Issue & Beyond

- **Biosecurity**
  Producers’ efforts to protect the food supply.

- **National Security**
  Deaths from terror attacks decline in the world.

32

LONELY, ONLINE, ANGRY
THANK YOU!
WE RAISED $65,459 FOR THE ASIS FOUNDATION!
THANK YOU!

Last year, I asked you to participate in the ASIS Foundation Matching Gift Challenge, and I am happy to announce that the Foundation raised over $65,000 in the last three months of 2018 and earned a $20,000 matching gift from me.

Your donations make such a difference to security professionals and ASIS members. With your support, we raised enough money to fund the following programs for 2019:

100 CPP Accelerator Scholarships: Members from all around the world were able to take the CPP exam free of charge.

20 Road to Certification Scholarships: Members received free certification preparation materials.

One $10,000 Security Education Grant: Helped one ASIS chapter host a 2-day educational program.

If you would like to apply for any of these awards, you can visit asisfoundation.org. Thank you again for all your support of the ASIS Foundation!

If you have questions, I’m always available; you can call my office line, which is 404-926-4202.
The keys to a smarter, safer city

Teamwork and innovation:
A winning combination

The City of Atlanta is focused on protecting its residents and businesses while also creating a safe and welcoming environment for tourists, like the thousands who recently attended the Super Bowl. Private and public sector partnerships between the Atlanta Police Foundation, the Atlanta Police Department and the business and philanthropic community have led to innovative solutions, including 24/7 surveillance throughout the city. Emergency personnel now have the ability to better prepare and respond more rapidly—delivering a big win for everyone.

From safe cities, stadiums, and transportation to retail, education and healthcare, discover how Axis Communications partners with you to help create a smarter, safer world. Visit our Axis Experience Centers:
- Boston, MA
- Chicago, IL
- Dallas, TX
- Fort Lauderdale, FL
- Los Angeles, CA
- Washington, DC

Discover innovative security and business solutions at www.axis-communications.com/atlanta

For product info #2 securitymgmt.hotims.com
“North America saw the largest increase in the impact of terrorism from 2016 to 2017, with the majority of terrorist activity taking place in the United States.”

Findings from the latest version of the Global Terrorism Index. It also found that this is the fourth successive year that terrorist-related deaths have risen in North America, from 65 in 2016 to 85 in 2017. PAGE 22

“The current emphasis on efforts to address gender equality and eliminate sexual harassment in the workplace runs counter to the Incel belief that women are inherently inferior to men.”

Behavioral science expert Steven Crimando writing about the extremist movement of involuntary celibates, or Incels. PAGE 35

Approximate number of security professionals who will gather in Chicago 8-12 September for Global Security Exchange 2019. PAGE 56

Estimated amount that the spread of antimicrobial resistance among disease-causing pathogens will cost the world economy on an annual basis by 2050, according to the Food & Agriculture Organization of the United Nations. PAGE 20
GSX is the security industry’s premier global event. Enhance your professional development by meeting new colleagues and business partners, researching and purchasing cutting-edge products, taking home new insights on market trends, and earning continuing education credits—all in one place at one time.

Registration is open! GSX.org/SM
COVER STORY

32

ALONE TOGETHER AND ANGRY: AN INCEL REVOLUTION

Recently designated a hate group by the Southern Poverty Law Center, Incels exist primarily as an online subculture espousing male supremacy and committing acts of violence against people who seem to have an easy time finding love and acceptance.

By Steven Crimando

LIABILITY
ON-DUTY AND VULNERABLE

Police and security officers are both vulnerable to civil rights-related violations under U.S. federal law.

By Brian Johnson and Naoki Kanaboshi

STRATEGY
RETURN ON EDUCATIONAL INVESTMENT

An annual English-language course held in Madrid by IE Business School and ASIS International tackles business school cases on corporate strategy and leadership.

By Michael A. Gips, CPP

EMERGENCY MANAGEMENT
SAFETY AND SECURITY: BUILDING RELATIONSHIPS FOR EFFECTIVE MANAGEMENT

As natural disasters worsen, both security and mitigation are vital components in today’s emergency management landscape.

By A. Benjamin Mannes, CPP
ELEVATE
YOUR PROFESSIONAL DEVELOPMENT
JOIN US IN ATLANTA, GA

This year’s program format includes a general session providing unparalleled opportunities for you to connect with other programs’ attendees, exchange ideas, and expand your professional network.

EXECUTIVE PROTECTION
24-25 June | Up to 14 CPEs

This comprehensive program covers the fundamental skills and procedures required to provide effective personal protection in this highly specialized field. Case studies reinforce the techniques and teach best practices.

IMPLEMENTING ENTERPRISE SECURITY RISK MANAGEMENT
24-25 June | Up to 14 CPEs

Increase your understanding of this strategic security program management approach. You’ll learn how to develop a security program in the ESRM model and how to use a business approach to communicate security concepts to the C-suite.

ASIS ASSETS PROTECTION COURSE™: PRACTICAL APPLICATIONS (APC II)
24-26 June | Up to 23 CPEs | Newly revised

This program guides you through real-life case studies and provides proven solutions, best practices, and field-tested strategies in five key areas. Gain conceptual insights on current trends and methodologies for successfully mitigating risks.

RISK, THREAT, AND VULNERABILITY ASSESSMENT
24-26 June | Up to 18 CPEs

Examine all facets of planning and implementing a successful risk assessment program in any type of organization, large or small, public or private. Hands-on exercises and a site visit provide practical application.

SAVE $100
When you register by 11 May.

Hotel deadline is 7 June.

ASIS WEBINARS—24/7 LEARNING OPPORTUNITIES
See what’s coming up:

20 March Travel Safety and Security for Traveling Abroad

FIND DETAILS ON ALL PROGRAMS AT
ASISONLINE.ORG/JUNECLASS
## CONTENTS

### DEPARTMENTS

<table>
<thead>
<tr>
<th>Page</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>LETTERS TO THE EDITOR</td>
</tr>
<tr>
<td>12</td>
<td>CONTRIBUTING AUTHORS</td>
</tr>
<tr>
<td>14</td>
<td>SM DIGITAL</td>
</tr>
<tr>
<td>16</td>
<td>EDITOR’S NOTE</td>
</tr>
<tr>
<td>22</td>
<td>NATIONAL SECURITY</td>
</tr>
<tr>
<td>26</td>
<td>CASE STUDY</td>
</tr>
<tr>
<td>28</td>
<td>CYBERSECURITY</td>
</tr>
<tr>
<td>56</td>
<td>ASIS NEWS</td>
</tr>
<tr>
<td>57</td>
<td>ASIS BOARD OF DIRECTORS</td>
</tr>
<tr>
<td>60</td>
<td>LEGAL REPORT</td>
</tr>
<tr>
<td>63</td>
<td>ADVERTISER INDEX</td>
</tr>
<tr>
<td>64</td>
<td>INDUSTRY NEWS</td>
</tr>
<tr>
<td>65</td>
<td>MARKETPLACE</td>
</tr>
<tr>
<td>66</td>
<td>THE LIST</td>
</tr>
</tbody>
</table>

---

### MARCH 2019

**LETTERS TO THE EDITOR**

Modern technology: perfectly addictive and problematic.

---

**NATIONAL SECURITY**

Terror attack fatalities have declined, but terrorism affected more countries than in previous years, new research shows.

*By Lilly Chapa*

---

**CASE STUDY**

Epiphany Healthcare uses a system to securely manage medical tests results.

*By Lilly Chapa*

---

**CYBERSECURITY**

U.S. officials are turning their focus to securing the 2020 elections.

*By Megan Gates*

---

**ASIS NEWS**

The industry’s flagship event, Global Security Exchange 2019, will be held 8-12 September in Chicago.

*By Mark Tarallo*

---

**LEGAL REPORT**

A Florida law may provide police officers immunity from prosecution.

*By Megan Gates*

---

**ADVERTISER INDEX**

---

**INDUSTRY NEWS**

---

**THE LIST**

Five steps for optimizing crisis notification.

*By Dorian Amstel, CPP*
LETTER TO THE EDITOR

I am writing about the January 2019 article, “How to Investigate #MeToo.” The author may have been well-meaning, but this statement in his opening paragraph reveals how much equivocation persists on this topic: “When true, the events behind these stories can leave the victims and their families scarred and damaged for life.”

Why is there a need to equivocate in this statement by suggesting that victims’ “stories” may not be true? Given the pain and suffering endured by those who seek justice for sexual assault and harassment, it is not only unlikely but there is no evidence to support that many victims are filing false claims. Sexual abusers and harassers are masters of committing their crimes when there are no witnesses so they will have plausible deniability. And so, the cycle of victim blaming continues.

It would have been easy for the author to say, “Sexual assault and harassment often leave victims and their families scarred and damaged for life.” This truthful statement avoids introducing the opportunity for those who treat #MeToo as a hoax perpetrated by manhaters and opportunists to once again dismiss the problem. Unfortunately, the author’s statement opens the door for that thinking and, hopefully unintentionally, enables it. On such a sensitive topic as this, please choose your words more carefully and check your personal biases at the door.

SUSAN SMITH
A 30-year veteran in the security and IT publishing industries

AUTHOR RESPONSE

Thank you for taking the time to comment on my article. My use of the formation, “when true” in the first paragraph was in reference to the previous sentence: “Many of these reports follow a similar scenario—a middle-aged, executive-level man allegedly uses his power and influence to target, and sometimes sexually assault, a person over whom he has power.” The phrase is not intended to attack the accuser. I am sure all would agree that regardless of the source, a professional investigator—assuming of course, that he or she follows industry standards such as the ASIS International Investigation Standard (ASIS/ANSI INV.1-2015) and best practices—should assert only that which can be sufficiently and properly proven.

GENE FERRARO, CPP, PCI, CFE, SPHR, SHRM-SCP
Chief Executive
Forensic Pathways
Denver, Colorado

COVERING THE #METOO MOVEMENT

Security personnel must maintain objectivity and apply best practices to all internal investigations to ensure that the results of these investigations are accurate. This, in turn, helps investigators gain the trust and cooperation of employees.

While it may seem biased against the accuser to approach all parties involved in a sexual harassment accusation as equally credible, it is crucial to assess each situation thoroughly and on its own merits.

For a more detailed account of this approach, readers can reference “Fair and Neutral,” an article by Steve C. Millwee, CPP, in our March 2018 issue. Millwee addresses why, when addressing sexual harassment allegations, investigators must be sure not to form an opinion about the truth of the accusations until the investigation is complete.

Millwee writes: “When these accusations come out, many organizations are quick to end established relationships with the person being accused—usually to protect the enterprise and the brand, but also to show support for those reporting the allegations. However, it is important to remember that conducting a competent investigation to uncover the truth is vital. It protects the enterprise and all parties involved, and it will encourage other victims of misconduct to come forward.”

Security Management is pleased to offer a forum to discuss this critical issue. We welcome comments on the topic via letters to the editor, on our social media feeds, and through ASIS Connects.

TERESA ANDERSON
Vice President, Editorial
Editor-in-Chief, Security Management

Tell us how we are doing. Letters to the editor are welcomed and encouraged on all matters pertinent to security professionals. Letters should be emailed to teresa.anderson@asisonline.org. Submissions may be edited for length and clarity.
12th Annual CSO Summit
5-7 May 2019
Capital Hilton, Washington, D.C.

CSO Influence: Adding Value ACROSS THE ENTERPRISE

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

Register today at csocenter.org/SummitRegistration
This event is open only to CSO Center members and those eligible for membership.
Steven Crimando is the principal of Behavioral Science Applications, a training and consulting firm focused on the human element in violence prevention and response. He serves as a consultant and trainer for many multinational corporations, government agencies, major city police departments, and military programs.

With 30 years of experience in the field, Crimando was involved in response to the 9/11 and 1993 World Trade Center attacks, as well as New Jersey’s anthrax screening center and other acts of international terrorism. He has contributed to several books, authored professional articles, and serves as an expert to the courts and major media outlets on the topic of violence prevention.

“Alone Together and Angry: An Incel Revolution” PAGE 32

Brian Johnson is a professor of criminal justice at Grand Valley State University in Grand Rapids, Michigan, where he teaches security-related courses. He holds a Ph.D. and master’s degrees in Criminal Justice and Industrial Relations from Michigan State University. Johnson has practical security experience in the hospitality and healthcare industries. Some of his security-related books include Introduction to Private Security, Principles of Security Management, and Safe Overseas Travel. He has conducted research and written articles on economic espionage, loss prevention, school violence, employee surveillance, and contemporary policing issues.

“On-Duty and Vulnerable” PAGE 40

Naoki Kanaboshi is an associate professor of criminal justice at Grand Valley State University in Grand Rapids, Michigan. Kanaboshi received his bachelor’s and master’s degrees in law at Aoyama Gakuin University and Waseda University in Tokyo. He later earned his master’s and S.J.D. degrees at the University of Wisconsin Law School.

He teaches criminal law, criminal procedure, and other law-related topics in criminal justice. His areas of research include the constitutional rights of inmates and their families, as well as civil rights legislation.

“On-Duty and Vulnerable” PAGE 40

A. Benjamin Mannes, CPP, is a subject matter expert in public safety, asset protection, and investigations. He has served federal and municipal law enforcement agencies, led global security and investigative operations for contractors and nongovernmental organizations, and served as director for the Office of Investigations for the American Board of Internal Medicine from 2008 to 2017.

Mannes has a master’s in Organizational Leadership and a bachelor’s in Criminal Justice. He is a Certified Exam Security Professional, and has completed training from the Transportation Safety Institute and FEMA.

“Safety & Security: Partnering for Effective Management” PAGE 50
HIGH SECURITY PERIMETER PROTECTION FOR PERSONAL, BUSINESS, & ENTERPRISE MATERIALS

AMIGUARD - The World’s Strongest Perimeter Security System

CHAMELEON - Upgrade Your Existing Chain Link Fence to a High Security Curtain Wall System for up to 40% Less Than New

ANC - Non Conductive High Security Perimeter Solution

855-552-6426
amirowsecurity@gibraltar1.com • amicosecurity.com
See Our Entire Line of Security Fences on Display in Birmingham, AL - Installation Training Available

For product info #6 securitymgmt.hotims.com
SECURITY MANAGEMENT DIGITAL

TOP TWEET
As 2019 begins, several new laws aimed at curbing sexual harassment go into effect.

TOP POST
ASIS President Christina Duffey, CPP, shares her thoughts on building a security career.

COMMENTS
Thoughts on crucial skills for security managers? See the Security Management article “The Hard Truth About Soft Skills” posted on the ASIS International LinkedIn page.

SM ONLINE

FACIAL RECOGNITION
Facial recognition software is improving at a rapidly increasing rate, reports the National Institute of Standards and Technology.

ELECTIONS
The Center for Strategic and International Studies released a report recommending the United States and others publicize Russian information attacks and increase the awareness of threats to election security.

USE OF FORCE
Florida’s Stand Your Ground law provides police officers immunity from prosecution and justifies their use of deadly force, the U.S. state’s supreme court ruled.

CLOUD SECURITY
ProdataKey released a free white paper to help dealers and end users understand the risks and benefits of cloud-based access control.

