening, according to Quest.

Several nationwide organizations have already taken steps to ease zero-tolerance policies, including AutoNation, Inc., which employs 26,000 people across the country.

Below is a selection of how employers across the country are adapting.

**Nevada**

Recreational use of marijuana was legalized in late 2016, but the market was not launched until last July—and took off from there.
*Forbes* reported that in just four months, Nevada sold $37.9 million in cannabis products—that’s compared to the $22.56 million that Colorado made in the first four months of its legalization.

The popularity of recreational marijuana is reflected in the Drug Testing Index, which found a 43 percent jump in employees who tested positive for marijuana in the last six months of 2017 alone. That also includes a 39 percent increase in marijuana positivity in safety-sensitive workers.

And less than a year after Nevada residents could start legally buying marijuana, companies are responding. Caesar’s Entertainment Corporation—owner of Caesar’s Palace in Las Vegas—announced in May that it would no longer screen job candidates for marijuana use. The organization has stated that it was missing out on quality candidates due to “counterproductive” marijuana prescreening policies. The company will continue to prescreen safety-sensitive positions, as mandated by the DOT, and will test employees who are believed to be impaired at work. No other gaming employers have publicly altered their prescreening policies as of press time.

**Maine**

In 2017, citizens of Maine approved a new law that not only legalized recreational marijuana use but made it illegal for employers to prescreen job applicants for marijuana use. While retail shops aren’t expected to open until next year, employers had to cease drug screening starting in February of this year. The law also states that employers cannot refuse to employ someone 21 or older who uses marijuana outside of the workplace. However, a previous mandate that employers could not discipline employees who tested positive for marijuana—because they may have used it outside of the workplace—was revised in May. The law “does not affect the ability of employers to enact and enforce workplace policies restricting the use of marijuana by employees or to discipline employees who are under the influence of marijuana in the workplace.”

Organizations that employ DOT-designated safety-sensitive workers—who, under federal law, must be tested for marijuana use—face a gray area in the contrasting state and federal laws. Those organizations are still federally required to drug test designated workers but are not exempt from the state’s rules on punishing employees who use marijuana outside of work. So, if a job applicant or employee in a safety-sensitive position tests positive for marijuana use, Maine employers might not be able to take any adverse action against them, beyond stopping the employee from performing safety-sensitive functions.

The antidiscrimination law was revised in May and now allows employers to discipline workers who are under the influence of marijuana in the workplace in accordance with the employer’s policy on marijuana. It remains to be seen whether Maine’s conflicting nondiscrimination provisions will be enforced by the courts, or how the revised disciplinary rule will play out in the workplace.

**New York**

While some employers may be quietly removing marijuana testing from their preemployment process, others may choose to enforce existing regulations more loosely. That appears to be the case with the New York Fire Department (FDNY), where reports have emerged that more than two dozen firefighters have returned to work after testing positive for drugs. The current FDNY manual describes a zero-tolerance policy, but more recently firefighters have been telling...
reporters that employees who fail a drug test are instead sent to an eight-week rehabilitation program and must acquire a dozen character references to rejoin the forces—albeit at a different firehouse.

Rhode Island
A state court decision last year may have big implications for employers who screen potential job candidates for marijuana use. Medical cannabis has been legal in Rhode Island since 2006, but—like most states with some form of marijuana legalization—a positive drug test could still mean being fired or passed over for a job.

However, a job applicant who was denied the position due to her medical marijuana card pursued the issue in court and won. The plaintiff had applied for a paid internship and disclosed to her potential employer that she would not pass a drug test because she used medical marijuana. When she was not hired, she sued the organization, noting that its policy only prohibited the use of drugs on company property.

The judgment has set a precedent that employers in Rhode Island cannot refuse to hire a medical marijuana cardholder, even if they cannot pass a preemployment drug test. The case does not require employers to make accommodations for medical marijuana users in the workplace but will certainly affect hiring processes in Rhode Island. And similar lawsuits in Massachusetts and Connecticut have been won by medical marijuana users in recent months, signaling a shift from courts’ consistently siding with employers on drug testing matters.

CONTACT ASSOCIATE EDITOR LILLY CHAPA AT LILLY.CHAPA@ASISONLINE.ORG. FOLLOW HER ON TWITTER: @LILLYCHAPA.
MULTIPLY YOUR KNOWLEDGE, TIME, AND RESOURCES IN LAS VEGAS.

Choose from these intensive, practical learning opportunities held prior to Global Security Exchange.*

PRE-CONFERENCE PROGRAMS

22-23 September
CPP REVIEW
PCI REVIEW
PSP REVIEW
Each of these classroom programs provides an accelerated, high-level overview of security concepts and practices tested on the respective certification exam. An excellent resource for identifying areas where you may need further study. (Does not include exam questions.)

23 September
THE ESRM LIFE CYCLE AND CONVERGENCE OF PHYSICAL AND CYBERSECURITY
Learn the basics of ESRM and how the overall life cycle functions to engage security as a true business partner to their enterprise executives. Interact as part of a team with ESRM and convergence leaders and apply lessons learned in a team exercise.

23 September
POLICY-WRITING WORKSHOP
Policies, procedures, training files, post orders, manuals – clearly written and legally defendable. This program offers simple steps to creating well-formatted, properly written resources that will help you and your team reach the objectives you want.

23 September
SUCCESSFUL SECURITY CONSULTING
Looking to successfully launch a new security consultant practice or jump-start an existing one? Learn from seasoned consultants how to develop and market yourself as a security consultant and avoid costly mistakes that can sabotage your success.

LEARN MORE AND REGISTER AT GSX.ORG/PRECONFERENCE

*Additional fees apply. Registration does not require attendance at GSX.
In the hit 1999 movie *The Matrix*, people go about their daily lives unaware they are in a simulated, alternate reality being controlled by greater powers. In one scene, the main character Neo, played by Keanu Reeves, sees a black cat walk past a doorway. A few moments later, the same cat walks by again.

“Déjà vu,” he says aloud. His comrades, who know they live in the Matrix, are disturbed by the claim and press him on what he saw. When he says he observed the same black cat walk by—twice—they spring into action, explaining that a déjà vu demarcates a glitch or change in their synthetic world.

A similar concept exists in the field of countersurveillance, referred to as the déjà vu effect. While traveling in a foreign place, if the same person or vehicle appears twice, it is likely not a coincidence. Someone could be following the traveler, scoping him or her out as a potential target for crime. I learned to rely on this principle during my time as a CIA case officer, traveling to some of the most dangerous parts of the globe to collect intelligence.

However, one does not have to be in a war zone or third-world country to encounter threats. Much like the Matrix, even a seemingly normal setting can quickly turn upside down and require quick thinking. Simple observation of one’s surroundings, like being on the lookout for the déjà vu effect, will greatly help solo travelers maintain their personal security.

Similar to a corporate travel security program that tracks executives or...
employees while on business, individuals can protect themselves by adopting a portable set of principles and concepts that they can take with them wherever they go.

There are three key concepts that must be in place for a personal travel security program to work. Just like a physical security or cybersecurity program at a large corporation, a personal travel security plan must first be effective to protect the individual. If a building has a fence that is not properly maintained or a camera system that is broken, the physical security program is considered ineffective. If someone relies on a personal security program that he or she cannot recall from memory and put into action, it will be unsuccessful.

