ORGANIC GROWTH
$72 MILLION NEW REVENUE
SINCE JANUARY 1ST
Since January 1, 2019, we have added $72 million in organic growth revenue across the United States. In the last few ads, we have mentioned several new acquisitions and partnerships, but we have also been focused on organic growth from new and existing customers. Here are some of the regions across the country where we have added significant growth since the beginning of the year:

<table>
<thead>
<tr>
<th>Region</th>
<th>Revenue</th>
</tr>
</thead>
<tbody>
<tr>
<td>Atlanta</td>
<td>$30,500,000</td>
</tr>
<tr>
<td>New York</td>
<td>$18,400,000</td>
</tr>
<tr>
<td>Seattle</td>
<td>$9,500,000</td>
</tr>
<tr>
<td>Detroit</td>
<td>$4,000,000</td>
</tr>
<tr>
<td>Raleigh-Durham</td>
<td>$2,000,000</td>
</tr>
<tr>
<td>Boston</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Florida</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Hawaii</td>
<td>$1,400,000</td>
</tr>
</tbody>
</table>

As a potential customer, why is this important? We are in business for the long haul. We are not for sale. We must give you better service and for less money. Private equity is fairly predictable; they are focused on shareholders, not customers, and in general, they want to sell and reap as much profit as possible in 3 to 5 years. Our mindset is **SERVICE, SERVICE, SERVICE**. Their mindset is **CUT, CUT, CUT** and **SELL**. So who do you want to manage your security?

If you have questions, call me and let’s talk; my office line is 404-926-4202.
CUTTING EDGE

The new quarterly supplement from Security Management examines technological solutions to security challenges. Security Technology features in-depth articles about revolutionary technologies, case studies, and thought leadership pieces from industry experts.

Watch for the next issue, bundled with June’s Security Management.
“The absence of chest-cam video reeks of coverup.”

High Point University Chief of Security Jeff Karpovich, CPP, on the pros and cons of body cameras. PAGE 17

395

The number of years it will take for the U.S. Coast Guard to repair its coastal infrastructure at current funding levels. PAGE 18

€50M

The first major fine handed down in response to a violation of the EU’s General Data Protection Regulation. PAGE 32

43%

Percentage of the U.S. workforce estimated to be involved in the gig economy by 2020. Security professionals are following suit. PAGE 42

Mieke Eoyang on how the emergence of 5G technology could disrupt intellectual property protection. PAGE 48

“If the network owner is not a country that shares our values, what happens to the communications that flow across it?”

“Every president wants to take his own approach. But until new programs are set up, there are no protections in place.”

Roberto Atilano, CPP, on the security crisis in Mexico as a new administration gets up to speed. PAGE 24

Security professionals are following suit. PAGE 42
A world of vital security news delivered to your inbox.

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

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

Check out the *Security Management* newsletters’ new features and design. To subscribe or resubscribe, e-mail ASIS International: [asis@asisonline.org](mailto:asis@asisonline.org).
MAY 2019

36
STARTING FROM SCRATCH
Land O’Lakes, Inc., hired a security leader to build a program from the ground up. Here’s how he did it.
By Don Taussig, CPP

MANAGING SECURITY & THE GIG ECONOMY
The project-based economy is on the rise. Global consultant Marko Cabric explains the ramifications for the security industry.
By Mark Tarallo

42
SUPPLY CHAIN
SIFTING THROUGH THE SUPPLY CHAIN
A public-private partnership brings together industry and U.S. government officials to address supply chain security and prevent nation-state attacks.
By Megan Gates

46
A DAY IN THE LIFE
ELIZABETH MOSLANDER, CPP
An ASIS leader, devoted parent, and Super Team tennis player details the typical day of a manager of physical security operations at Capital One.
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.
Developing new terminology for new endeavors.

Security and police departments weigh the benefits and drawbacks of body-worn cameras.

By Mark Tarallo

A global manufacturing firm unified its endpoint protection across disparate and legacy devices.

By Lilly Chapa

The first major GDPR fine highlights consent and transparency about users’ data.

By Megan Gates

Employers may be liable for not effectively addressing rumors in the workplace.