MONEY LAUNDERING
UBS Financial Services, Inc., will pay a $14.5 million civil penalty for willful violations of the Bank Secrecy Act.

GLOBAL TERRORISM
The latest Global Terrorism Index finds that although terrorism is more widespread, it is less deadly.

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

NATIONAL SECURITY
Weapon Weaknesses
By Mark Tarallo

STRATEGIC SECURITY
Top Angst: Cyber and Travel
By Michael Gips

PHYSICAL SECURITY
Smarter Access at the State
By Holly Gilbert Stowell

TRENDING ARTICLES
Your security risk is **complex**. Our security capabilities are **complete**.

This is our wheelhouse.

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

Take a **FREE** Security Risk IQ survey. Visit [SecurityRiskIQ.com](http://SecurityRiskIQ.com)

© 2019 G4S. All Rights Reserved.
n 1870, Edwin Rogers designed a push-button fire-alarm repeater. While security professionals might be drawn to the alarm aspect of the device, it was the button that made it revolutionary.

Rogers is credited with inventing the electric push button, which “made it possible for an alarm triggered at the location of one box on the street to strike multiple bells and gongs throughout the system, sending an alert without the aid of a central operator,” writes Rachel Plotnick, assistant professor at Indiana University, in her new book *Power Button: A History of Pleasure, Panic, and the Politics of Pushing*. “This case of pushing buttons in emergency situations demonstrated the potential potency of exerting minimal effort to signal across distance, to command responders to action.”

The idea quickly took root and buttons were adopted in factories, hotels, and elevators. While safety and security were an early target of button power, it quickly became clear that humans are hardwired to enjoy pushing buttons in any circumstance.

In *Irresistible: The Rise of Addictive Technology and the Business of Keeping Us Hooked*, Adam Alter, associate professor at New York University’s Stern School of Business, writes that modern technology has perfected the button to keep our attention and manipulate us into taking action.

“The people who create and refine tech, games, and interactive experiences are very good at what they do. They run thousands of tests with millions of users to learn which tweaks work and which ones don’t—which background colors, fonts, and audio tones maximize engagement and minimize frustration,” Alter writes. “As an experience evolves, it becomes an irresistible, weaponized version of the experience it once was. In 2004, Facebook was fun; in 2016, it’s addictive.”

For example, Alter writes about an experiment launched by Facebook’s Web developers—the “like” button. “It’s hard to exaggerate how much the ‘like’ button changed the psychology of Facebook use. What had begun as a passive way to track your friends’ lives was now deeply interactive…. A post with zero likes wasn’t just privately painful, but also a kind of public condemnation: either you didn’t have enough online friends, or, worse still, your online friends weren’t impressed.” The button was so successful that almost all social media platforms and comment sites now have a way to approve or upvote a post.

The need to impress or be impressed can lead to addictive behavior on Facebook. However, the impulse can be dangerous in the darker corners of the Internet. In this month’s cover story, Steven Crimando, principal of Behavioral Science Applications, discusses Incels. This group of mostly men participate almost exclusively in online groups. Like the earliest buttons, upvotes on these sites illustrate the potency of exerting minimal effort to command action from afar. However, instead of protecting people and property, these buttons allow lonely people to air grievances and, in the case of several high-profile mass shootings, sometimes promote violence.
IT’S YOUR SPACE.
MAKE SURE YOU KNOW WHEN SOMEONE INVADES IT.

SNEAK DETECTION
Our tailgate detection solution allows only one authorized person at a time. Its sleek design reduces cost and complexity versus mantraps and other devices, or it can even enhance those solutions. Your access control, made more secure—that’s the Detex effect.

DETEX.COM/SNEAK1 · 800.729.3839
For product info #8 securitymgmt.hotims.com
BARNYARD

BIOSECURITY

KEEPING THE U.S. FOOD SUPPLY SECURE IS NO EASY TASK, SO THE U.S. GOVERNMENT AND THE UNITED NATIONS ARE CALLING ON PRODUCERS TO TIGHTEN THEIR SAFETY PRACTICES. By Mark Tarallo

SECURING THE U.S. FOOD SUPPLY demands proactivity. In contrast, recalls of contaminated food, such as the nationwide romaine lettuce recall in 2018, are reactive. By the time of the recall, contamination had already occurred and efforts turned to damage control.

So, in the name of proactivity, both the U.S. government and the United Nations are calling on farmers to be a greater part of the frontline of food security.

In the United States, the U.S. Department of Agriculture’s (USDA) Animal and Plant Health Inspection Service (APHIS) launched a Defend the Flock biosafety campaign, aimed at preventing the spread of infectious poultry diseases.

Biosecurity, in general, refers to efforts to keep diseases (and the pathogens that cause them) from infecting animals and humans. The pathogens that can cause diseases include parasites, viruses, fungi, and bacteria.

“We’ve seen great strides in biosecurity since 2015, but biosecurity is an every day, every time effort,” said Jack Shere, USDA’s chief veterinary officer, in a public statement when the campaign was announced several months ago.

The biosecurity campaign was launched for a few reasons. One is that the United States experienced several poultry-related health safety issues in the last decade, such as the devastating epidemic of the highly pathogenic avian influenza virus in 2014–2015.

“This outbreak was the largest highly pathogenic avian influenza (HPAI) outbreak ever recorded in the United States and arguably the most significant animal health event in U.S. history,” USDA said in its final report on the 2014–2015 incident.

Approximately 43 million chickens and 7.4 million turkeys died from the disease during that time frame, according to government statistics.

Last year, a much smaller outbreak of the virulent Newcastle disease in southern California resulted in the euthanasia of more than 50,000 chickens. That outbreak featured the first Newcastle infection of a commercial chicken flock since 2003.

Another reason for the biosecurity campaign is that U.S. poultry is one of the country’s largest industries, and a contamination incident can have serious spillover ramifications.

“Disease outbreaks lead to devastation of our flocks and result in job and financial losses, quarantines limiting trade, and affecting prices on eggs, prepared poultry, and other staples,” the agency said in the campaign’s mission statement.

The campaign offers farmers a range of biosecurity resources they can use, including best practice guides, videos, checklists, fact sheets, and webinars, as well as information on related wildlife management practices and a media toolkit for becoming a “Flock Defender.”

“To sustain good practices takes awareness, training, and reminders,” Shere said.

Judy Fadden, a food safety consultant who heads Fadden Analytical Security and is a member of the ASIS International Food Defense and Agriculture Security Council, says she
believes that the USDA campaign is “a great idea” and that the best practices it promotes are sound and logical. However, she notes that maintaining tight biosecurity practices is no easy task. “There are a number of things that make it complicated,” she says.

She offers the example of farmers who attempt to maintain controlled barns that are contamination-free. Someone like a cleaner or sanitation worker may be going from barn to barn and can inadvertently transfer pathogens to several facilities. Similarly, delivery vehicles can unwittingly transfer pathogens, too.

“It doesn’t take much to contaminate,” explains Fadden, whose parents were chicken farmers.

She also agrees with the USDA that the spillover effects of contamination can be economically devastating. Many of the producers affected in the 2014–2015 outbreak did not have insurance when their flocks were decimated, she says.

Consumer confidence in chicken “was terrible,” which she says hurt the industry, as did the effect on “downstream” products such as cake and other baking mixes, which often contain dried egg. Bird flu can also kill people, although cases of infected humans are uncommon.

The current USDA biosecurity campaign combines and updates two previous campaigns, each of which was targeted at a specific segment of the poultry population.

“While each of the previous campaigns was successful, by combining them and emphasizing shared responsibility, USDA will improve its ability to promote biosecurity and protect avian health across the country,” Shere said.

Like the U.S. government, the United Nations is also calling on farmers to step up their practices in the name of safety and security. According to the Food & Agriculture Organization (FAO) of the United Nations, farmers have a vital role to play in stemming the spread of antimicrobial resistance (AMR) among disease-causing pathogens.

Experts say improper use of antibiotics and other antimicrobial agents partly increased the number of drug-resistant disease-causing microbes in both agriculture and medicine. These microbes, which have developed AMR,
SECURITY MANAGEMENT

BY JOHN J. FAY AND DAVID PATTERSON. Butterworth-Heinemann; Elsevier.com; 558 pages; $99.95.

THE FOURTH EDITION of Contemporary Security Management is an essential resource for anyone who is or will be in the security management field. As an instructor, I have used earlier editions as required textbooks. This new edition follows the same outline as previous ones, but has an expanded table of contents, which makes finding the content easier for both instructor and student.

What makes this edition even better is that it contains examples of security management assessment analyses and tools useful to any security manager, regardless of experience. The addition of Web resources is an improvement over the previous edition, as is the new section on self-assessment of IT security within the “Managing Risk” section. This is now a required element of any security program. The “No Intent and Key Resources” has been replaced with “The Importance of Policies and Procedures,” which is an improvement. Every security manager will face this, whether assessing and upgrading an existing security program or starting from scratch (a scary proposition). This essential addition explains how to write security policies and procedures, one of the most difficult tasks for a security manager. Another excellent feature is the framework tool in the appendices. I highly recommend this new edition of Contemporary Security Management and will be referring to it often. It will also be an invaluable study aid for those preparing to earn their CPP certification.

REVIEWER: Terry V. Culver, CPP, CMAS (Certified Master Anti-Terrorism Specialist), is a security program specialist for Georgia Tech Research Institute. She has more than 25 years of experience in defense and industry security management.

prove resistant to antibiotic-related infection cures.

The ramifications of this development are serious. According to the FAO, one person around the globe dies every minute from a drug-resistant infection.

Without action, the death rate will rise. By 2050, AMR will cost the world economy an estimated $6 trillion annually. AMR also has serious implications for food safety and security, the FAO said.

“Antimicrobial resistance is a concern for all of us,” FAO Assistant Director-General Bukar Tijani said late last year when his agency announced the AMR campaign. “There are over 7 billion consumers in the world, and food safety and quality are paramount.”

Antimicrobials are widely used for farm animals and are sometimes dusted on crops to combat infections. These medicines are also added to feed, even when animals are healthy, to prevent infections. Given this, FAO is calling on farmers to replace the practice with better measures to prevent infections and extend the lifespan of antimicrobials, the amount of which are limited.

These measures include guidance on practicing good farm hygiene, getting veterinary advice before using antimicrobials, and sharing information with neighbors to promote best practices.

“When we use antimicrobials excessively on farms, we’re contributing to the spread of AMR, as resistant pathogens move into the environment through animal waste and farm runoff,” FAO Chief Veterinary Officer Juan Lubroth said in a statement.

Fadden says the campaign to fight the spread of AMR is a “fantastic” development. Although adopting FAO’s recommended practices of stronger infection prevention may cost farmers money in the short term, she says it will help give them “the ability to be more sustainable,” which will likely pay off financially for them in the long run.

In addition, FAO is working to help governments, agricultural authorities, and livestock producers build their capacity to address AMR, with support from the U.S. Agency for International Development and various countries—including Russia, China, France, the Netherlands, Norway, and Sweden.

Lubroth called farmers “one of the important frontline defenders” in the battle to contain the growing threat of AMR.

“If we are to feed a growing population and keep antimicrobials working, we need to invest in our farmers and food production systems,” he said.

GOOD WITH FACES

Facial recognition software is improving at a rapidly increasing rate, says the National Institute of Standards and Technology (NIST).

Specifically, in the four-year time period of 2014 to 2018, facial recognition software became 20 times more accurate in searching a database to find a matching photograph, according to the study, NIST Interagency Report 8238, Ongoing Face Recognition Vendor Test (FRVT).

In its research, NIST evaluated 127 algorithms from 39 different software developers. The new report updates
ORGANIZATIONAL TRUST

People stated that their trust in their employer was stronger than their trust in other organizations, including their government or the media.

<table>
<thead>
<tr>
<th>Trust in organizations:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Their Employer</td>
<td>75%</td>
</tr>
<tr>
<td>NGOs</td>
<td>57%</td>
</tr>
<tr>
<td>Business</td>
<td>56%</td>
</tr>
<tr>
<td>Government</td>
<td>48%</td>
</tr>
<tr>
<td>Media</td>
<td>47%</td>
</tr>
</tbody>
</table>


NIST’s previous evaluations of facial recognition software published in 2010 and 2014 reports. The test performed in all three of the 2010, 2014, and 2018 evaluations judged how well the algorithm could match a person’s photo with a different photo of the same person stored in a large database. This is sometimes called a one-to-many search.

“The major result of the evaluation is that massive gains in accuracy have been achieved in the last five years (2013–2018) and these far exceed improvements made in the prior period (2010–2013),” the report finds.

The report says that the failure rate in one-to-many searches dropped from 5 percent in 2010 to 4 percent in 2014 to 0.2 percent in 2018. When an image of a person’s face is submitted to the recognition software, the search is considered a failed one if the software does not retrieve the matching face from the database.

The top-performing algorithms from the latest round of testing make use of a type of machine-learning architecture called convolutional neural networks. Such machine-learning tools have been rapidly advancing in the last few years, and this has had a major impact on the facial recognition industry.

“The test shows a wholesale uptake by the industry of convolutional neural networks, which didn’t exist five years ago,” the NIST report finds. “[Now], about 25 developers have algorithms that outperform the most accurate one we reported in 2014.”

However, the algorithms do not all perform the same; the best are far more effective than the rest of the pack. “There remains a very wide spread of capability across the industry,” the report says.

To read a copy of the NIST report, go to SM Online.
While ISIS’s clout has diminished in Europe, Iraq, and Syria—the number of deaths caused by the organization fell by 52 percent overall, dropping 75 percent in Europe alone—it remained the deadliest terrorist group in 2017. Its spread to North Africa, sub-Saharan Africa, and Southeast Asia is ongoing.

While Europe saw the biggest reduction in deaths from attacks in 2017, the number of terrorist incidents increased. According to the report, this highlights ISIS’s reduced capacity to plan and coordinate larger scale attacks.

Meanwhile, North America saw the largest increase in the impact of terrorism from 2016 to 2017, with the majority of terrorist activity taking place in the United States. This is the fourth successive year that terrorist-related deaths have risen in the region, from 65 in 2016 to 85 in 2017.

This is also the first year the report has distinguished far-right wing terrorism as a growing trend—white power extremists were responsible for nine attacks and seven deaths in North America in 2017, the report notes. This trend is expected to continue, based on the October 2018 attack on a Pittsburgh synagogue that left 11 people dead.

“The threat of far-right political terrorism is on the rise,” according to the report. “There were 66 deaths from terrorism caused by far-right groups and individuals from 113 attacks for the years from 2013 to 2017. Of those, 17 deaths and 47 attacks occurred in 2017 alone. In Western Europe, there were 12 attacks in the U.K., six in Sweden, and two each in Greece and France. In the U.S., there were 30 attacks in 2017 which resulted in 16 deaths. The majority of attacks were carried out by lone actors with far-right, white nationalist, or anti-Muslim beliefs.” Far-right groups and individuals accounted for nearly 60 percent of extremist-related American deaths in 2017, the report later notes.