The second aspect of a personal security program is the concept of risk. In enterprise security, there are assets, threats, vulnerabilities, and countermeasures. In personal security, the asset being protected is oneself. The threats are usually external to the traveler, but vulnerability—weakness—is a unique element of personal security risk. Vulnerabilities can exist both outside or within the individual. Understanding this unique aspect of personal security risk is crucial. The countermeasures
**Part of deterrence is making oneself appear less vulnerable.**

Travelers should research the area they are traveling to and familiarize themselves with the location geographically. Use the Internet and other means before arriving, but also conduct a mental site survey once you arrive on-site. In the Middle East, for example, few streets have names. Take note of major landmarks, roadways, and other characteristics that stand out in case you may have to remember where you were at any point in time.

Normally, bringing roughly $300 to $500 in U.S. currency should suffice, but be sure to work out how much cash you may need over the course of the trip. Small U.S. bills are handy, and something of value that everyone recognizes—the U.S. dollar is often an acceptable form of currency in a pinch. The traveler should break down the total amount into $20 bills and divide that roughly in half between checked luggage and the important items to be carried on.

Small bills also allow the traveler to find and pay cash for personal transportation upon arriving at the destination. When you do not have the luxury of prearranged travel by a corporate security program, choosing your own transport on-site is critical, versus having it solicited or having someone else choose it.

In some high-risk locales, drivers for hire typically wait outside airports, bus stations, and train stations, and are on call. It is advisable to be deliberate and maintain control of how you choose transportation. Look first for kiosks with taxis for hire or hotels with shuttle transport. If none are available, ask an airline representative what transport can be trusted. The last resort is to look for marked taxis outside and choose one—do not let it be chosen for you.

Keeping and maintaining the element of unpredictability is important to your security. If the driver you hire is reliable, it is worthwhile to keep the same driver to take you from place to place throughout the duration of your trip. This allows you to build a relationship with that person and have someone you trust to get you around the area.

**Detection.** The second principle to a personal security program is detection. It’s imperative for the traveler not just to see what is around him or her, but to observe it. Observing is intelligent detection and keeps you in the present moment.

Such skills can be important in preventing crimes such as pickpocketing. Travelers who are preoccupied, even mentally, make themselves a vulnerable target. Take off the ear buds or headphones, stay alert, and keep your mental focus on the here and now.

London’s Piccadilly Circus, for example, is an infamous place for pickpockets. These crews target travelers who are distracted, whether it be window shopping, talking on cell phones, or sightseeing. Pickpockets work in teams,
with one person designated to distract the victim, another to take the item, and a third to move it away from the crime scene. Someone on this team may have already scoped out where imported effects are kept without the individual's awareness.

The déjà vu effect discussed earlier comes into play in the element of detection. If you are walking down the street toward an ATM, for example, and someone seems to be following or keeping pace with you, pay attention to that. Being aware of this allows you to assess it and take proactive action. Most often, petty thieves move on to easier targets once they realize they have been spotted.

**Deterrence.** The third principle to an effective personal security program is deterrence. Deterrence is how you look and behave. Blending in with your environment helps eliminate the possibility that someone will see you as a target, but this is not just achieved by the clothes you wear.

While a subtle wardrobe is an essential element to maintaining personal security, so is a sense of confidence in the traveler's gait as he or she goes from point A to point B.

Keep smartphones and other valuable items tucked away in a bag. Be discreet when accessing them in a public place. Threat actors look for low-hanging fruit, so part of deterrence is making oneself appear less vulnerable to assault. The goal is to make it harder for the bad guys to go after the traveler in any way.

Deterrence can apply to the type of car you use when renting a vehicle. For example, while with the CIA and afterwards in the international consulting world, I took trips into Mexico, Yemen, Africa, and elsewhere in the developing world. I consistently looked for cars that were worn and unattractive. I drove through the first mud puddle I could find, and did not wash the vehicle over the course of the trip. The more dented and dirty, the better. It blends.

The last two principles of a personal security program—delay and defense—are a last resort and should not come into play if the first three principles are aptly applied. The traveler should deploy the last two principles to survive and escape threats with as little harm as possible.

**Delay.** The fourth element, delay, comes into play when you have been targeted, particularly on the street. Putting space between yourself and the threat buys you time—time to run, or time to prepare to defend yourself.

While traveling, I carry decoy items with me to create delay in a mugging situation. One is a throwaway wallet, stuffed with fake credit cards and petty cash sticking out of the sides. Tossing this to the threat creates enough time to get away without losing items of real value. I also wear a cheap watch that looks expensive. In Central America, I once used such a decoy watch to get away from a thief, who ended up with a cheap fake Rolex.

Carrying a whistle is also advisable, because it adds the element of surprise.
and draws attention to the scene—not normally an adversary’s desire. With delay, one is creating distance between oneself and the threat. The greater the distance, the greater the chance of survival.

**Defense.** The final principle is defense. What does the traveler do if his or her options are being mugged, injured, or killed—or fighting back? No matter a person’s age or level of physical fitness, there are certain defensive tactics that can increase one’s margin for survival and potentially limit the amount of harm done. Consulting a self-defense expert on tips and techniques, whether they are hand-to-hand combat, or firearms training, is certainly advisable. However, if the adversary has a weapon—particularly a firearm—it is wise to go along with his or her demands.

**Captivity.** Should you be abducted, if you are able, make a scene—yell and scream as loud as possible. Doing so creates witnesses, which can help when a search is conducted. One former U.S. drug enforcement agent did just this while being kidnapped in Mexico, and witnesses helped police in the search that eventually led to his rescue.

In the rare circumstance that you are kidnapped, once you’re physically controlled, stop struggling physically. The last thing you want is to go into captivity with a broken nose or broken bone. Part of a personal security program is staying alive, so be prepared for the possibility of this circumstance. Have one or two key phone numbers memorized, so that if you are unexpectedly released in an unfamiliar place you can make a call to someone who will answer.

Communicate with the captors and let them know if medication or other physical care is needed. Try to build a relationship with the people who are responsible for you so that they are inclined to hesitate before harming you.

Kidnaps for ransom have become increasingly commonplace in countries like Mexico and Colombia. Travelers should have a plan in place before leaving home for a lawyer or third party to help negotiate release. A loved one should not be responsible for negotiations, because they can bring too many emotions into the transaction.

One area where your family or loved ones can help, is having a prepared list of “signs of life” questions for those aiding in the release or rescue; statements or facts that only you and that person know. These can be communicated by the captors to the loved one so that they know the person is, in fact, alive. Duress phrases, such as, “make sure you water the garden,” (when, in fact, you might not have a garden) that signal safety or distress without the captor’s knowledge can be useful.

Finally, in a rescue operation, you should know that law enforcement or the military might not immediately recognize you as the victim. Let the operation unfold, keep low, and keep your hands visible so that you’re not inadvertently harmed in the cross fire.

**Skills for life.** While working as a CIA officer abroad, I traveled and worked for decades without a badge or weapon and learned to bring the aforementioned skills to bear to keep myself and those for whom I was responsible safe. With or without the support of an executive protection program, traveling solo requires a person to rely primarily on himself or herself for basic security.