By Sara Mosqueda

A new Mexican President Obrador shifted his focus on crime in 2018, the country saw its murder rate climb.

By Lilly Chapa

General John F. Kelly (USMC, ret.) will keynote GSX 2019 in Chicago.

By Sara Mosqueda

ASIS NEWS

ASIS BOARD OF DIRECTORS

LEGAL REPORT

INDUSTRY NEWS

ADVERTISER INDEX

GETTING TO KNOW

Jaime P. Owens, CPP

CHECK OUT MORE ONLINE at www.securitymanagement.com
Don Taussig, CPP, provides executive leadership for enterprisewide security and corporate travel functions for Land O’Lakes. He also serves on the ASIS CSO Center Advisory Board and the Domestic Security Alliance Council Governance Committee.

Taussig was appointed by President George W. Bush as director of security for the Executive Office of the President. He served the U.S. Army as a special agent in charge for executive protection for the Commander of NATO, as a CSO with the U.S. Bureau of Reclamation, as a security officer with Diplomatic Security at U.S. Department of State, and as a leader with the National Disaster Response Team.

“Starting from Scratch”

PAGE 36

David Thompson is responsible for strategic planning and the evolution of interview and interrogation content. He has managed a variety of cases and consulted on investigations ranging from theft and fraud to sexual harassment and homicide. As an instructor, Thompson has created many customized training programs.

At Wicklander-Zulawski, Thompson plays an integral role in the ongoing research and evolution of content and innovative teaching methods. He also worked with members of the Innocence Project, the Center on Wrongful Conviction of Youth, and other academic partners to further the enhancement of interview and interrogation protocols.

Book review

PAGE 17

Adrian Barnie, CPP, is a senior contract investigator at the U.S. Attorney’s Office in the Northern District of Ohio, where he works with the Financial Litigation Unit on asset recovery. Prior experience includes investigating money laundering and terrorist financing at a bank, corporate special investigations at an insurance company, and management positions with a private security agency.

Barnie has been a member of ASIS for more than 40 years and has written more than 30 book reviews for Security Management. Prior to his investigative career, he worked on archaeological excavations in the American southwest and in rural England. Barnie also taught at Case-Western Reserve University.

Book review

PAGE 33

Paul Barnard, CPP, has more than 40 years of government and corporate security experience. He served as the Command Security Officer for the U.S. Army TACOM LCMC and had oversight on numerous security programs. He is a Certified Information Security Manager (CISM) and has maintained his CPP certification for more than 35 years.

Barnard is an adjunct associate professor for Madonna University in the Criminal Justice and Emergency Management degree programs, and adjunct professor for Macomb Community College in the Public Service Institute. He volunteers as an expert-in-residence for the Macomb-Oakland University Incubator for Government & Homeland Security.

Book review

PAGE 64
AMICOGUARD - 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
amicosecurity@gibraltar1.com • amicosecurity.com
See Our Entire Line of Security Fences on Display in Birmingham, AL - Installation Training Available

For product info #5 securitymgmt.hotims.com
BODY CAMERAS
More than 80 percent of U.S. police agencies are either using body cams now or have plans to do so in the near future, according to a survey by the Police Executive Research Forum.

911 TECHNOLOGY
A new white paper explores how 911 communication centers can navigate Next Generation 911 technologies and the FirstNet public safety broadband network.

IT SUPPLY CHAIN
The U.S. Government Accountability Office assessed supply chains that U.S. federal agencies use to procure IT systems.

AGING INFRASTRUCTURE
The vast, aging U.S. Coast Guard infrastructure includes piers, docks, and other facilities. The Coast Guard estimates that its backlog of improvement projects would take $1.7 billion and nearly 400 years to address.

MEXICO
After a few years of declining murder rates, cartels in Mexico are locked in bloody turf wars, contributing to a dramatic rise in murders in 2017, according to a report from Stratfor.