It’s important to put reports like the Global Terrorism Index in context, emphasizes Michael Center, vice chair for subject matter experts and growth with the ASIS International Global Terrorism, Political Instability, and International Crime Council. When it comes to defining and quantifying terrorism trends, digging into the data to understand who committed attacks and what their motivations were can be enlightening.

“The report wrapped all forms of terrorism into one statistic—it makes the problem look bigger than it
“Especially in the United States, if you use the word ‘terrorism,’ you’re really talking about Islamic terrorism. When the report talks about the number of incidents in the United States, that includes groups like anti-Semetics, left-wing radicals, and white supremacists, all of whom outnumber Islamists these days. While the report defines the different groups, it doesn’t break down what those numbers are.”

One trend the report focuses on is the high rate of terrorism in countries classified as being “in conflict”—they had at least one conflict which led to 25 or more battle-related deaths. There is a correlation between battle-related deaths and deaths from terrorism, the report found—in 2017, almost 95 percent of total deaths from terrorism occurred in countries involved in violent conflict. Additionally, just 10 countries accounted for 84 percent of all deaths from terrorism in 2017, and all 10 of those countries were classified as being in conflict. “Countries involved in conflict are more susceptible to terrorism in part because of the lack of a fully functioning state,” the report notes. “Terrorism is also one of many tactics employed by insurgencies and paramilitaries in a civil conflict.”

Center notes that it can be hard to distinguish terrorism from insurgency in such situations, especially depending on how terrorist acts are defined. “In a country that’s going through conflict, if you have a conflict death as the result of violence due to wanting to create and instill fear for political gain, that’s a real gray area,” Center says. “Is it terrorism or insurgency? If I want to be a purist, and I’m looking at Syria, Iraq, or Afghanistan, these are open conflict countries and the parties involved are all fighting with each other. Is that really terrorism?”

Much of the report focuses on emerging trends gleaned from the START database, including the ongoing spread of terrorism activity. Despite the decline in terror-related deaths, 2017 saw the second-highest number of countries affected by lethal terror attacks. This is evident by the ongoing decentralization of terror groups, as well as the spread of terror activity into areas such as Africa’s Maghreb and Sahel regions, Southeast Asia, and Nigeria’s Middle Belt.

The report also mentions ongoing speculation about the threat of the estimated 40,000 radicalized foreign fighters who traveled to Iraq and Syria to aid ISIS.
THEORIES OF TERRORISM

BY DANIELA PISOIU AND SANDRA HAIN. Routledge; Routledge.com; 200 pages; $44.95.

DANIELA PISOIU and Sandra Hain from the Austrian Institute for International Affairs have written a book that provides readers with a theoretical framework, based on a spectrum of academic fields, for launching an informed discourse on terrorism studies. *Theories of Terrorism: An Introduction* views the subject through the lens of social science theories while anchoring the discussion to two paradigmatic approaches: traditional versus critical terrorism studies (CTS).

The widely debated question “What causes terrorism?” is tackled through a review of supporting literature based on deterministic, intentional, and relational approaches to the question. These approaches are used throughout the book as analytical paths to understanding past and present discourse on terrorism. The final chapter on counterterrorism explores how and why terrorism campaigns end.

The book does well to provide essential tools for exploring the current discourse on terrorism and offers further recommended reading lists. It is laden with supporting citations from the literature and historical examples drawn from the French Revolution of 1789 through the Algerian War of 1954–1962 and on to post-9/11 scenarios. The supporting academic evidence reminds the reader of the depth and richness of the discourse. Furthermore, it allows readers to venture into additional research. Various methodologies and approaches to the subject are explored, and the authors refrain from presenting unsupported opinions. Instead they present a plethora of published opinions to support the reader’s own thinking process.

This book is aimed at students of terrorism, political, and counterterrorism studies, but it will also interest security practitioners and policy makers who are charged with preparing counterterrorism strategies. It is an essential read for anyone who is serious about understanding the threat and mitigating the risk of terrorism.

REVIEWER: Andre Mohammed, CPP, is a member of the ASIS Global Terrorism, Political Instability, and International Crime Council. He is currently based in Pakistan as a security operations officer with the World Health Organization.

He does note that many Russian-speaking foreign fighters have been able to return home more easily—and covertly—than fighters from other European countries. “People should be looking at former Soviet satellite countries for future moves—terrorists will start emerging from that area more,” Center predicts.

The report also focuses on the nexus between crime and terrorism, especially when it comes to recruiting and radicalization in Western Europe. While conflict remains the primary driver of terrorism in most areas, countries with high levels of economic development are impacted by terrorism for different reasons: social alienation, lack of economic opportunity, and involvement in an external conflict. These hallmarks can lead to an affinity between disgruntled outsiders and jihadist groups and ideologies. Additionally, the report repeatedly cites studies finding that, in Western Europe, more than 40 percent of foreign fighters and those arrested for terrorist activity have some form of criminal background.

“It is difficult to know whether individuals with a criminal background are being deliberately targeted by terrorist recruiters,” the report states. “However, there is little doubt that there is considerable synergy between the needs of disaffected young criminals, and the needs of terrorist organizations.”

Center says the latent radicalized population in Europe is something that existed before ISIS and will continue to exist—the question is whether individuals will feel empowered to act.

“In Europe, you have a population of radicalized Muslims—just like you have people in the Ozarks in middle America who have a firm foundational version of their Christian beliefs—technically they are radicals within that population, but not all radicals are prepared to kill people,” Center explains. “Even though ISIS came and went, the radicalized population in Europe has not changed—they still exist, but nobody is talking about their motivation. Let’s say you have 10 radicalized people, and out of that 10, only one would be prepared to kill people. But given the fall of the ISIS caliphate, is that one person still prepared to fight? To kill?”

Similarly, Center points out that some factions of al Qaeda and other terror organizations joined ISIS during its rise, but it is yet to be seen whether those groups will stick with ISIS through its decline, regroup under the original franchise, or fall apart. The fate of these types of shifting identities will have a large impact on the global terror outlook in 2019.

“Political instability will certainly continue to grow, and violence will follow,” Center says.
WHY IS ABLOY®
SUPER WEATHER
PROOF THE
WORLD’S BEST
PADLOCK?


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

ABLOY SUPER WEATHER PROOF (SWP) padlocks were born - a locking solution in which the components are extremely well protected to ensure operation in all conditions. Security is guaranteed even with regular exposure to extreme heat or cold, storm-driven salt water or fine desert dust.

ABLOY secures people, property, and business operations on land, at sea, and in the air – in all circumstances.

ASSA ABLOY is the global leader in door opening solutions, dedicated to satisfying end-user needs for security, safety and convenience.

For product info #12 securitymgmt.hotims.com
Epiphany’s Cardio Server supports more than 950 hospitals around the world by aggregating and managing electrocardiograms and other cardiopulmonary test results in a browser-based application that can be accessed by healthcare teams anywhere. It allows doctors to use diagnostic tools to interpret and sign off on the tests, which are then sent off to a patient’s electronic medical record.

“Time is tissue in the world of cardiac care; it’s important that we get the study information to the doctor as quickly as possible where they can read and provide the diagnosis and treatment for that patient,” says Joe Noto, vice president of strategic alliances, partnerships, and marketing at Epiphany Healthcare.

There are dozens of testing device manufacturers in the cardiopulmonary field, and each has its own way of exporting test data. Because of this, Epiphany must be able to gather all types of personal health information (PHI) in a secure and efficient way. To migrate the data, vendors would have to zip and password protect the file to send it via email, and, if the file were too large, Epiphany would send the vendor a secure hard drive to complete the exchange—a process that involved its own set of security challenges.

“That whole process was really consuming time and money,” says Chad McQuarrie, system administrator at Epiphany. “With [regulatory] restrictions, we had to be aware of exactly where the drive was, who sent it out, and who had access to it. It was a very long procedure.”

And if vendors needed support with the transfer of the data, McQuarrie and other back-end employees had to take extra precautions to make sure they never opened files with PHI while troubleshooting. The support team also had to direct customers to take extensive measures to keep sensitive data secure.

“For our support team to go through that, [the customer would] have to email us a visual of what’s going on,” McQuarrie notes. “We’d explain that they still need to zip that part up and password protect it before they could send it to us.”

To simplify the secure transmission of PHI to Epiphany, McQuarrie began the search for an updated solution that would make the transfer of sensitive data easier and more secure for both Epiphany and its customers. McQuarrie says he considered about 20 options, looking for a solution that worked with the organization’s system and would replace its FTP server.

He found the answer in Egress Software, which met all of Epiphany’s requirements, especially when it came to the back end—most similar solutions required the use of a Microsoft Exchange server, but Epiphany uses Gmail.

“One of the key factors we needed was something that didn’t change our daily procedures, that could be
incorporated into our email, so that I didn’t have to retrain the whole company on how to handle PHI,” McQuarrie explains. “Egress was the only one I found that incorporated into the email system that we already have.”

With guidance from Egress’s experts, McQuarrie was able to seamlessly integrate encryption capabilities into the organization’s Gmail interface to protect the transfer of PHI over email.

“I didn’t have to stop the flow of anything to kick this off,” McQuarrie notes. “I could do all of this in the background and test it out, make sure it works, and then let everybody know how to do it through training. It’s pretty self-explanatory—a few settings in Google, a few tests here and there, and that’s it.”

Another benefit of the Egress system is one McQuarrie hopes will make the use of the external hard drives obsolete—a secure Web form where vendors can upload large files straight to Epiphany, where it’s now stored in the cloud.

“Customers could go to a Web page, literally upload their data, which is encrypted, and we get the email to pull it down and decrypt it,” McQuarrie explains. “In the past, if your email can’t handle the files, we’re going to have to send you a drive. Now, if you don’t want to wait for the drive, we can send you to this website and you can upload there. It’s something new we can offer.”

Epiphany also allows customers to upload data via a computer application. McQuarrie notes that they will still use the external hard drives, but only if a customer’s own firewall won’t allow them to send the data via one of the three methods. And now that the files are cloud-based, Epiphany does not need to store the data.

“Because the data is in a cloud atmosphere, if something were to happen to our data center, you don’t have to redo all your data that you sent to us,” McQuarrie says. “Before, we were holding the data and after six months deleting it. We don’t have to do that now.”

Egress gave McQuarrie the tools to make the transfer of PHI all but foolproof. He notes that the Web page allows vendors to choose the recipient of the data from a dropdown menu to avoid any mistakes.

And if a problem arises during the transfer, Epiphany’s back-end employees now have an easier way to identify the issue—Egress creates a detailed report of every transfer, so McQuarrie can see when the data was sent, who had access to it, and more. This bird’s eye view of the problematic transfer gives employees enough information to identify the problem without having to work around sensitive documents.

“I have an overview of everything, but I can’t see the data, even with an overview to the whole system,” McQuarrie explains. “If someone can’t get to their data, I can redirect it. If they want to cancel it, I can go in, cancel, and make a report about where it went and who accessed it. Having that capability was immensely positive for any of the audits that we go through.”

Because Epiphany manages PHI, it is audited by many organizations. McQuarrie says one of the biggest benefits of using Egress for the Cardio Server is the seamless auditing process thanks to the in-depth reports.

“It’s on us to prove that sensitive data was not touched or seen,” he explains. “There are reports on when it was accessed, the IP address, the exact time and day of when they opened it. Having that in a report to drop was huge—I can tell you nobody has touched it, and the customers could know exactly how things were done.”

FOR MORE INFORMATION:
MARK BOWER, MARK.BOWER@EGRESS.COM, 1.800.732.0746.
However, some are still skeptical about the security of the midterm elections, which saw a record number of Democrats elected to the House of Representatives while the Republican Party strengthened its majority in the Senate.

“About four-in-ten (38 percent) Americans say that Russia or other foreign governments definitely (9 percent) or probably (30 percent) influenced the congressional elections, while six-in-ten say foreign governments probably (44 percent) or definitely (16 percent) did not influence the elections,” according to Pew.

The rise in confidence may have come from the flurry of activity leading up to the midterms to prevent cyber attacks against election systems. Microsoft issued warnings about nefarious activity targeting conservative voters, Facebook and Twitter announced major takedowns of accounts linked to suspicious activity, and the U.S. Department of Homeland Security (DHS) worked with state and local election officials to enhance election security.

Just prior to election day in November, DHS Secretary Kirstjen Nielsen, then-Attorney General Jeff Sessions, Director of National Intelligence Dan Coats, and FBI Director Christopher Wray issued a joint statement on election day preparations.

“Our agencies have been working in unprecedented ways to combat influence efforts and to support state and local officials in securing our elections, including efforts to harden election infrastructure against interference,” they said. “Our goal is clear: ensure every vote is counted and counted correctly. At this time, we have no indication of compromise of our nation’s election infrastructure that would prevent voting, change vote counts, or disrupt the ability to tally votes.”

The officials cautioned, however, that all Americans should remain vigilant because threats to the system continue to exist.

“Americans should be aware that foreign actors—and Russia in particular—continue to try to influence public sentiment and voter perceptions through actions intended to sow discord,” the officials said. “They can do this by spreading false information about political processes and candidates, lying about their own interference activities, disseminating propaganda on social media, and other tactics.”

Following the midterms, Director of National Intelligence Coats provided the White House with a report about
In 2016, we were not prepared for the coordinated information operations we now regularly face.

The security of the election, which was required under a previous executive order issued by U.S. President Donald Trump.

The details of the report were classified, and are likely to remain so, but Coats said in a statement that the U.S. intelligence community did not see any indicators that compromised election security, such as preventing voting, changing vote counts, or disrupting the ability to tally votes.

“The activity we did see was consistent with what we shared in the weeks leading up to the election,” Coats said. “Russia and other foreign countries, including China and Iran, conducted influence activities and messaging campaigns targeted at the United States to promote their strategic interests.”

The intelligence community, however, did not assess what impact these campaigns may have had on the outcome of the midterms.

“The U.S. intelligence community is charged with monitoring and assessing the intentions, capabilities, and actions of foreign actors; it does not analyze U.S. political processes or U.S. public opinion,” Coats explained.

While there were some misinformation campaign efforts, Facebook attempted to thwart them by making explicit changes to its policies to ban posts that misrepresented voting information.

Facebook made the change in October 2018 after widespread criticism of how it handled misinformation campaigns on the platform in the runup to the 2016 presidential election.

“In 2016, we were not prepared for the coordinated information operations we now regularly face,” wrote Facebook founder and CEO Mark Zuckerberg in a post on the platform. “But we have learned a lot since then and have developed sophisticated systems that combine technology and people to prevent election interference in our services.”

Some of the changes Facebook made included banning posts that misrepresented how to vote in an election—such as giving the incorrect election day—and creating a reporting option specifically for voting information that Facebook users thought was suspicious or a violation of Facebook’s policies.

It also made changes to make its political ads sales more transparent to prevent nation-state actors from purchasing political ads targeting a candidate, similar to what happened in 2016.

Facebook has since adopted these practices for elections in Brazil, the United Kingdom, and India.

“Now anyone who wants to run an ad in India related to politics will need to first confirm their identity and location, and give more details about who placed the ad,” wrote Sarah Clark Schiff, product manager at Facebook, in the announcement. “The identity and location confirmation will take a few weeks, so advertisers can start that process today by using their mobile phones or computer to submit proof of identity and location.”