The five elements of a personal travel security program—preparation, detection, deterrence, delay, and defense—should be thought of as mental pegs. Take the details that go under each concept and hang them on those five pegs. Then you can quickly and effectively grab the tools needed in high-risk situations and environments. Internalizing these skills will help build good instincts, increase your awareness, and ultimately provide life-saving protection.
Together we can

Educate  Heal

Inspire  Nourish

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

Supporting Families Across America
OPENING GSX KEYNOTES
ANNOUNCED

FUTURE-FOCUSED VISIONARIES are coming to Vegas. Peabody Award-winning CNN host, columnist, and global thinker Fareed Zakaria and futurist and technology pundit Scott Klososky will bring vital insight to their opening keynote addresses at Global Security Exchange (GSX), formerly the ASIS Annual Seminar and Exhibits, September 23–27 in Las Vegas.

Zakaria will kick off the GSX conference program on Monday with his opening remarks. A former editor-at-large at TIME and current host of CNN’s flagship international affairs program, “Fareed Zakaria GPS,” he is a world-renowned expert on global trends. His columns and commentaries—on topics ranging from the future of the Middle East and America’s role in the world to innovation and the politics and culture of the global economy—reach millions through The Washington Post, CNN, and his daily digital newsletter.

Klososky returns to GSX as the Tuesday morning keynoter on the heels of his popular “The Technology Integration of Man” presentation in 2017. Since then, he has discussed enterprise security risk management and key change drivers in today’s security industry at ASIS Europe and the ASIS CSO Summit. At GSX he will tie all these thoughts together for a comprehensive look at the impact of today’s rapid digital transformation on security management and leadership. He will build a compelling case for managing and using technology—and knowing when not to use it—to gain a competitive advantage and lead successfully into the future.

For more GSX updates, visit gsx.org/blog. The GSX Blog offers previews of the education, products, and experiences available to participants in Las Vegas this September. Hear attendees, speakers, and exhibitors explain what they’re looking forward to at GSX and why this show—for the profession, by the profession—is the industry’s can’t-miss event.

STUDENT MEMBERS
ATTEND GSX FREE
ASIS International is making it easier than ever for students of all ages to enter the security profession, providing the information, networking, and
professional development opportunities needed to kick-start their careers.

Last year, ASIS reduced student membership fees to $20 per year. In 2018, ASIS has deepened its commitment to the profession’s next-generation leaders by offering all student members a complimentary all-access registration for Global Security Exchange (GSX).

The all-access pass allows students to participate in the onsite career center and job fair to learn about the diverse range of opportunities available across the profession and attend the full education program, including foundational sessions like “Security Careers: The What and the How” and “A Framework for Multigenerational Security Organizations.” Most importantly, they can begin to build a network that will support them through every stage of their professional journey.

Ron Martin, CPP, regional vice president, ASIS International Region 3D, and director, Open Security Exchange, has sponsored dozens of student members over the years so they could benefit from the education and networking that ASIS provides.

“I’ve long believed that it’s the responsibility of veteran security professionals to take the next generation under their wings,” Martin says. “An ASIS membership offers these students career-long connections to the lifeblood of the security profession. Mentors and experts in the field are always within reach and able to provide advice at every stage of their careers.”

ASIS has also started developing a new early careerist certification, envisioned to be the first rung on a security management professional’s career ladder.

The ASIS Young Professionals Council is hard at work to ensure that these next-generation leaders make the most of their involvement with the Society. Each ASIS chapter is encouraged to designate a Young Professionals liaison, who organizes events and advocates for young professionals and the issues that matter to them most.

Members are encouraged to reach out to their local chapter and identify students who can benefit from membership. For help getting started, contact the Academic and Training Programs Council via ASIS.ATPCouncil@gmail.com.

COUNCIL CORNER: ACADEMIC AND TRAINING PROGRAMS COUNCIL

Nearly two dozen professors, adjunct faculty, and security professionals with expertise in training development and delivery make up the Academic and Training Programs Council. These leaders promote and assist in the development of security academic education and professional training programs at academic institutions, professional associations, private organizations, and government entities.

The council’s work includes collaborating with universities that offer accredited academic programs in security management, national security, and cybersecurity.

#MYASIS IMAGE OF THE MONTH

@ASISCHAPTER190
30 years of success thanks to all former @ASISChapter 190 Chapter Chairs. Thank you for getting the chapter to where it is today. Heading down to meet our members at the boat. #VANCOUVER

ASIS BOARD OF DIRECTORS

PRESIDENT
- Richard E. Chase, CPP, PCI, PSP
  General Atomics
  San Diego, California

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

TREASURER
- Godfried Hendriks, CPP
  Revolution Retail Systems
  Alkmaar, The Netherlands

SECRETARY
- John A. Petruzzi, Jr., CPP
  G4S North America
  New York, New York

CHAIRMAN OF THE BOARD
- Thomas J. Langer, CPP
  BAE Systems Inc.
  Arlington, Virginia

DIRECTORS
- Charles E. Andrews, CPP
  Friends of Chuck
  Houston, Texas
- Howard J. Belfor, CPP
  Belfor & Associates
  Black Mountain, North Carolina
- Michael R. Bouchard, CPP
  Janus Global Operations
  Williamsburg, Virginia
- Gail Essen, CPP, PSP
  Professional Security Advisors
  Andover, Minnesota
- Radek Havlis, CPP
  PricewaterhouseCoopers
  Prague, Czech Republic
- Jeffrey J. Lee, CPP
  Saudi Aramco
  Dhahran, Saudi Arabia
- Richard F. Lisko, CPP
  Willis Towers Watson
  Dallas, Texas
- Timothy M. McCreight, CPP
  Online Business Systems
  Calgary, Alberta, Canada
- Darren T. Nielsen, CPP, PCI, PSP
  WECC
  Peoria, Arizona
- Jaime P. Owens, CPP
  Panama Canal Authority
  Panama City, Panama
- Malcolm C. Smith, CPP
  Qatar Museums
  Doha, Qatar
- Ann Y. Trinca, CPP, PCI, PSP
  SecTek
  Reston, Virginia
rity to share security-related trends and studies. The council also works with ASIS stakeholders to connect with undergraduate and graduate students in support of their development to become the next generation of leaders within the security profession.

In the coming months, the council will focus on updating the ASIS listing of institutions offering security academic programs, surveying universities and student members, improving curriculum development by promoting better understanding of broader skill sets required of security executives, and promoting increased understanding of enterprise security risk management (ESRM) and its linkage to business success.

CHAPTER EVENTS IN INDIA

Over a single weekend in May, the ASIS New Delhi and Mumbai chapters drew hundreds of attendees to chapter events to spotlight and celebrate security excellence.

On May 25, the New Delhi Chapter’s Women in Security event featured topics like “Breaking Barriers,” “Diversity and Inclusion,” and more, delivered by women security professionals from Boeing, Shell, and IBM, among others. Almost 100 professionals attended the event at the Bank of America’s Gurugram office.

“This meeting provided an excellent platform to showcase women security professionals at various levels,” says Manish Datta, chapter chair, ASIS New Delhi. “These women act as a guiding light for others to follow their passion and make this industry their professional choice.”

The Mumbai Chapter highlighted security excellence on May 26 via its CPP Review Session and Mentorship Program presentation. Nearly 150 professionals attended the virtual conference to learn about the chapter’s new CPP preparation program.

Through the program, CPP aspirants will be paired with a mentor. The mentor will conduct monthly discussions, and aspirants will participate in quarterly review sessions. After a year’s time, the program’s participants should have attained the requisite knowledge to attain the CPP certification.