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

TRENDING ARTICLES

1. PHYSICAL SECURITY
Partnerships and Potential in Chicago
By Lilly Chapa

2. CYBERSECURITY
When the Money’s Gone
By Megan Gates

3. PHYSICAL SECURITY
Should You Be Watching?
By Eddie Sorrells, CPP, PCI, PSP, and Bradley Gordon

"Focus on influencing. Because oftentimes what we’re doing, especially in the CSO role, is we are leading leaders.” Joe Olivarez, VP, global security for Jacobs Engineering, discusses leadership and career paths with host Chuck Harold in a special SM Podcast.

Get totally complete security under one roof.

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

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

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

For product info #6 securitymgmt.hotims.com
The mid-1200s, gentleman hunters in France developed a specialized vocabulary to describe groups of animals both mundane and exotic. These words, called "terms of venery" or "nouns of assembly," live on today in a "murder of crows," a "brood of hens," and a "shiver of sharks."

In a recent article, media company Quartz explored these phrases, noting that they were most likely devised as ways to show off snazzy vocabulary rather than as serious attempts to categorize. However, the name game proved to be popular. In time, nouns of assembly moved beyond animals and were applied to inanimate objects and people. They also became more exaggerated. Quartz makes special note of a "diligence of messengers," a "blast of hunters," a "subtlety of sergeants," an "execution of officers," and a "superfluity of nuns."

But not all of the terms are frivolous. Quartz notes that a "flight of stairs" is such common parlance that we rarely question the term. As a means to ascend to a higher level, climbing a flight of stairs makes sense. "And, of course, the platform at the top of the stairs or between two sets of stairs is often called a landing—because that's what you do after taking a flight," according to the article.

Playful or not, new categories can be helpful in organizing a fresh venture. For example, in this month's cover story, "Starting from Scratch," Don Taussig, CPP, found that building a security program for Land O'Lakes from the ground up required naming several types of groups. Taussig gathered lists of internal business partners, including HR, legal, real estate, and facilities. He compiled groups of duties and assembled a variety of guiding principles (page 40) to lead his new department.

New endeavors are also underway at Security Management as ASIS International adds two staff members to the masthead, Managing Editor Claire Meyer and Assistant Editor Sara Mosqueda. Meyer—who comes to ASIS from Security magazine—brings a deep knowledge of the security industry, as well as strong writing, editing, and project management skills. Mosqueda, formerly with S&P Global Market Intelligence, contributes her comfort with technical material and her copyediting and writing skills to help us move forward as we expand our content efforts.

Changes are afoot for existing Security Management staffers as well. Mark Tarallo takes on a larger role in managing projects in support of our content strategy. Megan Gates is the editor-in-chief of our new supplement, Security Technology. Flora Szatkowski will lend her considerable talents to our renewed book publishing efforts.

As Taussig notes of his new program, "When scarce resources are allocated, security has a seat at the table alongside other business functions. This type of feedback demonstrates that the function is adding value to the company."

Whether applied to a security program or a publishing group, the concept of adding value through strategy and business development deserves its own set of terms: an "excellence of influencers," a "whirlwind of changemakers," or perhaps an "influx of innovators."
NO MATTER THE WEATHER OR POWER, WE MAKE IT SECURE.

IMAGINE THAT.

OUTDOOR LATCH RETRACTION

Our solution lasts through the harshest conditions and stays locked from the pull side when power is lost. Assured security when electricity is far from a sure thing—that’s the Detex effect.

DETEX.COM/LATCH4 · 800.729.3839

For product info #7 securitymgmt.hotims.com
CAMERA COMPLICATIONS

MIXED RESULTS AND CLIMBING COSTS PROVE TO BE ONGOING CHALLENGES FOR POLICE AND SECURITY DEPARTMENTS DEPLOYING BODY-WORN CAMERAS

BY MARK TARALLO

USE OF BODY-WORN CAMERAS, or body cams, by police departments continues to trend up. According to a survey released in August 2018 by the Police Executive Research Forum, more than 80 percent of U.S. police agencies are either using body cams now or have plans to do so in the near future. More than 85 percent of the departments that currently use body cams would recommend them to others.

“Body-worn cameras can demonstrate that a police agency is willing to be transparent and accountable for its actions. The conceptual appeal of body-worn cameras has led to rapid adoption of the technology in police agencies across the country,” the report found.