Continuing these efforts will be key as campaigning for the 2020 presidential election gets underway. This is because most election experts, including Christopher Krebs, a DHS official who later became the first director of the department’s Cybersecurity and Infrastructure Security Agency (CISA), think it will be a major target.

At CyberTalks in Washington, D.C., in November, Krebs, in his capacity as then-undersecretary for the National Protection and Programs Directorate, said DHS was working through what an adversary could do to attack election infrastructure because “the big game is 2020...2018 is just the warm-up.”

HACKING FOR DUMMIES

BY KEVIN BEAVER. Wiley; wiley.com; 416 pages; $29.99.

ALTHOUGH more than 50 years have passed since the 1968 edition of Cassell’s New Latin English Dictionary was published, its translations of Latin words into English remain useful. In the dynamic world of computer security, things change almost daily, and a reference that’s two years old can be outdated.

Now in the sixth edition since its initial publication in 2004, Kevin Beaver’s Hacking for Dummies carries on the book’s tradition of giving readers in the trenches a guide they can use to ensure that their organization’s systems and networks are secure. Like previous editions, it is a practical guide that can teach the reader real-world hacking and penetration testing skills.

This edition has the same basic motif as the original book, but is updated to include Windows 10, Linux, macOS, and more; and it includes an updated list of currently available hacking tools.

The final section of the book, “The

REVIEWER: Ben Rothke, CISSP (Certified Information Systems Security Professional), PCI QSA (Qualified Security Assessor), is a senior security consultant with the Netitude Group.
DHS worked with state and local election officials to enhance their election systems before 2018 and into the future using $380 million from the U.S. Election Assistance Commission (EAC). Recipients could use the funds to replace voting equipment, implement a post-election auditing system, upgrade their computer systems, put election officials through cybersecurity training, and other security-related measures (see “Election Hardening,” Security Management, September 2018).

And a DHS official who spoke to Security Management during preparation for the midterms said the department was using a “risk management approach that we’re going to build upon in 2020 and beyond.”

The official said DHS was working with its partners to mature the Election Information Sharing and Analysis Center and would conduct exercises with federal partners and state and local governments to prepare for the 2020 election. Security Management reached out to DHS for an updated comment but was unable to speak to an official due to the partial U.S. government shutdown that was in effect as of press time.

Despite the work that the department did to prepare for the midterms and the millions of dollars made available, John Dickson—principal at cyber firm Denim Group—says he was “underwhelmed” with the resources that were allocated to address election security.

“Namely, states and local authorities did a poor job of putting the resources in play as quickly as they could have, and they spread federal monies too thinly across a variety of needs,” he explains. “Sadly, much of that money was directed to buy new voting machines, which were not the biggest risk in my opinion.”

Instead, Dickson says more resources should have been put towards addressing risks to the static election system components—registration and reporting systems.

Election officials should address threats to these components ahead of the 2020 election, Dickson adds, and adopt the same mindset that Krebs said DHS was using towards election security.

“I recommend they view their election infrastructure as the Russians might, identifying the most attractive targets to address first,” Dickson says. “We also strongly recommend election officials conduct tabletop exercises, conduct threat modeling, and engage third parties to conduct penetration tests to mimic sophisticated nation state threats like the Russians, Chinese, or North Koreans.”

And while cyberattacks to voting machines and reporting systems are a

### HANDLING CYBERATTACKS

Respondents from Argentina and Brazil said their countries are not well prepared to manage a major cyberattack, while most individuals from Israel and Russia responded that they are well prepared. Respondents from the United States were more evenly divided, with those who believe the country is well prepared outnumbering the others by only 10 percentage points.

<table>
<thead>
<tr>
<th>Responded “Not Well”</th>
<th>Responded “Well”</th>
</tr>
</thead>
<tbody>
<tr>
<td>Argentina 81%</td>
<td>Brazil 78%</td>
</tr>
<tr>
<td>United States 43%</td>
<td>Russia 19%</td>
</tr>
<tr>
<td>Israel 20%</td>
<td>67%</td>
</tr>
</tbody>
</table>

Source: International Publics Brace for Cyberattacks on Elections, Infrastructure, National Security; Pew Research Center, January 2019
threat, officials should not underestimate how misinformation campaigns could be used to influence voters, according to Suzanne Spaulding, former undersecretary for the National Protection and Programs Directorate at DHS.

Speaking at the American Bar Association’s Standing Committee on Law and National Security’s annual review, Spaulding explained that Russian propaganda efforts to divide Americans should be a major focus ahead of the 2020 elections.

“We’ve seen that Iran is trying to wade in; we know that China is engaged in its own sophisticated operation with its own playbook,” said Spaulding, who is now a senior adviser at the Center for Strategic and International Studies (CSIS). “But I’m focused on Russia because so far it’s only Russia we see engaging in this scorched-earth approach to weaken democracy—to weaken this country.”

Russia used misinformation on social media to attempt to influence Americans who lean Democratic or Republican, which experts fear could lead to violence.

Russia used misinformation on social media to attempt to influence Americans.

“We cannot dismiss the seriousness of an adversary constantly pouring gasoline on the flames of division, hatred, and fear that can lead to violence,” Spaulding said.

To curb the effect misinformation campaigns can have, Spaulding and a group of experts authored a report published by CSIS that recommended publicizing Russian misinformation attacks and increasing awareness of the threat to institutions.

The report also called for improved transparency into foreign adversary interference through campaign finance reform, foreign agent disclosure, and through promoting greater media literacy and understanding of government.

However, Spaulding said the recommendations—and government agency efforts—will not be as effective as they could be without support from the Trump administration.

“We need a whole-of-nation approach to counter Russia’s actions to try to weaken this country, and that’s very hard to do if you don’t have leadership from the White House,” she explained.

To read the CSIS report, visit SM Online.

For product info #15 securitymgmt.hotims.com
Recently designated a hate group by the Southern Poverty Law Center, Incels exist primarily as an online subculture espousing male supremacy and committing acts of violence against people who seem to have an easy time finding love and acceptance.

In 2004, Elliot Rodger killed seven people and injured 14 others in Isla Vista, California, striking back at those who would not permit him into their social circles. In a series of videos and a 141-page manifesto, Rodger blamed popular young women for his loneliness and the fact that he was still a virgin. In his writing, Rodger described himself as “the supreme gentleman” and fantasized about his retribution for the perceived wrongs that he suffered at the hands of popular and beautiful people. Today Elliot Rodger is not simply the name of a notorious mass murderer; in the language of Incels, it is also a verb, as in “the guy went Elliot Rodger” or “E.R.”

Incels, shorthand for involuntary celibates, exist primarily as an online subculture espousing male supremacy. Incel is not simply a form of self-identification, but rather an ideology and self-described movement of disaffected, disconnected, and angry individuals—primarily men—who have found justification for violence against people who seem to have an easy time finding love and acceptance. This extreme ideology was recently added to the list of designated hate groups by the Southern Poverty Law Center.

Rodger predicted an Incel revolution. In April 2018, 25-year old Alek Minassian heeded Rodger’s call to action and plowed a rented van into pedestrians along the streets of Toronto’s North York Centre, killing 10 and injuring another 16. Shortly before launching his attack, Minassian posted a message to Facebook that included the phrase “The Incel Rebellion has already begun!... All hail the Supreme Gentleman Elliot Rodger!” In November 2018, Scott Paul Beierle, 40, walked into Hot Yoga
Tallahassee and opened fire, killing two people and wounding five others before turning the gun on himself. In YouTube videos posted in 2014, Beierle articulated misogynistic views, made resentful statements about women who would not date him, and identified with Incels.

Is it Terrorism?
There is a fine and often blurry line between hate crimes and terrorism. Increasingly, Incels are viewed as involved in a form of gender-based terrorism; ideologically motivated, with a clear social agenda. Incels are not simply men’s rights activists—they are much more dangerous. Incels place the blame on women for their misery, and in doing so provide the motivation and justification for acts of extreme violence. Much like other recognized extremist groups, there is a well-worn path leading from radicalization to mobilization. In many ways the path to becoming an Incel is no different from the path to other extremist groups like ISIS. The Internet has allowed isolated people to connect, which in turn can increase the potential for radicalization. Those in the Incel community are alone, but now they are alone together, and sharing a hateful message attractive to many, who like Rodger, harbor fantasies of revenge. To turn a phrase, the Internet allows them to form a pack of angry, lonely wolves.

The Incel Dictionary
There are 125 different terms comprising the Incel dictionary. Across this narrow spectrum of attitudes within a sexist and entitled subculture, the most unifying elements are “red pills” and “black pills.” Adapted from elements of the 1999 science fiction movie, The Matrix, Incels refer to a red pill as a person who is said to have awakened to the fact that society discriminates against men, not women. The black pill represents the idea that if someone is considered physically unattractive, they are unworthy of love; therefore, any attempts to form lasting relationships are not only destined to end in failure but are probably going to result in even greater unhappiness. Other significant Incel terminology includes:

**Alphas:** High-status males who get all the sex they desire because they have controlling and socially-dominant personality styles that all females are irresistibly attracted to.

**Betas:** Betas are males who are somewhat inept in relationships with females and thus don’t get enough sex.

**Beta uprising:** The uprising predicted to happen when betas and omegas become filled with rage and collectively commit acts of violence.

**Blackops2cel:** A man whose photo Incels have taken as an icon of their community; someone emblematic of what an Incel looks like.

**Chad:** The archetypal alpha and perennial object of the Incel’s envy and resentment.

**ER - Elliot Rodger:** The 22-year old man who shot and killed multiple people in Isla Vista, California, in 2014, and author of a manifesto that blamed the women who had rejected him for causing him to commit murder. Known as Saint Elliot, he is revered as a martyr on Incel forums.

**Hypergamy:** A term borrowed from biology used to describe the phenomenon of females mating with males of higher status.

**Incels:** Involuntarily celibate, a term originally coined by a Canadian feminist, now used almost exclusively by men to describe people who want to have sex, but cannot, due to reasons beyond their control.

**LDAR:** A directive to “lie down and rot,” or just give up hope of being involved in a sexual relationship.

**MGTOW:** “Men going their own way,” an alternative to being celibate against one’s will. Analogous to the sovereign citizen movement, they reject the idea of seeking a romantic partner as a sovereign citizen might reject the federal government.

**NEET:** A person who is “not in education, employment, or training” or having zero status in society.

**Normie:** Anyone who is normal: average-looking and of average intelligence.

**Omega:** A male who has no prospects for sexual relationships, and who is on the lowest rung of the Incel’s imaginary sexual hierarchy.

**STACY:** A woman who allegedly has her pick of sexual partners; an unattainable female ideal that is targeted for revulsion and perhaps even violence.

**WIZARD:** Someone who is a virgin at the age of 30 or older.
“Loners” have long been associated with risk of violence. Whether in discussions about violence prevention or news reports of violent incidents, there is the perception that being alone raises the risk of violence. Although social isolation is a known risk factor, why someone is a loner is more important to understand than simply if they are a loner. There are many people who, by their nature, are more comfortable on their own than in groups or in relationships. There are others who try to break in to social groups, form relationships, and crave the acceptance of others. However, due to their temperament, lack of social skills, or mental health issues, they are pushed away, and leave with feelings of anger and rejection. These individuals are not loners, but more accurately, incompetent joiners. The incompetent joiner is not necessarily prone to violence. Some, still seeking acceptance, find it in chat rooms and on social media platforms inhabited by others with a shared life experience.

Radicalization is characterized by a shift in opinions, attitudes, and beliefs, while mobilization is a shift in action. Within the Incel community and other extreme ideologies, many may become radicalized, but far fewer will mobilize. Those who mobilize are the ones seen in the news, but for every Incel that mobilizes, thousands are leading a lonely existence, connecting with the world primarily through their keyboards and computer screens. In online Incel communities, where the volume is loud and the language is vulgar, the incompetent joiners can easily become self-radicalized, and further radicalize each other. At this dangerous intersection, a personal grievance collides with an extreme ideology. Acceptance of this ideology can be a slippery slope because there is a powerful message that anyone who truly believes in the cause does not sit idly on their hands; they act. True believers are not talkers; they are doers. For some in the Incel community, Rodger’s writings and videos provide justification for violence and a call to action.

Workplace Violence
The current emphasis on efforts to address gender equality and eliminate sexual harassment in the workplace...
Cover Story | By Steven Crimando

runs counter to the Incel belief that women are inherently inferior to men. The message of the #MeToo movement has further stoked feelings of aggrieved entitlement by some, who feel they are being denied the right to the affection and sex they deserve and blame women, rather than themselves, for their personal and professional failures.

While no workplace is immune from violence, there are some environments where there is greater exposure to the various types of violence, and some in which Incel-related violence may be more likely.

The shooter at Hot Yoga Tallahassee chose a populated and confined space with predominately female targets to open fire. George Sodoni did the same when he attacked a women’s aerobics class at the LA Fitness Center in a suburb of Pittsburgh in August 2009. Three women and the shooter were killed, and another nine injured. The gunman, who maintained a website that included his blog describing his inability to cultivate relationships and friendships, left a note in his gym bag expressing his hatred for women.

Regardless of whether the perpetrator of workplace violence is a disgruntled or disturbed employee, an angry customer or client, or someone motivated by an extremist ideology, employers must be aware of the risks and recognize the warning signs of someone on the pathway to violence. (See sidebar, “Stopping Incel Violence.”)

The Language of Incels

The Incel community occupies a dark corner of the Internet. In November 2017 Reddit banned the main online community of Incels for violation of its policy prohibiting content that calls for violence or physical harm. After exploring other alternative platforms, the Incel community eventually migrated back to Reddit while also launching Incel websites. The content of the discussions

Stopping Incel Violence

Like others who may be on a pathway to violence at work, on campus, or in the community, Incels share some common attitudes, beliefs, and behaviors that can serve as warning signs or preincident indicators.

Indicators that are shared with others, but not exclusive to Incels include:

- The “grievance collector;” chronic victimhood
- Externalized blame for their unhappiness or distress
- Relationship problems
- Depression or withdrawal
- Paranoia, or concerns that others are trying to cause harm or limit their success
- Hopelessness
- Rage, anger, seeking revenge
- Feeling trapped
- No reason for living; no purpose in life
- Self-identification as a warrior, pseudo commando, or agent to advance a particular cause or belief system
- Militarized style of dress or speech
- Expression that violence is necessary or justified
- Indicating an intent to mobilize or take action

Indicators unique to Incels include:

- Self-identification as an Incel
- Adoption of Incel terminology and worldview
- Empathy with others who have committed violent misogyny
- Participation in chat rooms and online communities espousing violence toward women or successful men
- Extreme social awkwardness, social anxiety, or body dysmorphia
- Perception of unattractiveness or undesirability
- Overt anger or resentment toward women
- Indications of preoperational hostile surveillance of places frequented or populated primarily by women

These are the signals of someone who needs help. Employee Assistance Programs, campus counseling centers, and emotional support helplines all can be sources of support for someone trying to cope with isolation and rejection. Although help is available, the gravitational pull of an extreme ideology can make it difficult for some people to break free and explore alternative ways of thinking or interacting with the world around them.
In the world of the Incel, there is a **strong bias** against seeking mental health treatment. On these platforms remains misogynistic and violent.