“The overwhelming attendance for this program is a clear reflection of the growing potential of the security industry in India,” says Sanjeev Mishra, CPP, chapter chair, ASIS Mumbai. “This initiative will go a long way in both spreading awareness about ASIS and the CPP certification and sharing valuable knowledge needed for security professionals to thrive.”

Datta presented closing thoughts at the Mumbai event, demonstrating the collaborative spirit these chapters share in their efforts to advance the profession.

To stay up to date on the work ASIS chapters do all year long, read monthly regional Dynamics member newsletters at asisonline.org/Dynamics.
ASIS LIFE MEMBER
ASIS congratulates Frank W. Robinson, CPP, on becoming a Life Member. Robinson has been a member of ASIS for 36 years and has held the CPP certification since 1983. He served on the Commercial Real Estate Council.

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

MEMBER BOOK REVIEW

Business continuity plans must be simple, strategic, and service-oriented: that is the key message of this book by Rachelle Loyear. The author advocates a new model—the Three S Philosophy—as an approach to improve engagement and support for business continuity management (BCM) programs.

Traditional BCM programs face various challenges and roadblocks that make them cumbersome for business subject matter experts and even for the experienced risk professional. To counter those obstacles, Loyear urges planners to focus on the essentials, stripping away complexity and putting strategy and business value front and center to help the risk owner in the BCM journey.

This guide will provide great value for anyone engaged in BCM, whether as an experienced risk professional or a functional expert. The Three S Philosophy, which endorses simplicity, strategy, and service, provides a powerful yet uncomplicated framework that focuses on value. The reader will appreciate various references in the manuscript to enterprise security risk management, as well as practical templates and checklists to facilitate further use.

REVIEWER: Rachid Kerkab has almost two decades of experience in criminology, strategy, risk, and resilience. He is a member of ASIS.

CERTIFICATION PROFILE
SANJEET MISHRA, CPP

As chair of the ASIS Mumbai Chapter, Sanjeev Mishra, CPP, is a major advocate for board certifications in India, and his chapter recently spearheaded a free Certified Protection Professional® (CPP) review program that drew registrants from all across India. He is happy to tell the story of how ASIS board certification has bolstered his career.

A captain with the Indian Army in the mid-1990s, Mishra surveyed the social, cultural, and political landscape, closely observing conflict trends. “I realized that the black-and-white character of conflicts, in which borders and combatants could be clearly characterized, were taking on an unconventional gray character,” he says.

These thoughts followed him as he made the choice to transition from the military to a security career. “With sovereigns focusing on inward security, and corporations getting in on the act, I decided to devote my skills to safeguarding business interests just the way I’d protected borders.”

He joined the profession as a security manager for Reliance Industries Limited (RIL) in 1996. After spending a decade working in industrial security, he left RIL in 2006 to join a U.S. banking start-up. Determined to catapult his career to new heights, he decided to pursue the CPP certification.

“My CPP certification made me stand out from the crowd and embedded me into a league of extraordinary security professionals,” he says. “Not only did I enjoy support and admiration from my security community, my accomplishment was also appreciated by business leaders in the form of speedy promotions and exceptional pay hikes in the ensuing years.”

In 2011, he returned to RIL as vice president of global corporate security. In this role, he is responsible for developing strategy, maintaining oversight, and leading daily security operations. He manages a team of 90 security executives and more than 1,400 outsourced staff in the business infrastructure, life sciences, healthcare, education, and aviation sectors. In a typical day, his duties are as diverse as conducting field visits, auditing site security operations, participating in strategic reviews, and developing liaisons with business resiliency agencies and built networks within local and global security communities.

“I have been recommending the CPP program to all budding security professionals,” he says. “To me, CPP stands for Credibility, Proficiency, and Professionalism. This certification equipped me with the requisite credentials, competences, and confidence to voice a well-rounded professional opinion to senior leadership and be heard.”

Mishra opened his chapter’s May CPP review session by sharing his career journey. Perhaps the most important advice of his inspirational talk was that certification “is worth every bit of effort.”

“It is important to take the first step,” he notes. “Do not give in to procrastination. Be steady in your pursuit. It will take hundreds of hours of hard work and there are no shortcuts. Just as in your security practice, create a plan, make it time-bound, and follow through on it. You are bound to succeed.”

“This profession is full of challenges and rewards. There is never a dull moment in our industry. We put in the effort because we believe in our work, because we are passionate about it, and because we’re helping people who need it.”

PROFILE BY STEVEN BARNETT, ASIS COMMUNICATIONS COORDINATOR
JUDICIAL DECISIONS

PREVENTION. The Supreme Judicial Court of Massachusetts ruled that a college and its professors are not responsible for a student’s suicide but held that a duty to prevent suicide may exist in some instances.

Han Duy Nguyen was a graduate student at the Massachusetts Institute of Technology’s (MIT’s) Sloan School of Management and lived off campus. After his first two years at MIT, Nguyen contacted Sloan’s program coordinator for assistance with test-taking. He explained that he was failing his classes because he did not know how to take exams, according to court documents.

The coordinator referred Nguyen to an MIT student disability services office coordinator. After two meetings in July 2007, however, Nguyen told the program coordinator that the disability services office coordinator meetings were “absolutely no use,” the lawsuit said. The program coordinator then referred Nguyen to MIT’s mental health and counseling service.

After meeting with a psychologist who attempted to provide him with information on test anxiety, Nguyen interviews or made age-related comments, such as “Seasons 52 girls are younger and fresh,” according to the EEOC. Under the consent decree, Seasons 52 will compensate affected individuals 40 and older who applied to work at the restaurant chain but were denied positions because of their age. (EEOC v. Seasons 52, U.S. District Court for the Southern District of Florida, No. 15-cv-20561-JAL, 2018)

DISCRIMINATION
Restaurant chain Seasons 52 will pay $2.85 million and other relief to settle a class age discrimination lawsuit brought by the EEOC. In litigation, 135 individuals under sworn testimony said that Seasons 52 managers asked them their age during interviews or made age-related comments, such as “Seasons 52 girls are younger and fresh,” according to the EEOC. Under the consent decree, Seasons 52 will compensate affected individuals 40 and older who applied to work at the restaurant chain but were denied positions because of their age. (EEOC v. Seasons 52, U.S. District Court for the Southern District of Florida, No. 15-cv-20561-JAL, 2018)

HARASSMENT
Goodwill Industries of the East Bay Area and its affiliate, Calidad Industries Inc., will pay $850,000 to settle a sexual harassment and retaliation lawsuit brought by the U.S. Equal Employment Opportunity Commission (EEOC). The suit alleged that six female janitors on the night shift employed by Goodwill were subjected to routine sexual harassment by their supervisor, such as putting his arms around them. The employees reported the harassment to two managers, who were disciplined in retaliation for supporting their claims. (EEOC v. Goodwill Industries, U.S. District Court for the Northern District of California, No. 4:16-CV-07093, 2018)

GAMBLING
The U.S. Supreme Court struck down a U.S. law that prevented states from legalizing sports gambling. The law in question was the Professional and Amateur Sports Protection Act of 1992 (PASPA), which Congress promulgated to protect the integrity of sports, according to its sponsors. The law permitted live sports betting only in Nevada casinos. This ruling paves the way for other states to establish their own regulated sports betting. Writing for the majority, Justice Samuel Alito wrote that the law was a violation of the anti-commandeering doctrine—a provision of the 10th Amendment that says if the Constitution does not give a power to the U.S. federal government or keep it from U.S. states, it is reserved for the states or the people. (Murphy v. National Collegiate Athletic Association, U.S. Supreme Court, No. 16-476, 2018)

LEGAL HIGHLIGHTS

ISSUE: Discrimination
BILL: H.B. 1339
VENUE: New Hampshire
STATUS: Enacted
SIGNIFICANCE: Prohibits gender identity discrimination in employment, public accommodations, and housing.