Other developments have helped drive this swift adoption. In late 2014, the Obama administration proposed the $263 million Body-Worn Camera Partnership Program, a federally funded body-camera advocacy initiative for states and localities. The program was later approved.

Around the same time, the police department in Rialto, California, participated in an influential study, *Self-Awareness to Being Watched and Socially-Desirable Behavior: A Field Experiment on the Effect of Body-Worn Cameras on Police Use-of-Force*. The study found that, during a year-long trial period of body cam use, public complaints against officers fell 88 percent compared with the previous 12 months.

But lately, there have been a few reality checks. In 2017, Washington, D.C., officials released the surprising results of their own randomized controlled trial of body cam use by the city’s police department. The study found that body cam use had no detectable effects on police discretion, as measured by arrests for disorderly conduct. And the D.C. study featured more than 2,000 police officers, compared to 54 in the Rialto experiment.

“These results suggest we should recalibrate our expectations” that body cams will cause a large-scale behavioral change in policing, particularly in contexts similar to Washington, D.C., the study explained.

Another challenge is cost. Video storage can be expensive, especially when volume is high. These cost factors have recently caused some police departments to drop, or consider dropping, their body cam programs, according to recent media reports.

For example, in February, Unified Police Department officers in Salt Lake County, Utah, said their agency may discontinue use of body cams, partly due to the high costs for digital video storage. Previously, the department had outfitted 125 of its 410 officers with body cams, using funding from a grant that expires this year. But supplying all officers would cost more than $400,000 per year, according to the agency.

Cost can also be an issue for smaller departments, such as the one in East Dundee, a village suburb of Chicago. The police department there had previously ordered body cameras for its 17 police officers. Before they could be put to use, a new police chief persuaded local officials to cancel the program. The chief argued that the $20,000 annual fee for the cameras...
and video storage couldn’t be justified as a budget expense.

Still, while not every police department is jumping on the body cam bandwagon, others have expressed great satisfaction with their programs. Jeff Karpovich, CPP, the chief of security and director of transportation at High Point University in High Point, North Carolina, has found that his security force’s use of body cameras—called “chest cams” because of where they are worn on the uniform—has been a big help, for several reasons.

One is that they have increased accountability. “Our officers are as human as anyone else out there, and some may have the inclination to say things and do things that they probably shouldn’t do if nobody is looking,” says Karpovich, who is a member of ASIS International. But an active chest cam acts as a “digital supervisor,” nudging officers to comply with all rules and regulations.

Another reason is that chest-cam video frequently serves as a means of exoneration in response to complaints lodged against officers. “It proves to others what they were supposed to do,” he explains. “It has exonerated them time and time again.”

Furthermore, chest-cam video has great value as evidence. “If a picture is worth a thousand words, video is worth a million words,” Karpovich says. However, this value comes with a responsibility: video must be produced when it is needed, so technical glitches are costly. Citizens understand if a scuffle between an officer and a civilian leads to unwatchable or unusable video, Karpovich explains. But if an incident that should have been recorded was not recorded, or if there is an unexplained gap during crucial moments in a video, citizens become suspicious. “The absence of chest-cam video reeks of coverup,” Karpovich says. “If we have a program like this, we had best have it working properly.”

High Point’s security force follows rules set out in its standard operating procedure (SOP), but since it is not a police department, it is not covered by the growing types of state regulations that are now being formulated regarding public access to body cam video. In 2018, lawmakers introduced legislation in 36 states and D.C. aimed at creating statewide rules governing the use of body cameras, according to a recent Washington Post report. Often, these efforts are driven by an effort to increase transparency.

For example, in February, a New York appellate court determined that the public has the right to view footage from body cameras. The ruling rejected an argument made by the Patrolmen’s Benevolent Association, the New York City police union, that public access to video should be blocked under a state law that requires police personnel records to be kept secret.

At High Point, Karpovich says the chest cam program developed into a successful and beneficial enterprise. Although video is not kept forever, it is stored for a limited amount of time in case relevant complaints are made, making costs manageable. Also, certain safeguards prevent video from being released on YouTube or social media, such as password protections that greatly limit the number of people in-house who can access video.

“I don’t see anything derailing this,” he says of the camera program. “It’s a proven tool.”