Incels have developed a unique and complex lexicon. (See box, page 34.) Knowledge of this terminology can be helpful in identifying those who subscribe to this belief system or are radicalizing to a more extreme Incel view. It may also be useful in determining the level of concern about potential violence because some of the terminology has militaristic undertones.

**Incels and Mental Illness**

While involuntary celibacy is not a psychiatric diagnosis, and not all Incels are mentally ill, some people who self-identify as Incels do have mental disorders and some have physical disabilities. These physical and emotional conditions may lead to isolation and loneliness that can be an obstacle to meeting people and forming satisfying and healthy relationships. Across the entire spectrum of Incels, with or without diagnosable mental disorders, the most common emotion experienced is profound and painful loneliness.

It is important to recognize that research consistently supports the fact that people with mental illnesses are no more likely to be violent than other members of society. There are certain conditions, and symptoms of those conditions, that can increase the likelihood of violence. In the world of the Incel, an overwhelmingly male environment, there is a strong bias against seeking mental health treatment. Members of Incel forums who discuss depression often meet with encouragement for suicide or acts of mass violence followed by suicide.

**Incels in the Threat Landscape**

While misogyny and isolation are not new phenomena, the radicalized subculture of Incels has provided an added dose of justification for violence against women and romantically successful men. There are often themes of racism interlaced in the Incel worldview. While the first instances of Incel-inspired violence date back nearly three decades, today’s Incel community has become more extremist and violent through cross-population with other online hate groups and alt-right white supremacist male groups.

There is agreement throughout the intelligence community that the greatest threat to the homeland at present is not necessarily foreign terrorist organizations, but rather homegrown violent extremists and lone actors of various ideologies, with domestic hate groups at the forefront. It will be increasingly necessary to understand the mindset, motives, language, and indicators of the Incel culture. The pathway to violence runs in both directions. Left unchecked, angry isolated Incels will remain in the margins of mainstream society, smoldering with resentment against those who have denied them the affection and satisfaction they feel they deserve. Early identification and intervention can turn a disaffected acceptance-seeker around, away from the siren song of radicalization, and toward effective ways of coping, communicating, and negotiating a place in society.

---

**STEVEN CRIMANDO** is the Principal of Behavioral Science Applications, a training and consulting firm focused on human factors in crisis prevention and response. He is a Board-Certified Expert in Traumatic Stress (BCETS) and a consultant for corporations, government agencies, police, and military programs.
EXTRACT SIGNALS
From the Noise
ADVANCED ANALYTICS EMPOWER SECURITY AND RISK MANAGEMENT TEAMS TO EXTRACT INSIGHTS AT SCALE

In August 2016, a largely unpublicized storm struck Louisiana. Over a 10-day period, roughly 7.1 trillion gallons of rainfall resulted in widespread flooding across the state. The organization, which maintains a large portfolio of private and commercial loans in the area—needed a way to quickly assess the impact of the storm and brief key executives on the results. Faced with a rapidly escalating situation, a senior manager was tasked with creating a response team to conduct this holistic damage assessment.

The senior manager and his team quickly discovered that their greatest challenge was finding a common framework to effectively analyze vast amounts of data in a short amount of time. “We were worried about the disaster’s impact on our physical footprint [branch locations] as well as the amount of our portfolio that could be lost from this kind of weather event,” he stated. “We didn’t want to wait three weeks to do an exercise after the fact. We needed a way to do this in real time.”

“What we needed was a way to transcend emotions and get to the bottom of what was really happening in our portfolio,” argued the senior manager. Leveraging Esri® technology for location intelligence, the senior manager applied a single pane of glass to analyze the organization’s disparate threat feeds in a common view. Additionally, the response team configured mobile applications that empowered employees to submit real-time updates from the field, providing context at a hyperlocal level. This approach helped the team to better understand which areas of their portfolio were most affected.

Utilizing location intelligence, the senior manager provided his executives with an in-depth report that accurately assessed the impact to their portfolio. Additionally, he shared other strategic applications for Esri technology to provide compassionate care to their customers. “We were not only able to quickly ascertain what this event meant to the bank,” said the senior manager, “but also [we could] provide real-time situational updates to our customers in what was their time of need. We’re talking about people being displaced from their homes [and] possessions lost... Esri provided the only platform that’s able to ingest and analyze data at scale.”

Responding to crises would be much easier if organizations could simply trust the outputs of static threat feeds at face value. However, elite corporate security and risk management teams understand that even the most trustworthy data feeds have their limitations when analyzed in isolation. A Fortune 500 company in the financial industry experienced this firsthand, learning that—to overcome the noise of disparate threat feeds and extract valuable signals that empower decision-makers before, during, and after a crisis—incident data needs to be analyzed from a single pane of glass.

To learn how location intelligence can empower your corporate security and business resilience teams to mitigate threats, visit esri.com/ASIS.
Awareness of police misconduct and calls for reform in the United States have increased over the last decade. In some cases, officers were investigated and prosecuted at the state level for their actions. Other incidents investigated by the U.S. Department of Justice resulted in criminal prosecution of a police officer for violating a person’s constitutionally protected rights.

For example, from 2009 to 2012 the U.S. Department of Justice charged 254 police officers throughout the United States with violating the individual rights of Americans.

The private security industry remains historically insulated from claims of civil rights-related violations and the resulting criminal sanctions that can be imposed against security personnel. The private security industry in the United States is much larger than the public sector police force; the industry outnumbers public police by a ratio of at least three to one. This growing number of security personnel could lead to increased civil rights violations.

The security industry is also less regulated, meaning that security personnel have varying amounts of training while public sector police counterparts have mandated training programs. This discrepancy in training can also become a problem because many private security personnel have direct contact with the public, often performing quasi-judicial police-related activities.

CRIMINAL SANCTIONS

One federal statute that has been used to prosecute police officers for civil rights violations is Title 18 of the United States Code, Section 242. It makes it a crime for anyone acting “under color of any law, statute, ordinance,
regulation or custom” to willfully deprive a person of a right or privilege protected by the U.S. Constitution or state and local laws.

The statute also applies to public officials violating a person’s civil rights, including elected officials, public facilities’ care providers, correctional officers, court staff, and security officers. For example, if a police officer assaults a citizen, the officer can be prosecuted for assault and battery and be charged at the federal level for violating the citizen’s Fourth Amendment rights under Section 242.

A conviction under the statute requires three elements. First, the act must violate a protected right guaranteed by the U.S. Constitution. If defendants reasonably understand that their actions are constitutionally impermissible, they can be held accountable for their actions.

Second, the accused must be acting under “color of law,” meaning an officer authorized under state or federal law and acting in his or her official capacity. Lastly, there must be intent to “deprive a person of a right which has been made specific either by the express terms of the Constitution or laws of the United States or by decisions interpreting them,” according to Screws v. United States (U.S. Supreme Court, 1945).

This case clarified that a defendant violated Section 242 when engaged in activities to deprive an individual of his or her rights and was also “aware that what he does is precisely that which the statute forbids,” according to the Court’s opinion.

PROSECUTIONS
Few federal Section 242 prosecutions have involved security personnel. Of those cases, however, private security personnel were prosecuted when they conferred with police powers, were working off duty or moonlighting, or when they were employed as security guards under government contracts. Police powers. Some security personnel were prosecuted under Section 242 when they were granted state-related powers and considered “state actors.”

In the events leading to Williams v. United States (U.S. Supreme Court, 1951), Williams was a private detective with a special police officer's card issued by the City of Miami. He had also taken an oath. Lindsey Lumber Company hired Williams to investigate a series of thefts, and during the investigation Williams used “brutal methods,” displayed his badge, and included the presence of a policeman to “lend
SOME CASES ARE BASED ON VIOLATIONS OF A PERSON’S RIGHT TO BE FREE FROM CRUEL AND UNUSUAL PUNISHMENT.

authority” to the interrogations of four suspects who were “unmercifully punished for several hours,” according to court documents.

A jury convicted Williams of violating Section 242. He appealed the ruling, ultimately appearing before the U.S. Supreme Court to answer the question of whether private persons could be prosecuted under the statute.

In its opinion, the Court reasoned that Williams was acting under color of law and was not a private person. The Court concluded Williams’ actions were an “investigation conducted under the aegis of the state” because a regular police officer attended the interrogation and Williams was “asserting the authority granted him and not acting in the role of a private person.”

The Court upheld his conviction and noted that Williams was “no mere interloper but had the semblance of a policeman’s power from Florida” and his conduct violated the due process right to be free “from the use of force and violence to obtain a confession.”

Another case where private security personnel were convicted under Section 242 was United States v. Hoffman (U.S. Seventh Circuit Court of Appeals, 1974). In the case, two members of the Penn Central Transportation Company’s police force were convicted for physically assaulting trespassers on or near company property.

The officers admitted that they attacked trespassers but argued that they were not acting under Illinois law. Instead, they said they were acting in a purely private capacity and as private persons at the time they committed the crimes.

Ultimately, the appellate court determined the officers were acting under color of law because Illinois state statute had given the railroad company’s police force “police powers as those conferred upon the police of cities,” according to court documents.

Moonlighting. Off-duty police officers granted government powers in a private security capacity have also been prosecuted and convicted of civil rights violations, such as in 2003 when a federal court ruled that a security guard in a strip club was acting under the color of law when he assaulted a dancer.

The off-duty police officer, moonlighting as a private guard, was wearing his badge and gun during the assault, identified himself as a police officer, and prevented the victim from calling the police. He also filed an arrest report against the victim for allegedly assaulting him.

The officer was found guilty under Section 242 and received a 27-month sentence as well as three years of supervised release.

The officer appealed the decision, and the federal circuit court upheld the original ruling (United States v. White, U.S. Court of Appeals for the Sixth Circuit, 2003). A federal judge found that “displaying signs of state authority” by wearing his gun and badge, declaring himself to be a police officer while off-duty, and filing a police report “underscores his imposition of state authority,” according to court documents.

Government contract. The third identified theme is that security personnel can be prosecuted under Section 242 when operating under a contractual relationship with the state.

In cases where security personnel employed as contractors for the state were prosecuted under Section 242, private security personnel had positions within a state agency, making the parties liable for their actions under the statute. Private security personnel working in correctional settings have also been prosecuted under similar circumstances.

Some of these cases are based on violations of a person’s Eighth Amendment right to be free from cruel and unusual punishment. In United States v. Mendez (U.S. District Court for the Eastern District of Texas, 2009), the defendant, an employee of a privately-owned prison transport company, received six months imprisonment and one year of supervised release for assaulting an inmate in her care and custody.

In another case, United States v. Fuller (U.S. District Court for the District of New Mexico, 2009), four defendants who worked for the Wackenhut Corporation, a contractor for a New Mexico county correctional facility.

Employed as correctional officers, two of the defendants physically assaulted an inmate, kicking him in the head multiple times. Prosecutors charged another defendant with failing to prevent the attack and indicted the fourth defendant with conspiracy for fabricating evidence, lying to, and providing false statements to police investigators.

A jury convicted three of the defendants—the two defendants directly involved in the assault and the employee that lied to investigators—for violating Section 242.

Fifth Amendment violations involving contract security also exist. In United States v. Loya (U.S. District Court for the Southern District of Texas, 2009), Loya was employed as a contract guard at an Immigration and Customs Enforcement (ICE) detention facility.

While working in the facility’s infirmary, Loya sexually assaulted female inmates—a violation of the detainees’ Fifth Amendment right, to
“life and liberty, including the right to bodily integrity.” Loya pleaded guilty to Section 242 violations and served a 36-month sentence.

LESSONS
These cases show that private security personnel can be prosecuted under Section 242, but also raise questions as to why so few cases have been brought. This may be because people fail to report violations, prosecutorial discretion, or the use of other federal statutes to prosecute security personnel for civil rights-related violations.

For example, federal prosecutors can recommend a case for diversion instead of prosecuting suspects under Section 242 when the accused agree to probation and dismissal of the charges upon completion of probation.

Additionally, proving all requirements to secure a Section 242 conviction can be a barrier. “Color of law” and the “willfulness” standards can be difficult to establish, subsequently insulating security officers from prosecution.

Despite these factors that may limit prosecutions of private security personnel, the security industry should be aware of these liabilities, which could become greater as public-private partnerships expand to fight crime. Security managers should train their officers to protect the constitutional rights of the people they serve.

BRIAN JOHNSON, PH.D., IS A PROFESSOR IN THE SCHOOL OF CRIMINAL JUSTICE AT GRAND VALLEY STATE UNIVERSITY. HE IS THE AUTHOR OF FOUR BOOKS, INCLUDING PRINCIPLES OF SECURITY MANAGEMENT.

NAOKI KANABOSHI, S.J.D., IS AN ASSOCIATE PROFESSOR IN THE SCHOOL OF CRIMINAL JUSTICE AT GRAND VALLEY STATE UNIVERSITY. HE WRITES ON CONSTITUTIONAL LAW, CIVIL RIGHTS, AND LEGAL ISSUES FOR CRIMINAL JUSTICE PRACTITIONERS.

WHEN THE UNEXPECTED STRIKES EXPECT THE BEST FROM BROWNGUARD®

There are no surprises with the Brownyard Group. For more than 65 years we have been delivering winning insurance solutions to Security Professionals.

Let us take a swing at a competitive insurance quote.

Brownguard®
Insurance when you expect the BEST

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

ALL OF THESE FACTORS CAN POTENTIALLY EXPOSE SECURITY PERSONNEL TO CIVIL RIGHTS-RELATED VIOLATIONS.

Don’t Get Sucker-Punched By Your Insurance!

For product info #19 securitymgmt.hotims.com
A Return on Your Investment

Is time travel possible? Is there life after death? Those questions might be answered before the security professional’s own existential mystery is solved: Can security be a value generator, or is it always a cost?

Lots of ink, pixels, and perhaps tears, have been shed over that very issue. Some practitioners who think security’s value can be quantified as a return on investment cite as examples enhanced business efficiency as a byproduct of security measures, beneficial acquisitions resulting from security’s due diligence, and third-party consulting services spun out of a proprietary security function. José María García Rodríguez, head of digital infrastructure security at Mapfre SA, a Madrid-based insurance company, says that his department is seen as a profit center in terms of fraud prevention and cybersecurity practices.

Detractors say that security will never deliver ROI, and that there are only a few ways to “move the needle on security.” These include significant incidents, compliance requirements, and the security professional’s ability to sell the function to senior management.

The issue of security’s value, and demonstrating it to corporate decision makers, threaded through the four-day curriculum of “Effective Management for Security Professionals,” an annual English-language course held in Madrid by IE Business School and ASIS International under the directorship of Juan Muñoz, CPP. The students, all at mid-to-senior levels of security, tackled business school cases on corporate strategy and leadership, squared off in negotiation scenarios, analyzed the business
case for upgrading card readers in a U.S. airport, and confronted their own leadership strengths and deficiencies.