ISSUE: Cybersecurity
BILL: H.R. 3776
VENUE: U.S. Senate Committee on Foreign Relations
STATUS: Received
SIGNIFICANCE: Would create the Office of Cyber Issues at the U.S. Department of State to replace the previously discontinued Office of the Coordinator for Cyber Issues.
initially refused services because he did not want to be stigmatized for doing so.

Nguyen went back to meeting with the psychologist, however, where he disclosed a history of depression and two prior suicide attempts during college. Roughly a month later in August 2007, Nguyen declined to meet with the MIT psychologist saying that he had made other arrangements for treatment with a local psychiatrist.

In September of that year, Nguyen emailed an assistant dean in the student support office asking for help taking exams and seeking counseling services that taught study skills. In a subsequent meeting, Nguyen disclosed to the assistant dean his history of mental health issues and depression, and that he was seeing a psychiatrist off campus.

Nguyen later met with the assistant dean again and shared that he’d been having frequent suicidal thoughts, but that he was seeing his psychiatrist and had an appointment with a therapist in Rhode Island. Nguyen also gave the assistant dean permission to contact the psychologist, the psychiatrist, and the therapist.

After the dean reached out to the psychiatrist and left a voicemail, however, Nguyen revoked his permission to contact the psychiatrist. According to court documents, Nguyen emailed the assistant dean that he would “like to keep the fact of my depression separate from my academic problems. I’d prefer that we not any further discuss the depression, that my academic problems can be framed in terms of a deficit in study skills instead.”

Nguyen continued to see a variety of professionals for treatment, and in 2009 he met with an MIT professor who told him an email he sent was unprofessio

ional and rude. Immediately after the meeting, Nguyen committed suicide by jumping off a bridge.

Nguyen’s family sued MIT, charging that the university and the professor had a duty to care for Nguyen and prevent his suicide because they were aware of his mental health problems.

MIT argued that Nguyen’s mental health issues predated his enrollment at the university and that he had refused to use MIT’s support services, opting to receive treatment from other professionals.

A district court dismissed Nguyen’s family’s case, which reached the Supreme Judicial Court of Massachusetts on appeal.

That court also dismissed the case, explaining that the university did not have a duty to prevent him from committing suicide and that “a 25-year-old graduate student’s right to privacy, autonomy, and self-determination were properly respected.”

Despite the dismissal, however, the court said that colleges could have a duty to protect their students if they know of a previous suicide attempt...
while the student was enrolled, or if he or she communicated an intention to commit suicide.

The court wrote that “…failing to act to intervene to save a young person’s life, when it was within the university’s knowledge and power to do so” would carry “moral blameworthiness” for the university and those with that knowledge. (Nguyen v. MIT, Supreme Judicial Court of Massachusetts, No. SJC-12329, 2018)

RETENTION. A former CIA contractor pleaded guilty to illegally retaining classified materials during his employment.

Reynaldo B. Regis, 53, was assigned to the CIA as a contract worker between August 2006 and November 2016. During that time frame, he used classified CIA databases to conduct unauthorized searches and copied classified information into notebooks for his personal use. Regis then took those notebooks home without authorization, according to the U.S. Department of Justice (DOJ).

“When initially interviewed by federal law enforcement, Regis lied about having done so,” the DOJ said. “During a search of his home, FBI agents recovered approximately 60 notebooks containing classified information. The classified information contained in the notebooks included information relating to highly sensitive intelligence reports, disclosure of which could cause serious damage to the national security.”

Regis could face up to a maximum of five years in U.S. federal prison for his crimes. His sentencing is scheduled for September 21, 2018. (U.S. v. Regis, U.S. District Court for the District of Virginia, No. 1:18-cr-209, 2018)

AIRPORT SECURITY. Three Muslim-American men will be allowed to move forward with a case against FBI agents for detaining them at airports, a U.S. court of appeals ruled.

Muhammad Tanvir, Jameel Algibah, and Naveed Shinwari were all born abroad and legally immigrated to the United States early in their lives. All three were approached by U.S. federal agents and asked to serve as informants for the FBI.

“Specifically, plaintiffs were asked to gather information on members of Muslim communities and report that information to the FBI,” according to court documents. “In some instances, the FBI’s request was accompanied with severe pressure, including threats of deportation or arrest; in others, the request was accompanied by promises of financial and other assistance.”

All three plaintiffs refused to participate, based in part on their religious beliefs. In response, according to their lawsuit, the agents put the plaintiffs on the national “No Fly List,” despite never having posed, or being accused of posing, a threat to aviation safety.

These actions, the plaintiffs said, forced them into an “impermissible choice” between following their religious beliefs and being placed on the “No Fly List.” They alleged it “placed a substantial burden on their exercise of religion,” court documents said.

Being placed on the “No Fly List” also caused the plaintiffs to allegedly suffer emotional distress, reputational harm, and economic loss, in addition to prohibiting them from flying for several years.

In response, Tanvir, Algibah, and Shinwari filed suit against senior U.S. law enforcement officials and others, alleging that for refusing to serve as informants they had been placed on the “No Fly List”—a violation of their First Amendment and Religious Freedom Restoration Act (RFRA) rights.

The plaintiffs and defendants agreed to stay the official capacity claims, and a district court dismissed the individual capacity claims because it held that “RFRA does not permit the recovery of money damages against federal officers sued in their individual capacities,” according to court documents.

The plaintiffs appealed the decision, and the U.S. Court of Appeals for the Second Circuit reversed the district court’s decision. The appellate court concluded that the RFRA does authorize individual capacity claims against U.S. federal officers, allowing the plaintiffs’ suit to move forward.

“…we hold that RFRA…authorizes a plaintiff to bring individual capacity claims against federal officers or other ‘person[s] acting under color of [federal] law,’” the court explained.

The appellate court also said that the RFRA allows plaintiffs to obtain relief against the government, including in the form of money damages from U.S. federal officers sued in their individual capacities.

The appellate court reversed the district court’s decision and remanded the case. (Tanvir v. Tanzin, U.S. Court of Appeals for the Second Circuit, No. 16-1176, 2018)
REGULATIONS

DRESS CODES. New guidelines from the United Kingdom’s Government Equalities Office prohibit employers from singling out women in dress codes.

The guidance is designed to prevent sexism in the workplace and will require employers to have similar dress standards for men and women at work.

“It is best to avoid gender specific prescriptive requirements, for example the requirement to wear high heels,” the guidance said. “Any requirement to wear make-up, skirts, have manicured nails, certain hairstyles, or specific types of hosiery is likely to be unlawful.”

The guidance also says that transgender employees should be allowed to dress in the manner that reflects their gender identity, including being provided a staff uniform that matches their gender identity.

Additionally, the guidance says employers should “be flexible and not set dress codes which prohibit religious symbols that do not interfere with an employee’s work.”