**WHY THEY DO IT**

**BY EUGENE SOLTES. Public Affairs; publicaffairsbooks.com; 464 pages; $18.99.**

**THE CRIMINAL MIND** is a fascinating and popular topic of exploration and study, especially in “serious” cases such as homicide, sexual violence, and terrorism. Often overlooked are white-collar criminals and the questions of how and why they perpetrate corporate fraud and multimillion-dollar crime schemes.

In the book, *Why They Do It: Inside the Mind of a White-Collar Criminal*, author Eugene Soltes does an excellent job giving the reader contextual knowledge of white-collar crime, including historical evolutions of the investigative and legal frameworks that surround it. The content applies to a wide variety of investigative professionals, students of criminal justice, and anyone operating a business. For those interested in learning about the progress of litigation and prosecution surrounding corporate fraud, this book provides specific examples and a chronological flow of the escalation of these crimes.

As the author tells the story of how white-collar crimes became more prevalent and the shift in feeling protected as a wealthy business owner to becoming vulnerable, he provides historical examples of this progression. He leads the reader through multiple cases, going beyond just the case facts. Readers will come to understand how the crime was initiated, the rationalization process in the criminal mind, and the consequences of these actions.

This knowledge can help in creating better business procedures to minimize the opportunities for crime, as well as in understanding red flags and indicators of fraud. The other perspective that is extremely helpful for practitioners is understanding the thought process and justification of a white-collar criminal. This provides an ideal roadmap for showing empathy and understanding when interviewing someone accused of these crimes.

The book delivers on its promise, providing readers an inside look into “why they do it.” Practitioners, students, and instructors will find value in this book, especially in understanding the full scope of how these crimes develop from the offender’s perspective.

**REVIEWER:** Dave Thompson, CFI (Certified Forensic Interviewer), is vice president of operations for Wicklander-Zulawski & Associates. His responsibilities include the development of interview and interrogation content and instructing these methodologies globally to both the private and public sectors.
The vast coastline infrastructure administered by the U.S. Coast Guard, which includes piers, docks, and many mission-critical facilities, is in dire need of repair. But it may take a bit of time to complete the improvements—roughly 395 years if current funding levels stay the same, according to the U.S. Government Accountability Office (GAO).

This repair time frame of nearly four centuries reflects the extensive nature of the Coast Guard’s holdings. The agency owns or leases more than 20,000 shore facilities, including boat stations and housing units, at more than 2,700 locations. The replacement value of these facilities is approximately $20 billion.

The GAO was asked to review the agency’s management of its infrastructure. In its report, the GAO found that nearly half (45 percent) of the Coast Guard’s shore infrastructure is beyond its service life, and as of 2018, it had a backlog of maintenance and recapitalization projects that would cost at least $2.6 billion to address.

This deferred maintenance backlog includes more than 5,600 projects, and these deteriorating facilities hinder the Coast Guard’s ability to secure the coastlines. “While the Coast Guard has a culture of ‘making do’ with the resources it has, these backlogs pose financial, safety, and mission performance risks,” the report found.

And wait, there’s more: the Coast Guard said there are 205 other backlogged projects that do not yet have cost estimates.

How can the Coast Guard improve its infrastructure, and reduce the security risks? The GAO made several recommendations in the report.

The GAO recommended that program managers develop standards to assess facilities, including milestones and time frames. The program managers should also establish shore infrastructure performance goals, measures, and baselines, so that the Coast Guard can track the effectiveness of maintenance and repair investments and provide feedback on progress.

The GAO also recommended that the Commandant of the Coast Guard should work with Congress to develop a process that would periodically align the agency’s shore infrastructure portfolio with mission needs. Afterward, the agency could plan on disposing of all unneeded assets.

Finally, the GAO recommended that the Coast Guard use models that could predict the outcomes of investments in its assets and analyze trade-offs, so that the best decisions among competing investments could be made.
Video Surveillance, Transformed

The upcoming release of Avigilon Control Center (ACC) 7, our latest and most advanced version of ACC™ video management software, is designed to revolutionize how users interact with and gain situational awareness from their video surveillance systems.