Your Inner Rock Star

Few security professionals would compare themselves to the “Material Girl,” but Madonna provides an excellent study in adaptability and positioning, said Professor of Strategy Caterina Moschieri. In the 1980s, Madonna styled herself as an ingenue singer, accentuating her prominence through marriage to Sean Penn and assiduously working the media. A decade later, she reinvented herself as a controversial sex symbol, sealing it with a relationship with Warren Beatty and sultry movie appearances. In the 2000s, she became the voice of New Age spiritualism, operating at the intersection of sexuality and politics, and most recently she has emerged as an entrepreneur, philanthropist, and adoptive mother. In each era, she adapted to the zeitgeist and always regained relevance.

Security executives could learn some lessons from her, Moschieri said. For example, experienced CSOs have likely seen corporate priorities and mindsets shift, such as from merger-mania in the 1990s, to the stampede toward globalization in the 2000s, to digital transformation, sustainability, and corporate social responsibility today. The shrewd security professional keeps on top of these trends and how they fit into corporate, and thus security, strategy. A C-suite or board of directors might be laser focused on making their company sustainable, so security executives might position their initiatives in terms of how they advance that corporate goal.

To help get security professionals thinking like trusted business advisors, Moschieri broke students up into groups to evaluate whether they would advise their C-suite to enter several industry sectors. The class harnessed Porter’s 5 Forces, which explain why some industries are more profitable than others. Those forces are industry competition, potential of new industry entrants, power of suppliers, power of customers, and the threat of substitute products. Through this analysis, the teams rejected investments in airlines—aircraft manufacturers, caterers, and airports make good returns while airlines don’t—and higher education, with a qualified endorsement of automotive industry investments. A key takeaway was how to use economic, industry, social, and other trends to position security as a strategic asset.

Let’s Make a Deal

People negotiate every day—with kids, with spouses, with work colleagues, and with neighbors. But when it comes to formal negotiations—over a contract, a large purchase, and so
on—many people unravel or shift into a hyper-aggressive mode. In fact, the hardest task in negotiations is “to be something you’re not,” said Professor of Negotiation Mari Cruz Taboada. When your natural personality leaks through, “you lose credibility,” she warned.

The four golden rules of negotiation are: know your opponent (and yourself), focus on interests (not positions), have a backup plan, and prepare scrupulously—even to the extent of simulating the setting down to table size and configuration and considering social aspects of the negotiation. Key is understanding the other side’s requirements: what are they looking to gain and why? Just as important is knowing what your purpose is, and understanding your default negotiation style, which inexperienced negotiators often revert to.

As a preliminary exercise, students were paired up in an exercise resembling the “Prisoner’s Dilemma.” Each party showed either an open or closed hand on cue. If both participants showed an open hand, they equally shared a hypothetical monetary award. If one showed an open hand and the other a fist, the person with the closed hand received an award that exceeded the total payout if both had revealed an open hand. The other person got nothing. If both parties showed closed hands, neither got anything. Each pair went through three rounds of the exercise, and each round upped the stakes.

Some students deceived their partners immediately, promising to show an open hand but revealing a fist instead. That typically destroyed trust right away, with the counterpart trying to flip the script on the next go-round. Some people cooperated in the first two rounds but betrayed their partner in the third, most lucrative, round. In one case, the partners betrayed each other on the last round and ended up with nothing. One pair cooperated throughout the exercise, collectively reaping more rewards than any other negotiating pair.

The group was then divided into three-person teams to do simulated negotiations in a “Shark Tank” scenario involving an app and smartphones. Afterwards, the professor played videos of the discussions, pointing out signals the class missed. For example, the author unconsciously covered part of his face during a difficult part of the exercise, when he was communicating concern about the inability to protect intellectual property in China. That’s a tell indicating discomfort, the professor said, which others could have exploited. In other groups, video showed participants frowning or looking away during discussions, cues that the speaker did not pick up. Some used a ploy called
“price anchoring.” Although conventional wisdom says that the first person to mention a price is at a disadvantage, several members of the class did so anyway, on the theory that it would psychologically anchor their counterparts to that number. The salvo worked in most cases, and in fact research supports its efficacy.

**Access Control as ATM**

Can a card reader make you a 1,000 percent return on investment? Probably not, but that’s the trap students fell into in an exercise on making the business case for corporate security. After reading a case from the Kellogg School of Management at Northwestern, the class was asked to calculate the return on investment of installing a state-of-the-art credentialing system at San Francisco International Airport. The new system would allow the airport to vastly expand its service capacity—such as by cutting wait times, decreasing service time, and streamlining credentialing operations with full audit and compliance—while meeting federal security requirements and reducing costs such as system replacements, compliance-violation fines, and labor and materials expenses.

For comparison and context, the case provided cost, efficiency, and other failures. Finally, phantom cost savings snuck into the calculus.

The upshot was that there were too many variables to yield an ironclad result. “Play with the numbers before you present them,” advised Gómez, because small changes can produce large discrepancies. It’s also critical that security not develop a business case in isolation. Other business units must get involved—operations, human resources—to develop a better-rounded, more accurate estimate. The lesson? “Never use numbers that you can’t defend,” said Gómez. “You have to look credible.”

**Follow the Leader**

What kind of leader are you? That’s a question that Professor Juan Carlos Pastor helped students confront through exercises, simulations, case studies, and discussions. The least effective leaders only act to respond to problems; they avoid taking action until they need to put out fires. Their staff’s behavior is based on fear. One level up is the transactional leader, who rewards achievement and closely monitors staff performance to correct deviations and errors. This style leads followers to a job-description-level of performance, but no more. The highest tier of leader, said Pastor, is the transformational leader. That person is authentic, builds trust, acts with integrity, inspires others, thinks innovatively, and develops people. Protégés of these leaders become emotionally committed, exceptional performers.

But that doesn’t mean that the perfect leader is wholly transformational. One student proudly announced that he wasn’t transactional because he didn’t micromanage his staff. But it turns out that he wasn’t corrective enough. His staff needed him to more regularly oversee their work and correct errors. Others coached their staffs but didn’t ask for or receive coaching from their own bosses, which could come off as arrogant or hypocritical. Older workers frequently scorned coaching, Pastor said. Many students criticized themselves for not taking enough risks: “We are cowards. We don’t want to hurt anyone’s feelings,” one commented.

True leaders derive their power from themselves, not their position, Pastor said. Managers gravitate to positional power—typified by title, formal authority, visibility, and coercion. Leaders are imbued with personal power, which comes from expertise, energy, charisma, reputation, and social capital.

And that cohort of the IE Effective Management for Security Professionals course, hailing from locations as diverse as Saudi Arabia and Sudan, Sweden and Spain, seemed well on their way to becoming authentic leaders. As Program Director Juan Muñoz concluded, “A leading security executive does more leading, and less security.” They will leave the time travel question to others.

---

Michael A. Gips, CPP, CSYP, CAE, Chief Global Knowledge Officer at ASIS International, was a student in the July 2018 rendition of this course. He has been Vice President of Publishing and Senior Editor at Security Management.
Let’s Talk Security

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

Available on iTunes

Apple and the Apple logo are trademarks of Apple Inc., registered in the U.S. and other countries. iTunes Music Store is a service mark of Apple Inc.
The U.S. Federal Emergency Management Agency’s (FEMA) operation in Puerto Rico after Hurricane Maria was the largest and longest response in the agency’s history.

Yet, as it had been with its responses to Hurricanes Katrina and Sandy, FEMA was widely criticized for how it handled the disaster, which caused more than $100 billion in damages to the island and killed possibly thousands of people.

There were numerous factors that could have influenced this response. A U.S. Government Accountability Office (GAO) report found that 54 percent of federal emergency personnel were not qualified for the positions they held in October 2017—a month after Hurricane Maria made landfall. This challenge was echoed after Hurricane Katrina as well, largely due to differences between federal hiring processes that emphasize administrative background and education versus those in many state and local emergency management departments that recruit

As natural disasters worsen, both security and mitigation are vital components in today’s emergency management landscape.
FEMA also faced numerous challenges that “complicated response efforts,” the GAO said. These challenges included the timing and overlapping of three major hurricanes that caused staffing shortages and logistical challenges that complicated efforts to deploy resources and personnel quickly. They also included the overall limited preparedness of the U.S. Virgin Islands and Puerto Rico for a Category 5 hurricane and the “incapacitation of local response functions due to widespread devastation and loss of power and communications,” the GAO explained.

FEMA “essentially served as the first responder in the early response efforts in Puerto Rico,” the GAO found. “FEMA officials said that many services provided—such as power restoration, debris removal, and commodity distribution—are typically provided by territorial or local governments.”

This again highlighted a major lesson learned in the governmental response in New Orleans when planning and infrastructure deficiencies at the local level hindered the federal government’s ability to provide effective support and logistics.

Furthermore, FEMA and other U.S. government agencies also faced challenges in getting personnel on the ground in Puerto Rico to respond to the hurricane because of limitations on air travel and power outages. Instead of using commercial travel, FEMA had to rely on agency partners to provide chartered air transportation.

The GAO’s analysis also found that while officials from Puerto Rico and U.S. Virgin Islands had engaged in disaster preparedness exercises before Hurricane Maria, they had not experienced or stored the resources that would be necessary to respond to a hurricane of its strength. “Specifically, Puerto Rico officials had not considered that a hurricane would cause a loss of power for as long as Hurricane Maria did,” the report said.

The challenges revealed by the response to Hurricane Maria highlight one major concern with emergency management disciplines—that they vary from place to place. Issues arise when the plans, capabilities, and management of the state and local partners receiving emergency management assistance are thwarted by operational issues that may create obstacles to disaster prevention, mitigation, or recovery.

The Role of FEMA
Since 1803, the role of emergency management has morphed from an act of the U.S. Congress requiring...
that it provide financial assistance to local jurisdictions following disasters to civil defense functions to the current all-hazards approach to continuity of government and disaster recovery.

While the validity of the function of emergency management has never fallen into question, the landscape has changed with the addition of terrorist and active shooter incident mitigation to the already prevalent natural disasters officials plan for, mitigate, and recover from. Emergency managers are responsible for planning for worst-case scenarios.

With FEMA, the U.S. federal government’s ultimate obligation is to help state, local, or individual entities with funding, equipment, and manpower support in overwhelming circumstances. Emergency managers in the private and nongovernmental sector are responsible for the safety of their assets and continuity of essential operations.

Staffing—and even the existence of offices of emergency management—within state and local government agencies, critical infrastructure, education, and business vary widely depending on the area and the scope of the organization.

The role of emergency management has traditionally been defined as a planning and support mechanism for dealing with risk—and risk avoidance—from a broad range of situations. These professionals were normally tasked with disaster planning, emergency communications, command center operations, and obtaining funding for mitigation and recovery.

Emergency managers have had closer relationships with fire services in the past than with the security and law enforcement communities. However, emergency management is integral to the security of organizations, and its integration with the security planning and response landscape is vital to its roles in response to recent major disasters.

To address this area of vulnerability with FEMA, U.S. President Donald Trump appointed Brock Long as FEMA administrator. Before being placed at FEMA, Long worked for the Georgia Emergency Management Agency and was Alabama’s state emergency manager.

The appointment of a career emergency manager marks a departure from prior administrations who typically appointed administrators with no prior experience in disaster management. FEMA is also addressing how it hires, trains, and retains staff to ensure that it is prepared to respond to disasters that may occur simultaneously.

With FEMA revamping its operations and staffing up in response to the latest hurricane season; it is imperative for state, local, and private emergency management to do the same. Many emergency managers outside of the U.S. federal government—and larger states and cities—perform basic business continuity planning to ensure incident survival.

**Assessment**

Consideration of security threats is essential to the operational survival of local jurisdictions, businesses, and non-governmental organizations. Therefore, emergency management must expand its current planning, response, and recovery operations to include security threats to ensure the physical safety of first responders and stakeholders.

Organizations should create emergency management functions within security management roles. Jurisdictions that already have emergency managers can also assess current operations and seek to create preincident working relationships with law enforcement and security agencies. These emergency managers are normally the incident commanders during man-made disasters, like terrorist attacks, until such time as the FBI or law enforcement takes over.

An example of this on the U.S. federal level was illustrated when former President George W. Bush signed the Homeland Security Act of 2002 into law, creating the U.S. Department of Homeland Security (DHS). The act charged the new cabinet-level agency with the mission of protecting the United States from terrorist attacks and minimizing the damage from attacks and disasters. This act incorporated FEMA into DHS.

**Teamwork**

To ensure that security management and emergency management are working together, the author organized three roles into one directorate while serving as a director for North America’s largest medical board: chief security officer, head of investigations, and emergency manager. This configuration allowed the security department to work with cross-functional staff to create policies, procedures, and countermeasures that would allow the organization to protect its human, physical, and intellectual assets in an efficient way that addressed both emergency mitigation and security threats.

Assuring that emergency management coordinates effectively with all facets of public safety is a key function of mitigation. This differs from other emergency management disciplines in that it presents long-term solutions to reducing risk, instead of accepting that risks exist and preparing, responding to, or recovering from their eventuality.

However, mitigation involves coordination across a wide spectrum of public
and private sector stakeholders. For instance, New Orleans officials hampered evacuation efforts after Hurricane Katrina by parking its fleet of buses in a lot susceptible to flooding—which delayed evacuation procedures until a new fleet could be sourced.

In the wake of Hurricane Maria, FEMA conducted its own after-action report—in addition to the GAO analysis—and is making changes to address security planning and mitigation to address the shortcomings of the response in Puerto Rico.

“FEMA...made improvements in staffing for incidents, logistics operations, and refining communications from land mobile radios to satellite communications,” wrote Jim H. Crumpacker, CIA, CFE, director of departmental GAO-OIG Liaison Office for DHS in its response to the GAO report. “Finally, FEMA has updated high priority national level contracts to be better prepared to cope with responding to multiple concurrent disasters across the nation.”

Additionally, FEMA incorporated objectives in its 2018 to 2022 strategic plan, including improving readiness of incident workforce cadres; building staff, equipment, and contract capacity; and streamlining the disaster survivor and grantee experience.

“Disaster can strike at any time and in any place, building slowly, or occurring suddenly without warning,” Crumpacker wrote. “FEMA is part of a larger team of federal agencies, state, local, tribal, and territorial governments, and nongovernmental stakeholders that share responsibility for emergency management and national preparedness.”

Those in charge of security for a particular location need to cross-plan for natural disasters and environmental threats. They also need to factor in the probable response by their federal, state, and local partners.

Just as threats like active shooters, unpermitted protests, and flash mobs have changed the face of security management, security threats have changed the face of emergency management. It’s incumbent upon security and emergency management professionals to work together before an incident to plan and assess their threats accordingly.

A. BENJAMIN MANNES, CPP, CESP, IS THE FORMER DIRECTOR, OFFICE OF INVESTIGATIONS, FOR THE AMERICAN BOARD OF INTERNAL MEDICINE, AND HAS SERVED FEDERAL, MUNICIPAL, AND NONGOVERNMENTAL EMPLOYERS IN LAW ENFORCEMENT, INTELLIGENCE, AND HOMELAND SECURITY CAPACITIES THROUGHOUT THE CONTINENT. HE CURRENTLY SERVES AS A PUBLIC SAFETY AND SECURITY CONSULTANT AND CAN BE CONTACTED AT WWW.MANNESANDASSOCIATES.COM.
Join the Security 5K/2K at ISC West on April 11, 2019 at Sunset Park, Las Vegas as we celebrate our 10 year anniversary! All proceeds generated by the race will be contributed to Mission 500 to help children in crisis in the USA. Show your industry pride, have fun, stay healthy and help fight poverty in America!