INFORMATION TECHNOLOGY. U.S. President Donald Trump issued an executive order to empower government agency chief information officers (CIOs) to ensure system security, efficiency, accessibility, and effectiveness.

“Enhancing the effectiveness of agency CIOs will better position agencies to modernize their IT systems, execute IT programs more efficiently, reduce cybersecurity risks, and serve the American people well,” the order said.

Under this executive order, CIOs will report directly to the agency head, serve as the primary strategic advisor to the agency head on the use of IT, have a role in annual and multiyear planning related to IT, and approve the appointment of any component CIO within that agency.

LEGALIZATION

United States

BACKGROUND CHECKS. Georgia Governor Nathan Deal signed legislation into law that requires nursing homes and long-term care facilities to run extensive background checks on employees.

The “Georgia Long-Term Care Background Check Program” requires employers with workers that provide “direct access” to seniors in long-term care facilities to conduct national background checks on those employees. The law applies to businesses that provide personal home care, assisted living communities, private home care, home health agency, hospice care, nursing home care, skilled nursing facility, or adult day care.

The law, however, excludes physicians, dentists, nurses, and pharmacists who are licensed by the state of Georgia. It also excludes individuals that are contracted with an organization but do not provide direct care to patients, such as accounting staff.

This requirement goes into effect on October 1, 2019. It was passed in response to a rise in elder abuse in Georgia.

New York

HARASSMENT. New York City Mayor Bill de Blasio signed legislation into law designed to protect employees from sexual harassment.

The Stop Sexual Harassment in NYC Act requires employers with 15 or more employees to conduct a yearly interactive anti-sexual harassment training that meets certain requirements, including descriptions and practical examples of sexual harassment, internal complaint processes available, and the importance of bystander intervention.

The law also requires supervisors and managers to receive additional training, including on their responsibilities to prevent sexual harassment and retaliation.

Additionally, the law extends the statute of limitations for filing claims under the New York City Human Rights Law from one year to three years after the alleged conduct occurred.

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

ASIS STORE

Your comprehensive clearinghouse for security-related publications, certification reference materials, and ASIS merchandise.

Go to asisonline.org/store to browse offerings and start shopping.
PARTNERSHIPS AND DEALS

**Acuant** announced a strategic integration with **Okta** to provide enterprise customers with reliable, seamless authentication.

**AITHERAS** is partnering with **VS Systems** to expand public safety with **U.S. federal and state agencies, local law enforcement, and school campuses nationwide.**

**Ashridge Group** is working with **VPS** to provide security for a major energy provider as it recommissions two compressor stations in Cambridgeshire, England.

**HID Global** was appointed the official ticket producer for the **2018 FIFA World Cup**, delivering more than 3 million secure RFID tickets for the 64 matches held in 11 host cities of the Russian Federation.

**Hanwha** Wisenet devices are integrated within **Arteco NEXT Video Event Management Software** and include embedded video and audio analytics applications.

**Preferred Office Properties** selected **Datawatch Systems, Inc.**, to integrate access and security technology at **Three Ravinia**, a 31-story office building near Atlanta.

**EMERgency24** is integrating the **SecuraTrac Mobile Defender** into its mass notification system to enable two-way dialogues about emergency events.

**The FIDO Alliance** announced that **Facebook** was appointed to its board of directors to help reduce reliance on passwords by using stronger, simpler authentication.

**Hanwha** Wisenet devices are integrated within **Arteco NEXT Video Event Management Software** and include embedded video and audio analytics applications.

The LaHaye Fitness and Recreation Center at **Liberty University** is using **Boon Edam Speedlane 300 turnstiles** for secure access control.

**Preferred Office Properties** selected **Datawatch Systems, Inc.**, to integrate access and security technology at **Three Ravinia**, a 31-story office building near Atlanta.

**EMERgency24** is integrating the **SecuraTrac Mobile Defender** into its mass notification system to enable two-way dialogues about emergency events.

**The FIDO Alliance** announced that **Facebook** was appointed to its board of directors to help reduce reliance on passwords by using stronger, simpler authentication.

**Hanwha** Wisenet devices are integrated within **Arteco NEXT Video Event Management Software** and include embedded video and audio analytics applications.

**HID Global** was appointed the official ticket producer for the **2018 FIFA World Cup**, delivering more than 3 million secure RFID tickets for the 64 matches held in 11 host cities of the Russian Federation.

**GAME STRATEGY**

**PORTABLE BARRIER SYSTEMS** from **Delta Scientific** were selected to protect people attending the 2018 **Commonwealth Games** on the Gold Coast, Queensland, Australia. The games featured 4,400 athletes from 70 Commonwealth nations competing in 19 sports.

Security planning began years prior to the games. Perimeter security measures were aligned with the recently implemented Australia and New Zealand Counter Terrorism Committee strategy for the protection of places of mass gatherings, which includes implementation of hostile vehicle mitigation (HVM) measures at key locations. As the Australian partner of Delta Scientific, **Knight Brothers Pty. Ltd.** secured the contract for the vehicle barrier systems and liaised with organizers to ensure that specific security measures could be achieved.

Barriers protected major event venues, including the main games stadium, Gold Coast Convention Centre, the Athletes Village, and critical streets. Portable barriers enabled access for emergency and authorized vehicles during the event. At the games, standalone battery-operated hydraulic systems with supplementary solar power charging and remote-control operation activated the barriers and kept traffic moving.

**PROMOTIONS**

**Acuant** announced a strategic integration with **Okta** to provide enterprise customers with reliable, seamless authentication.

**AITHERAS** is partnering with **VS Systems** to expand public safety with **U.S. federal and state agencies, local law enforcement, and school campuses nationwide.**

**Ashridge Group** is working with **VPS** to provide security for a major energy provider as it recommissions two compressor stations in Cambridgeshire, England.

**HID Global** was appointed the official ticket producer for the **2018 FIFA World Cup**, delivering more than 3 million secure RFID tickets for the 64 matches held in 11 host cities of the Russian Federation.
IDEAL Networks and Mayflex have formed a distribution partnership.

Just Add Power announced that its 3G Ultra Over IP platform is delivering content to the new video wall system installed in the atrium of the University of Indianapolis Health Pavilion, allowing the school to share information across campus.

Oncam partnered with BDF Securezza Latina to provide the company’s full suite of products as Italy’s first Oncam distributor.

Pivot3 expanded its relationship with HyTrust to deliver secure, compliant video surveillance infrastructure solutions with high levels of data protection.

PSA announced that Active Risk Survival, Inc., joined its Business Solutions Provider program to provide tactical awareness training for sales professionals representing security integrators and manufacturers.

RTI and Channel Vision Technology integrated Channel Vision’s Elite Series SI-8000 front door station with RTI control devices featuring intercom capabilities.

Shieldox is collaborating with Microsoft Information Protection to extend the protection capabilities of information collaboration within the walls of an organization and beyond, while in motion.

Thales extended its distribution agreement with Arrow Electronics to bring data security solutions and services to more territories in Europe, the Middle East, and Africa.

Maecenas Fine Art, a blockchain-based art marketplace, adopted Thomson Reuters World-Check to meet due diligence obligations and mitigate financial crime risk.

Vicon Industries, Inc., implemented its end-to-end Valerus video management system at the Greek American Institute in Bronx, New York.

Video Mount Products named Ascheman Marketing Group its new Central Midwest Representative. Vietnamese telco VinaPhone is partnering with German security specialist Secucloud to protect customers’ Web interactions.

GOVERNMENT CONTRACTS

American Signal Corporation has been contracted by the city of Milwaukee, Wisconsin, to retrofit the county’s 57 sirens with protection against activation tampering.

Avigilon Corporation, a Motorola Solutions company, was selected by the Long Beach Housing Authority to improve safety for its residents in Long Beach, New York.

Elbit Systems Ltd. announced that Canadian subsidiary GeoSpectrum Technologies Inc. was awarded a contract from STX Engine Co. to deliver its Underwater Sound Source System and software package to the Republic of Korea Navy.

The Electrical Safety Foundation International won a Fire Prevention and Safety Grant from the U.S. Department of Homeland Security to develop a fire safety awareness campaign that targets older adults.

Hikvision USA, Inc., and ADT/Protection 1 provided a security system upgrade for Battleship North Carolina, a veteran memorial in Wilmington, North Carolina.

Ionic Security Inc. was awarded a Phase 4 contract by the U.S. Department of Homeland Security Science and Technology Directorate’s Silicon Valley Innovation Program to commercialize data security for the Internet of Things.

The European Commission Horizon 2020 Research & Innovation Programme awarded MazeBolt Technologies a grant for its Non-Disruptive DDoS Testing Technology.

NAPCO Security Technologies, Inc., announced that Allegheny County Public Schools in North Carolina will be using NAPCO’s Trilogy Networx Series Locks.

The U.S. Air Force awarded a contract to Raytheon for its all-digital radar warning receiver.

Seal Network was selected by the European Commission to co-create a blockchain-based anticounterfeiting platform for Europe.

Serco Inc. won a contract to provide life cycle sustainment, acquisition, and integration support for Anti-Terrorism/Force Protection Naval Electronic Surveillance Systems for U.S. Naval Facilities Engineering Command and other Department of Defense agencies; the Department of Homeland Security; Marine Corps; and other government programs.

Smiths Detection reports that the Airports Authority of India placed an order for its CTX 9800 DSI systems.

TagMaster North America, Inc., in conjunction with International Controls and Equipment, deployed a parking solution for law enforcement and emergency service vehicle access for the Sterling Heights Municipality in Michigan.
Emergency callers to 911 benefit from streamlined public safety call handling from Total Response, which is being used by the Norwalk Police Department in Connecticut.

Unisys Corporation announced that U.S. Customs and Border Protection, part of the Department of Homeland Security, selected the company to develop, operate, and manage systems used for risk assessments of people and cargo entering the United States.

Denbigh High School in Virginia purchased a RescueSim aviation system from VSTEP Simulation to teach students about safety standards and emergency readiness in the school’s Aviation Academy. The purchase was made through FAAC.

AWARDS AND CERTIFICATIONS

ASSA ABLOY announced that several of its products were named 2017 GOOD DESIGN award winners from The Chicago Athenaeum: Museum of Architecture and Design.

Boon Edam Inc. announced that its Speedlane Swing and Open optical turnstiles are certified to conform with UL standards 325 and 2593, and CSA 22.2 for Canada.

Conduent Incorporated won a challenge prize from the U.S. Department of Justice for crime forecasting using technology to predict where the larger concentration of street crimes would occur in Portland, Oregon.

DERMALOG set a new world record by matching 3.6 billion fingerprints per second, which was certified by SGS-TÜV Saar.

Feenics participated in CA Technologies’ Veracode Verified and received the seal of Verified by Veracode.

The International Card Manufacturers Association gave IDEMIA an award for redesigning the California Department of Motor Vehicles’ REAL ID compliant driver’s license and ID card.

Jumio announced that its Netverify solution was named Best Product in Biometrics and Hot Company in Fraud Prevention at the 2018 InfoSec Awards created by Cyber Defense magazine.

March Networks is Cyber Essentials Canada certified by the National Cyber Security Centre.

Masergy was named the Most Innovative Managed Security Service Provider in the 2018 InfoSec Awards based on enhancements to the Unified Enterprise Security managed detection and response platform.

Milestone Systems was voted one of the 100 Best Companies to Work for in Oregon by Oregon Business magazine.

MOBOTIX was named a Platinum Technology Partner by Genetec.

Securitec Screening Solutions won the Rising Star award for its modern court data software from the Roanoke–Blacksburg Technology Council.

Suprema ID announced that its BioMini Plus 2 fingerprint authentication scanner received a UIDAI Registered Device Level certification from the Government of India Standardization Testing & Quality Certification.

ANNOUNCEMENTS

ASSA ABLOY will acquire Concept Frames, Inc., a manufacturer of custom-made steel doors and frames.

Axon acquired VIEVU, the public safety camera provider and a subsidiary of the Safariland Group.

Biamp Systems announced a consultant program that will streamline the

<table>
<thead>
<tr>
<th>WHO</th>
<th>WHAT</th>
<th>OF/WITH</th>
<th>RESULT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Canon, Inc.</td>
<td>ACQUISITION</td>
<td>BriefCam</td>
<td>The move complements Canon’s previous acquisitions of AXIS Communications and Milestone Systems with an innovative video content analytics solution.</td>
</tr>
<tr>
<td>TruTag Technologies</td>
<td>ALLIANCE</td>
<td>Tag-it Tech, Inc.</td>
<td>The goal of the alliance is to bring safety, security, and traceability to the North American cannabis market.</td>
</tr>
<tr>
<td>Siemens Building</td>
<td>ACQUISITION</td>
<td>Enlighted, Inc.</td>
<td>The two companies will enhance building performance by gathering multiple streams of data to improve transparency and efficiency.</td>
</tr>
<tr>
<td>technologies</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Division</td>
<td>PARTNERSHIP</td>
<td>Intelligent Security Systems</td>
<td>The partnership will provide a practical solution to the monitoring of transportation infrastructure, where maximum situational awareness is paramount.</td>
</tr>
</tbody>
</table>
process of identifying and specifying audiovisual solutions.

Convergint Technologies acquired Integrators Australia, a systems integrator based in Port Melbourne, Victoria, Australia, and French systems integrator Astrec Security, based in suburban Paris.

Edesix opened a new office in the United Arab Emirates.

Everbridge, Inc., completed its acquisition of Unified Messaging Systems ASA.

Myanmar Strategic Holdings Ltd. announced that its subsidiary, Myanmar Strategic Services Pte. Ltd., has exchanged contracts for the acquisition of the entire issued share capital of EXERA.

Fujitsu Limited and Fujitsu Friontech Limited announced that sales of the Fujitsu Biometric Authentication PalmSecure palm vein authentication series have exceeded one million units.

Holland & Knight established a cybersecurity, data breach, and privacy team within the firm’s litigation section.

IndigoVision, Boston Networks, and Dell Technologies provided a security system to Social Bite, whose mission is to end homelessness in Scotland.

Brevard Nam Knights and INTEL-LEO combined resources to donate 15 cooling vests to the Brevard County Sheriff’s Office K9 Unit in Florida.

LogPoint established its base for North American operations in Boston, Massachusetts.

Mission 500 raised $113,000 at its ninth annual Security 5K/2K Run/Walk at this year’s ISC West.


Nortek Security & Control LLC acquired IntelliVision Technologies Corp.

The North Dakota State University Department of Computer Science announced the launch of four new cybersecurity-enhanced graduate degree programs.