**Ways to get involved:**
- Sign up to run or walk
- Create a team within your organization
- Start a fundraising campaign
- Sponsor the event
- Volunteer

Learn more and register at Security5K.com
At GSX 2018, the exhibit hall was transformed into a learning lab environment, which facilitated discussions between security professionals and their vendor partners about how innovative solutions can solve today’s problems and shape tomorrow’s organizational security strategies. The overwhelmingly popular D3 Xperience returns in 2019, providing attendees with showcases and hands-on demonstrations around the use of drones, droids, and anti-UAV defense systems.

Networking opportunities in interesting places will be plentiful, from the opening reception to the President’s Reception. A happy hour on the show floor will enable participants to mingle informally. And there will be other opportunities to meet with like-minded people, from CSOs and women in security to young professionals and executives from around the globe.

GSX 2019 will deliver a diverse array of educational formats, experiential learning, and dynamic and cutting-edge educational tracks focused on embracing technology to find effective solutions to security challenges.

Start making plans today to attend GSX 2019. Registration is open at GSX.org/2019. Save $200 on the All-Access Pass when you register by 14 June. Expo-Only registration is free when you preregister any time before the show begins.

GSX 2019 HEADS TO CHICAGO

TWENTY THOUSAND SECURITY PROFESSIONALS will gather 8–12 September in Chicago, Illinois, USA, for Global Security Exchange (GSX) 2019—the newest evolution of the security industry’s flagship event. Formerly the ASIS International Annual Seminar and Exhibits, GSX unites the entire industry for the most comprehensive, exciting security event in the world.

GSX 2019 will deliver a diverse array of educational formats, experiential learning, and dynamic and cutting-edge educational tracks focused on embracing technology to find effective solutions to security challenges.

At GSX 2018, the exhibit hall was transformed into a learning lab environment, which facilitated discussions between security professionals and their vendor partners about how innovative solutions can solve today’s problems and shape tomorrow’s organizational security strategies. The overwhelmingly popular D3 Xperience returns in 2019, providing opportunities to meet with like-minded people, from CSOs and women in security to young professionals and executives from around the globe.

Start making plans today to attend GSX 2019. Registration is open at GSX.org/2019. Save $200 on the All-Access Pass when you register by 14 June. Expo-Only registration is free when you preregister any time before the show begins.

#MYASIS MEMBER STORIES

Are you making the most of your ASIS membership? Do you wonder what motivates members to keep turning to the ASIS community? In the new #MyASIS video campaign, members describe how ASIS has supported them during defining moments of their careers.

For years, ASIS members have used the #MyASIS hashtag on social media
to share their ASIS experiences. Now, #MyASIS takes on a new life. We are excited to share these stories with you!

Visit the ASIS International YouTube channel at youtube.com/ASISInternational to watch a new member story every Monday. Videos will also be available on the ASIS website and throughout social media: Facebook, LinkedIn, and Twitter.

**PSEO GUIDELINE UPDATED**

ASIS International is rolling out the first update to the Private Security Officer (PSO) Selection and Training Guideline in nine years.

The private security industry employs millions of security officers worldwide. This updated PSO Guideline provides a framework that organizations can implement in their officer hiring and training programs.

Applicable to both proprietary and contract security, the guideline’s framework can be tailored to an organization’s unique operational and regulatory needs. ASIS members are entitled to a free download of each ASIS standard and guideline. To get

---

**ASIS BOARD OF DIRECTORS**

**PRESIDENT**  
Christina Duffey, CPP  
Sos Security LLC  
Phoenix, Arizona

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

**TREASURER**  
Malcolm C. Smith, CPP  
Qatar Museums  
Doha, Qatar

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

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

---

**ASIS CHAPTER ANNIVERSARIES**

Congratulations to the ASIS Chapters celebrating milestone anniversaries in the first quarter of 2019.

**10 yrs**  
Kuala Lumpur, Malaysia

**30 yrs**
- Toronto
- Jeddah

**35 yrs**
- Fresno Valley
- South Jersey

**45 yrs**
- Smoky Mountain
- Venezuela
- Florida West Coast

**60 yrs**
- Greater New Orleans

---

**#MYASIS IMAGE OF THE MONTH**

LISA TERRY  
Spending valuable work time with some of the dedicated leaders from Group 4 (NC, SC, GA, FL, TN, and Northern AL) at the 2019 ASIS International Leadership Exchange. #myasis #leadership #wncasis
CERTIFICATION PROFILE
JAMES MORRIS, CPP

To James Morris, CPP, a career in security is all about the people. “I’ve traveled to amazing places, met truly fantastic professionals at every level of organizations, and worked alongside interesting companies, but my most memorable moments are all people-related,” he notes. “The colleagues I have supported. The clients who have been open to learning and collaborating. We are a people industry. People are the key factor.”

Morris was an engineering student when he enlisted with the British Army for a tour in Iraq in 2004. Near the end of his tour, he was approached by a security company filling contracts in the region, and he signed on for two years of reconstruction work in Iraq. He pivoted to an intelligence role for the British Embassies in Basra, Iraq, and Afghanistan. Then, in 2005, he took on a position as a security analyst for the gold mining industry in sub-Saharan Africa.

While spending more than a decade overseas, he experienced the power of ASIS to help cultivate his security prowess. “I heard about ASIS while looking for opportunities to increase my knowledge and broaden my network when working in Afghanistan,” he shares. “I’ve found that the greatest benefit of membership is the professional network. Wherever I go, I can rely on ASIS members to answer my call.”

Recognizing the need for an ASIS chapter after he relocated to Ghana, he was a founding member of the ASIS Ghana Chapter in late 2011 and served as its inaugural secretary in 2012.

Returning to the United Kingdom a few years later, he served as security manager of the Europe, Middle East, and Africa (EMEA) region for two financial services firms. These roles require a healthy amount of travel—he currently spends seven to ten days per month abroad—as he supports security needs around the globe.

Driven to prove his place among his management peers, Morris earned the Certified Protection Professional (CPP®) certification in 2016. “The CPP is the stamp of authority that demonstrates to other professionals that I have the knowledge and experience needed by senior leaders in the security industry,” he says.

“Studying for the exam was also an opportunity to identify best practices, and it amazed me the number of times I was able to link examples from my studies to actual scenarios that I had worked through,” he adds. “I still refer to my study materials while working with clients to discuss best practices and global standards.”

It all maps back to people. With a wealth of experience and the gold standard of security certification at his back, he pays his experience forward to the young professionals of the ASIS United Kingdom Chapter.

“I find that the more I put into my membership, the more I get out of it,” he explains. “So I serve as director of the UK Young Professionals Group and try to give as much time as I can to ASIS members who ask for help. My work history demonstrates how dynamic our industry is. Whether you’re a security officer or an analyst, or working in investigations, compliance, or cyber roles, there are more security careers available than you might think. I want to do my part to communicate these opportunities to the leaders of tomorrow.”

PROFILE BY STEVEN BARNETT, ASIS COMMUNICATIONS COORDINATOR

2019 ASIS INTERNATIONAL CUP
Do you want to receive a free all-access pass to GSX, a three-night hotel reservation, and $500 towards GSX travel expenses?

The ASIS International Cup, the Society’s annual member-get-a-member recruitment campaign, kicks off this month and continues through June, offering great prizes to top recruiters—including the GSX Grand Prize to the person who recruits the most members.

The Cup is an important way for ASIS to reach new members and strengthen the association for years to come. To learn how you can get involved and to locate recruitment tools, visit asisonline.org/InternationalCup and start recruiting!

LIFE MEMBER
ASIS congratulates Michael A. Pepper, CPP, PSP, on becoming a Life Member. As an ASIS member for 20 years, he supported the Society on local and regional levels. He served as chapter chair and vice chair for the New Zealand Chapter. Pepper also served as a regional vice president and a member of the ASIS Asia Pacific Advisory Council. He earned his CPP in 2002 and his PSP in 2004. Pepper now resides in the United Kingdom.

MEMBER BOOK REVIEW
The Five Technological Forces Disrupting Security. By Steve Van Till. Butterworth-Heinemann; available from ASIS; asisonline.org; item #2953; 244 pages; $62 member; $66 nonmember.

This provocative book by Brivo CEO Steve Van Till covers a wide spectrum of topics regarding emerging technologies and the speed at which technology integration is taking place. The Five Technological Forces Disrupting Security clearly explains why physical security industry professionals should educate themselves in this area and be aware of the benefits that technol-
ogy offers, focusing on cloud, social, mobile, big data, and the Internet of Things (IoT).

The author provides a unique perspective on how new technologies are affecting the physical security systems that we use every day. He demonstrates that the security industry has been slow to adopt change and is behind on making any real integrated transformation. Drawing on his years of experience as both a practitioner and a leader of industry associations, Van Till walks the reader through the issues of each technology, providing detailed guidance on how to understand what is working and what is not. He has a clear futuristic vision for the industry and how it should move forward, with strategies such as combining social communication with buildings instrumented with IoT.

Not all emerging technology works well with other technology because many systems are proprietary, and several vendors are reluctant to adopt national or international standards when they upgrade technology. This book makes an excellent business case for moving to cloud-based security. Van Till emphasizes the importance of the cloud as the platform for everything else. He argues that if you’re not moving towards a cloud strategy in your physical security, you’re cutting yourself off from all the new technology opportunities available including mobile, big data, IoT, and artificial intelligence.

The author also explains that information gathered through IoT will help the security professional make better decisions about what to do next, how to protect people, and how to keep buildings and assets safe. The proliferation of connected sensors leads to an explosion in information, thus to better situational awareness and safety.

Well written and easy to comprehend, this book was named the ASIS Security Industry Book of the Year. If you care about technology and security in today’s facilities, you should read this book. Overall, it is an enlightening read.

REVIEWER: Mark H. Beaudry, CPP, is a frequent reviewer for Security Management and a longtime member of ASIS.

ASIS CLASSROOM PROGRAMS

JUNE
24–25 Enterprise Security Risk Management (ESRM), Atlanta, Georgia, USA
24–25 Executive Protection, Atlanta, Georgia, USA
24–26 ASIS Assets Protection Course: Practical Applications (APC II), Atlanta, Georgia, USA

ASIS GLOBAL EVENTS

MARCH
27–29 ASIS Europe, Rotterdam, The Netherlands

SEPTEMBER
8–12 Global Security Exchange (GSX), Chicago, Illinois, USA

ASIS WEBINARS

MARCH
20 Travel Safety and Security for Traveling Abroad
View all educational offerings at asisonline.org/education

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, email ASIS International: asis@asisonline.org.

ASIS
SECURITY
MANAGEMENT
USE OF FORCE. Florida’s Stand Your Ground law provides police officers immunity from prosecution and justifies their use of deadly force, according to the Florida Supreme Court.

The ruling stems from a lawsuit brought after Broward County Sheriff’s Deputy Peter Peraza shot and killed Jermaine McBean in 2013. In the lawsuit, Peraza claimed that McBean pointed a gun at him. McBean was walking home holding an air rifle that he had just purchased at a pawn shop.

Someone called 911 to report McBean walking through their neighborhood holding a firearm. Peraza and two other deputies responded to the call, arrived on the scene, and commanded McBean to stop. McBean continued to walk—allegedly because he was wearing headphones and could not hear the officers.

Peraza claimed that after McBean walked into his apartment complex with the deputies behind him, he turned toward the deputies and pointed the air rifle at them. Peraza—assuming the air rifle was a real gun—then shot McBean twice, killing him. McBean’s family contests the sequence of events.

DISCRIMINATION. Technical Marine Maintenance Texas LLC and Gulf Coast Workforce LLC will pay $857,868 in civil penalties for violating the Immigration and Nationality Act (INA). The two companies discriminated against workers based on their citizenship status during the employment eligibility verification process by asking U.S. citizens to produce IDs and Social Security cards but asking for immigration documents from non-U.S. citizens. “The INA prohibits employers from limiting workers’ choice of documentation to present for employment verification based on the workers’ citizenship, immigration status, or national origin,” according to the U.S. Department of Justice.


DISCRIMINATION. Wilmington Trust Corporation will pay $700,000 to settle a disability discrimination lawsuit filed by the U.S. Equal Employment Opportunity Commission (EEOC). The corporation had a policy of placing employees with disabilities or impairments on involuntary leave unless a medical provider cleared the employee to return to work with no restrictions. This denied employees of reasonable accommodations for disabilities, an alleged violation of the Americans with Disabilities Act. (EEOC v. Wilmington Trust Corporation, U.S. District Court for the Southern District of New York, No. 17-cv-05077, 2018)

HARASSMENT. The owner-operator of more than 12 Subway franchises will pay $80,000 to settle a sexual harassment lawsuit brought by the U.S. Equal Employment Opportunity Commission (EEOC). The EEOC alleged that a former general manager sent text messages to two 17-year-old female applicants, offering them positions in exchange for sex. The teenagers did not comply, and they were not hired. The franchises’ owner will pay the penalty, revise its policy for prohibiting sexual harassment, conduct anti-harassment training, post a public notice about the settlement, and report all sexual harassment complaints to the EEOC. (EEOC v. Draper Development, LLC, U.S. District Court for the Northern District of New York, No. 1:15-cv-877, 2018)
of events and claimed that the use of deadly force was unjustified. A grand jury indicted Peraza for manslaughter, but a trial judge dismissed the case based on Peraza’s argument that he should be granted immunity from prosecution under Florida’s Stand Your Ground self-defense law.

The law says that “a person is justified in the use of deadly force and does not have a duty to retreat if... he or she reasonably believes that such force is necessary to prevent imminent death or great bodily harm to himself or herself or another...” according to court documents. The law also grants immunity from criminal prosecution or civil action for a “justifiable use of force.”

The state appealed the trial judge’s decision, and ultimately the case went before Florida’s Supreme Court. It ruled in favor of Peraza because Stand Your Ground provides immunity to any person who acts in self-defense. “Put simply, a law enforcement officer is a ‘person’ whether on duty or off, and irrespective of whether the officer is making an arrest,” the court wrote in its opinion. “Although neither of the two statutes defines the word ‘person,’ it must be given its ‘plain and ordinary meaning.’”

Because of this, “law enforcement officers are eligible to assert Stand Your Ground immunity, even when the use of force occurred in the course of making a lawful arrest,” the court added. (Florida v. Peraza, Supreme Court of Florida, No. SC17-1978, 2018)

**FRAUD.** German automotive company IAV GmbH pleaded guilty to a felony and will pay a $35 million fine for its role in a Volkswagen AG corruption scheme to sell diesel vehicles in the United States by cheating on emissions tests.