ONVIF is celebrating its 10th anniversary this year.

SafeToNet Limited acquired Toronto-based VISR Inc., which specializes in using artificial intelligence to help detect the emotional well-being of children online.

TruTag Technologies was part of the Hawaii Pavilion representing Hawaii Life Sciences at the BIO International Convention.

Valiant Integrated Services completed the purchase of Cubic Global Defense Services.

VisioLogix Corporation is offering a free cloud-based evidence management service to U.S. law enforcement agencies.
The newest iteration of the NetAXS-123 Web-based access control solution from **Honeywell** of Louisville, Kentucky, offers increased efficiency with a faster, user-friendly design that makes it simple to install and easy to operate and maintain. Optimized for Google Chrome, NetAXS-123 version 6.0 offers flexibility to be managed through the new embedded interface, in the cloud via MAXPRO Cloud, or via on-premise software with WIN-PAK’s integrated security suite. NetAXS-123 allows users to securely manage systems anywhere there is an Internet connection with no dedicated PC or software costs. Version 6.0 offers single-interface management including consolidated alarm and event management for multi-panel loops, as well as systemwide back-up and restore.

**Qognify** of Pearl River, New York, introduced a physical security information management (PSIM) based solution, featuring pre- or auto-configured components to minimize the time and cost of implementation. Qognify ISM reduces the configuration drain associated with complex PSIM projects. New automation tools provide simplicity for the operator, including automated video verification configuration, smart data intake, security subsystems dashboards, management dashboards, and more. The system can highlight trends and data for organizational improvement by monitoring key metrics such as number of incidents, user activity, resolution times, and incident locations.

**OpenEye** of Liberty Lake, Washington, released version 1.4 of OpenEye Web Services (OWS), which includes new integrations, spot monitor functionality, support for an HD analog retrofit solution, and advanced camera management. Updates give users more control over who can access cameras with advanced camera management at the User Group level, instead of global settings managed on each individual recorder. New alarm panel and central station integrations in OWS give users more ways to access their video, and the new Thumbnail Report gives them a quick and easy way to check on their business.

**Just Add Power** (J+P) of Largo, Florida, announced that its 3G Ultra HD Over IP series of solutions now deliver Ultra HD video signals over IP with just 16 milliseconds of latency from source to screen. Leveraging a common IP infrastructure, J+P’s devices allow integrators to choose the model that best meets clients’ hardware and budget requirements. These solutions are designed for any size UHD distribution and matrixing application. Made in the United States, the non-OEM solutions are designed to remove the limitations and expense of traditional matrixes and replace them with a more scalable, flexible, and reliable approach.
CROSSMATCH of Palm Beach Gardens, Florida, introduced the NOMAD 30 Pocket Reader, a FAP 30 PIV single fingerprint reader that incorporates the latest in fingerprinting technology. The device uses a space-saving capacitive thin-film transistor sensor that provides superior outdoor and bright-ambient-light performance and is not impacted by tattooed or stained fingers. The reader connects to a range of mobile computing devices, including cell phones, tablets, and laptops. It is easily shared or swapped as shifts change or use cases demand. Bundled with the ArcID Mobile application on a smart device, the reader offers reliable PIV-level identity assurance for law enforcement, government, and banking applications. 805

FINGERPRINT READER

PPSS GROUP of Knaresborough, United Kingdom, specializes in the design, development, and manufacturing of high-performance body armor and clothing with protection from firearms, edged weapons, and hypodermic needles, as well as blunt force trauma and human bites. The firm’s stab-resistant vests are now being issued to international homeland security agencies, such as the prison service, border control, immigration, and customs, as well as privately owned security and facility management firms. 806

CROSSMATCH

PROTECTIVE VESTS

CIRCLE #  PAGE #  CIRCLE #  PAGE #
13  Abloy Security, Inc. 25  Mission 500 59
14  Ameristar Security Products 27  NA PCO Security Services 76
02  Assa Abloy 04  PATLITE 32
20  Commport Technologies 39  Prosegur 41
25  Detex Corporation 13  Quantum Secure 06
09  dormakaba 19  Robert H. Perry & Associates 20
05  DSI (Designed Security Inc.) 11  SDC – (Security Door Controls) 37
07  DSX Access Systems, Inc. 15  SecurAmerica 2-3
11  G4S 21  Special Response Corporation 23
17  MEDC 75  TSCM America 40

ADVERTISERS ONLINE

Abloy Security, Inc.
www.abloyusa.com
Ameristar Security Products
www.ameristarsecurity.com
ASSA ABLOY
www.assalocallock.com
Commport Technologies
www.commport.com
Detex Corporation
www.detesign.com
dormakaba
www.dormakaba.com
DSI (Designed Security Inc.)
www.dsiglobal.com
DSX Access Systems, Inc.
www.interlockinc.com
G4S
www.g4s.com
MEDC
www.michiganbusiness.org
Mission 500
www.mission500.org
NA PCO Security Services
www.napcosecurity.com
PATLITE
www.patlite.com
Prosegur
www.prosegur.com
Quantum Secure
www.quantumsecure.com
Robert H. Perry & Associates
www.roberthperry.com
SDC – Security Door Controls
www.sdcsecurity.com
SecurAmerica
www.securityusa.com
Special Response Corporation
www.specialresponse.com
TSCM America
www.tscmamerica.com

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.
European terrorist attacks have been tracked by Europol since 2007. Since then, the number of terrorist attacks has decreased each year, largely due to a drop in the number of separatist attacks. Meanwhile, the threat of jihadist terror has increased, and in 2017 the total number of attacks increased from 142 in 2016 to 205 in 2017.

**SNAPSHOT**

**Total Number of Attacks in 2017**

![205 attacks chart]

- **33** Foiled, failed, and completed jihadist terrorist attacks
  - BELGIUM 2
  - FINLAND 1
  - FRANCE 11
  - GERMANY 1
  - ITALY 1
  - SPAIN 2
  - SWEDEN 1
  - UNITED KINGDOM 14

- **137** Foiled, failed, and completed separatist terrorist attacks
  - FRANCE 42
  - NORTHERN IRELAND 88
  - SPAIN 7

- **24** Foiled, failed, and completed left-wing terrorist attacks
  - FRANCE 1
  - GERMANY 1
  - GREECE 8
  - ITALY 7
  - SPAIN 7

- **6** Foiled, failed, and completed unspecified terrorist attacks
  - ITALY 6

- **5** Foiled, failed, and completed right-wing terrorist attacks
  - UNITED KINGDOM 5

**SOURCE:** European Union Terrorism Situation and Trend Report 2018, Europol, June 2018
As cyber becomes more embedded in life and business, one state is developing revolutionary new initiatives to advance cybersecurity. Michigan. The nation's leader in tech job growth, our state is also home to the Michigan Cyber Range, a virtual unclassified platform for cyber exercises, product testing and digital forensics to foster cyber talent and industry engagement. Which makes Michigan a smart move for cybersecurity businesses.
how safe is your Campus?

Know with Napco, solutions for all needs & budgets

See us at GSX (ASIS) Booth 1543

Napco • Alarm Lock • Continental Access • Marks USA

Contact us for Free Security Evaluation 800.645.9445 or download our Campus Safety Whitepaper & S.A.V.I. Self Diagnostic Tool at www.savischool.com

For product info #33 securitymgmt.hotims.com