The U.S. Department of Justice (DOJ) charged IAV with one count of conspiracy to defraud the United States and Volkswagen’s U.S. customers by violating the Clean Air Act and misleading the Environmental Protection Agency and others about whether their vehicles complied with U.S. vehicle emissions standards.

“IAV and its co-conspirators knew the vehicles did not meet U.S. emissions standards, worked collaboratively to design, test, and implement cheating software to cheat the U.S. testing process, and IAV was aware that VW concealed material facts about its cheating from federal and state regulators and U.S. customers,” according to the DOJ.

“By at least 2008, an IAV manager knew the purpose of the defeat device software, instructed IAV employees to continue working on the project, and directed IAV employees to route VW’s requests regarding the defeat device software through him; the manager was involved in coordinating IAV’s continued work on it,” the DOJ said.

As part of the plea agreement, IAV will plead guilty to the crime, will serve probation for two years, will be placed under an independent corporate compliance monitor for two years, and will fully cooperate with the ongoing DOJ investigation and prosecution of individuals involved in the Volkswagen scheme.

IAV’s guilty plea is one of the most recent developments in the DOJ’s investigation. Volkswagen previously pleaded guilty to criminal charges in 2017 that it deceived U.S. regulatory agencies by installing defeat devices in diesel vehicles emissions control systems that were designed to cheat emissions tests. Volkswagen paid a $2.8 billion criminal fine and agreed to an independent corporate compliance monitor for three years.

The DOJ also charged eight individuals for their role in the scheme; two of them pleaded guilty and were sentenced. The other six are thought to be in Germany. (U.S. v. IAV GmbH, U.S. District Court for the Eastern District of Michigan, No. 16-CR-20394, 2018)

**REGULATIONS**

**ANTI-MONEY LaunderING.** UBS Financial Services (UBSFS), Inc., will pay a $14.5 million civil penalty for willful violations of the Bank Secrecy Act. The U.S. Treasury Department’s Financial Crimes Enforcement Network (FinCEN) found that UBSFS failed to develop and implement appropriate, risk-based anti-money laundering (AML) programs to address the risks associated with accounts for traditional brokerage and banking services.

“UBSFS failed to implement appropriate policies and procedures to ensure the detection and reporting of suspicious activity through all accounts—particularly for those accounts that exhibited little to no securities trading,” FinCEN said in a press release. “The firm did not adequately structure its AML program to address the use of securities accounts for the purpose of moving funds rather than trading securities.”

**ISSUE:** Cryptocurrency  
**BILL:** H.R. 428  
**VENUE:** U.S. House of Representatives  
**STATUS:** Passed  
**SIGNIFICANCE:** Would require the undersecretary of homeland security for intelligence and analysis to develop and share a threat assessment on terrorists’ use of cryptocurrency.

**ISSUE:** Intelligence  
**BILL:** H.R. 769  
**VENUE:** U.S. House of Representatives  
**STATUS:** Passed  
**SIGNIFICANCE:** Would create a board at the U.S. Department of Homeland Security to coordinate and integrate intelligence, activities, and polices related to counterterrorism efforts.
FinCEN also found that UBSFS failed to provide resources to ensure AML compliance, including inadequate staffing that led to a backlog of alerts and decreased the firm’s ability to file suspicious activity reports (SARs) in a timely matter.

“Law enforcement investigators rely upon SARs to recognize and pursue financial criminals and other bad actors to protect our national security and our people from harm," FinCEN said. “Allowing a backlog of transaction alerts and delays in filing SARs stifles the ability of law enforcement agents to fulfill this critical national security mission.”


**FIREARMS.** The DOJ issued a new rule that bans bump stocks, devices that make semiautomatic rifles fire in sustained, rapid bursts—similar to an automatic weapon.

The new regulation bans the sale or possession of bump stocks. Anyone who owned these devices had until late February to destroy them or turn them in to the U.S. Bureau of Alcohol, Tobacco, Firearms, and Explosives.

“With limited exceptions, the Gun Control Act, as amended, makes it unlawful for any person to transfer or possess a machine-gun unless it was lawfully possessed prior to the effective date of the statute," according to the regulation. “The bump-stock-type devices covered by this final rule were not in existence prior to the effective date of the statute, and therefore will be prohibited when this rule becomes effective.”

Bump stocks were used in the mass shooting in Las Vegas in 2017, where a gunman opened fire to kill 58 people and wound hundreds of others at a country music festival. U.S. President Trump directed DOJ officials to find a way to ban the devices following the mass shooting at Marjory Stoneman Douglas High School in Parkland, Florida, even though bump stocks were not used to carry out that shooting.

**European Union**

**DISASTER RESPONSE.** The European Parliament Committee on the Environment, Public Health, and Food Safety reached a deal to move legislation forward that would aid EU member states’ disaster response.

The draft law would create a “rescEU” reserve of resources, including field hospitals, emergency medical teams, high-capacity pumps, and forest fire-fighting plans. When a disaster strikes, the rescEU, following a decision by the European Commission, would step in with additional resources to help the affected member states.

“We managed to work quickly to be ready before next summer and avoid another Greece 2018 and Portugal 2017,” said lead negotiator Elisabetta Gardini of Italy in a statement. “Effective means and tools were needed to save lives.”

**New York City**

**ACCOMMODATION.** The New York City Council passed legislation that creates new requirements for lactation rooms for employees.

The law, which goes into effect on 18 March 2019, requires employers with at least four employees to create lactation rooms for employees and maintain a written policy on their accommodation that is made available to employees when they are hired.

This column should not be construed as legal or legislative advice.
REQUEST DETAILED PRODUCT INFORMATION THROUGH OUR MONTHLY E-RESPONSE, VISIT HTTP://SECURITYMGMT.HOTIMS.COM, OR USE YOUR SMART PHONE TO ACCESS THE QR CODE ON THIS PAGE.

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

<table>
<thead>
<tr>
<th>CIRCLE #</th>
<th>PAGE #</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>25</td>
</tr>
<tr>
<td>S2</td>
<td>06</td>
</tr>
<tr>
<td>20</td>
<td>47</td>
</tr>
<tr>
<td>06</td>
<td>13</td>
</tr>
<tr>
<td>02</td>
<td>04</td>
</tr>
<tr>
<td>19</td>
<td>43</td>
</tr>
<tr>
<td>15</td>
<td>31</td>
</tr>
<tr>
<td>S1</td>
<td>02</td>
</tr>
<tr>
<td>08</td>
<td>17</td>
</tr>
<tr>
<td>09</td>
<td>19</td>
</tr>
<tr>
<td>26</td>
<td>68</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CIRCLE #</th>
<th>PAGE #</th>
</tr>
</thead>
<tbody>
<tr>
<td>18</td>
<td>38-39</td>
</tr>
<tr>
<td>07</td>
<td>15</td>
</tr>
<tr>
<td>23</td>
<td>55</td>
</tr>
<tr>
<td>S3</td>
<td>12</td>
</tr>
<tr>
<td>13</td>
<td>27</td>
</tr>
<tr>
<td>10</td>
<td>21</td>
</tr>
<tr>
<td>22</td>
<td>54</td>
</tr>
<tr>
<td>01</td>
<td>2-3</td>
</tr>
<tr>
<td>16</td>
<td>35</td>
</tr>
<tr>
<td>S2</td>
<td>11</td>
</tr>
<tr>
<td>11</td>
<td>23</td>
</tr>
</tbody>
</table>

ADVERTISERS ONLINE

Abloy Security, Inc.
www.abloyusa.com

Altronix Corp.
www.altronix.com

Ameristar Security Products
www.ameristarsecurity.com

AMICO
www.amicosecurity.com

Axis Communications
www.axis.com

Brownyard Group
www.brownyard.com

CEIA USA
www.ceia-usa.com

Dataminr
www.dataminr.com

Detex Corporation
www.detex.com

DSI (Designed Security Inc.)
www.dsigo.com

DSX Access Systems, Inc.
www.dsxic.com

esri
www.esri.com/ASIS

G4S
www.g4s.us

Mission 500
www.mission500.org

NAPCO Security Services
www.napcosecurity.com

Par-Kut International, Inc.
www.parkut.com

Research Electronics, Int'l
www.reiusa.net

SDC – Security Door Controls
www.sdcsecurity.com

SecurAmerica
www.securamericallc.com

Special Response Corporation
www.specialresponse.com

TEAM Software
www.teamsoftware.com

TSCM America
www.tscmaroma.com

*Security Technology supplement denoted in orange.
**TERMINAL SURVEILLANCE**

A new rail freight hub, **iPort Rail**, opened in South Yorkshire, United Kingdom, with 6 million square feet of space across 337 acres. The new iPort Rail terminal features an 800-meter reception siding and two 400-meter handling sidings, with storage for 1,500 shipping containers. **Buckingham Group Contracting Ltd.** worked with **Daemon Fire & Security** to implement the video surveillance system for the perimeter of the enormous terminal. The company chose **Bosch** cameras and video management, towers from **Altron**, and an Ethernet switch network from **AMG Systems**.

**AWARD**

**Senstar** received the Fixture Seal of Approval from the **International Dark-Sky Association** for its Senstar LM100 perimeter intrusion detection and intelligent lighting system. The seal recognizes lighting that minimizes glare, reduces light trespass, and doesn’t pollute the night sky.

**CONTRACT**

**USmax Corporation** was awarded a contract by the **U.S. Department of State’s** Bureau of Overseas Buildings Operations. USmax will provide technical security services for intrusion detection, access control, CCTV, emergency notification, explosives detection, and IP-based security systems.

**ANNOUNCEMENT**

**ProdataKey** released a free white paper, *Safely Invisible: The Powerful Security of Cloud-Based Access Control*, to help dealers and end users understand the risks and benefits of cloud-based access control.

**MERGERS & MOVES**

**Qognify** acquired **On-Net Surveillance Systems, Inc.**

**ACRE** acquired **Open Options**

**Identiv Inc.** acquired **Viscount Systems, Inc.**

**Qognify** becomes one of the largest video management, video analytics, and critical incident management companies in the world.

**Bold Perennial** acquired **SIMS, Inc.**

The acquisition signifies continued growth and innovation, as well as expanded products and services for both companies’ customers.

**PARTNERSHIPS**

**BIOMETRIC ACCESS**

**Auburn University** installed **IDS software** and **Access200 iris readers** from **Princeton Identity** to secure athletic facilities.

**CYBERSECURITY**

**Ernst & Young LLP** and **Symantec Corporation** formed a strategic alliance to address intellectual property and data protection.

**FRAUD PREVENTION**

**ACI Worldwide** joined forces with **BioCatch** to protect customers from online banking fraud.

**AWAWARENESS**

**Texas A&M University-San Antonio** deployed the **SafeZone indoor positioning solution** from **Critical-Arc** for detailed views of buildings in emergencies.
MARKETPLACE

FOR MARKETPLACE

FORCE TRAINING INSTITUTE of Sherman Oaks, California, offers the Multi-Threat Shield (MTS) for law enforcement personnel and others who need a light, versatile ballistic shield. The rapidly deployable shield defends against multiple impacts from handgun, shotgun, and pistol caliber submachine guns, as well as attacks from knives and blunt objects. The device looks like a laptop computer bag and weighs about 7 pounds. It includes an expandable utility pouch with covert access to carry a wide range of equipment and accessories, from a handgun or Taser to a laptop or tablet. A flick of the wrist deploys a 3-foot long shield of protection for one or more people. The MTS is certified NIJ Level IIIA (Level III with optional Rifle Plate Insert). 301

HANWHA TECHWIN AMERICA of Teaneck, New Jersey, introduced the Wisenet TNV-7010RC corner mount camera. Focused on the unique needs of correctional facilities, the IP-based camera’s corner mount design provides broad room coverage. Infrared (IR) is emitted at a higher wavelength than traditional glowing IR emitters, making it invisible to the human eye so as not to disturb inmates at night. The camera captures video at up to 30 frames per second, so details are preserved. The vandal-resistant housing includes shock detection to alert operators if the camera is subject to abuse. Additional features include a built-in microphone and audio line out for two-way communication. Multiple privacy-masking zones can also be configured. 302

KEY CONTROL

The KeyWatcher Touch key management system from MORSE WATCHMANS of Oxford, Connecticut, is a modular, scalable key control and management solution with intuitive, time-saving features. Updates include a new database design, a desktop fingerprint reader that allows users to enroll fingerprints through TrueTouch software, and the ability to use multiple KeyWatcher Touch server instances with a single SQL database. KeyAnywhere enables return of a key to any KeyWatcher in the enterprise, and KeyFind helps the user locate a specific key. My Keys Out allows users to see which keys they have checked out and when their keys will become overdue. 303
FIVE STEPS FOR OPTIMIZING CRISIS NOTIFICATION

DORIAN AMSTEL, CPP, IS THE SENIOR DIRECTOR OF PHYSICAL SECURITY FOR DYNCORP INTERNATIONAL LLC, A MILITARY CONTRACTOR WITH OPERATIONS IN THE MIDDLE EAST.

1. **COOPERATE.** Implementing a crisis notification system requires cooperation. Once HR has determined that all data is accurate, policies and procedures should be in place before using the system.

2. **DELEGATE.** Just because an organization has a crisis notification system does not mean it’s being properly used. Appointing an apt system administrator is crucial; typically, the company’s head of global resiliency or crisis management is well-suited for the role. For example, an organization’s head of crisis management is often familiar with the current in-house teams, so he or she can outline the benefits of such systems and incentivize the teams to adopt the technology.

3. **REGULATE.** Establish distinct administrative rights and limits. The system will have employees’ personally identifiable information, making regulated access to such information critical. A delineated role structure with specific system rights per level will curb potential abuse. This is crucial when it comes to the executive crisis management team, which usually includes certain C-suite executives. Access to such groups must be closely safeguarded.

4. **TRAIN.** Training is integral to getting people comfortable with the system, and it should not solely consist of a cursory introduction. Vendors have training resources for their systems, from online videos to quick reference guides to prerecorded Web-based modules. They may even offer live training sessions via WebEx or another virtual meeting platform. In most cases, you can insist on including training with the system while negotiating the contract.

5. **TEST.** Failure to properly train employees can have serious, wide-ranging effects. Just think back to the message sent out by the Hawaii Emergency Management Agency in January 2018: “BALLISTIC MISSILE THREAT INBOUND TO HAWAII. SEEK IMMEDIATE SHELTER. THIS IS NOT A DRILL.” The employee who sent the message did not know that a drill was taking place and thought a real attack was underway. Crisis management tabletop exercises and other training iterations should include use of the system as it would be applied in a real-life situation. Testing employees on their ability to properly use the system is important in establishing and communicating clear protocols that differentiate training from real-life scenarios.
LET YOUR VOICE BE HEARD.
WITHOUT SAYING A WORD.
FOLLOW US ON SOCIAL MEDIA

SECURITY MANAGEMENT

Follow us on facebook at: facebook.com/SecMgmtMag

Follow us on twitter at: @SecMgmtMag

Keep in touch with Security Management – digitally. Voice your opinions by commenting or tweeting. You can also like us or follow us to get up-to-date notifications about breaking news, events, and access to the invaluable content Security Management provides online and in print.
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 | DSXINC.COM

For product info #26 securitymgmt.hotims.com