Focus of Attention Interface
Introducing Focus of Attention — a cutting-edge user interface for live video monitoring that leverages AI and video analytics technologies to determine what information is important and should be presented to security operators.

AI-Powered Analytics
Using our deep learning video analytics and Unusual Motion Detection technologies, ACC 7 software is designed to provide customers with actionable information to help ensure critical events don’t go unnoticed.

Dark Mode
ACC 7 software introduces a new theme with colors specifically chosen to reduce eye strain and improve user experience in dark environments, such as video surveillance control rooms.

avigilon.com/acc7  |  asksales@avigilon.com
A SIX-YEAR RESET

MEXICO SAW ITS HIGHEST MURDER RATE EVER IN 2018. CORPORATE SECURITY IS NOW ON HIGH ALERT AS CARTELS DIVERSIFY AND THE NEW PRESIDENT ESTABLISHES A NATIONAL SECURITY STRATEGY.

BY LILLY CHAPA

2018 MARKED A YEAR of symbolic change for Mexico. The country elected a new leftist president, Andrés Manuel López Obrador, who won by a landslide in July and assumed office in December, promising a new approach to addressing violence and corruption.

In November the United States–Mexico–Canada Agreement was signed, which will replace the North American Free Trade Agreement (NAFTA) if approved by the countries’ governments and will increase trade and improve working conditions, especially for women and migrant workers. The trial of infamous Mexican drug lord Joaquín “El Chapo” Guzmán kicked off in the United States, highlighting the flow of drugs through Mexico and the broken systems that allow cartels to flourish. And high-profile migrant caravans, along with ongoing rhetoric about security along the U.S.–Mexico border, shone a light on the flow of people between countries.

Not all of last year’s changes were symbolic, though. Murders in Mexico rose by 33 percent in 2018—authorities opened 33,341 murder investigations, the highest number ever. That statistic from the Interior Ministry is accompanied by other sobering trends: a 19 percent increase in cargo theft throughout the country, and a similar increase in kidnappings. Oil and gas theft continues to be an issue as well, as evidenced by the January explosion caused by an illegally tapped gas pipeline north of Mexico City that killed at least 85 people. And El Chapo’s recent conviction on 10 counts of drug trafficking and money laundering serves as a reminder that Mexico’s drug cartels are continuing to evolve and operate without conventional leaders, groups, or regions.

All of these changes have led to precarious times for corporate security in Mexico, says Roberto Atilano, CPP, the Mexico and Central America corporate security manager for consumer goods company Ferrero. “I have seen more kidnappings of businessmen in the past few months than over the past few years,” Atilano tells Security Management.

“And they are happening in areas where it’s normally not an issue.”

A reset in Mexico’s federal security programs, as well as the ongoing fracturing of cartels, has led to an increase in localized crime. And according to Atilano and other experts, the recent rise in murder rates, kidnappings, and cargo theft is not going to stop any time soon.

Cartels. When geopolitical intelligence platform Stratfor started documenting Mexican drug cartel trends in 2006, the dynamics were simpler—there were only a handful of cartels, each operating in its own region and under an established hierarchy. But following a sharp increase in cartel-fueled murders from 2010 to 2012 and the subsequent military crackdown, the groups began fragmenting, both due to pressure from the outside and competing factions inside the organizations. After a few years of declining murder rates, the splintered cartels have regrouped and are locked in bloody turf wars, contributing to the dramatic rise in murders in 2017 and continuing today, Stratfor reports.
While the Sinaloa cartel has suffered the loss of its leader El Chapo—as well as the airing of its drug-smuggling logistics during his trial—the group continues its dominance of northwestern Mexico and remains one of the last legacy cartel groups with clout. In central Mexico, the Cartel de Jalisco Nueva Generacion—a splinter of Sinaloa—has emerged as the country’s most violent drug-smuggling group.

“Its efforts to expand its area of control are largely responsible for the persistent wave of violence racking Tijuana, Juarez, Guanajuato, and Mexico City,” the Stratfor report notes.

Ongoing cartel infighting and the government’s attempts to control the drug trade have brought violence into areas that have long been considered safe. “Most of the violence has been cartel-on-cartel or government-on-cartel, but with the cartels using automatic weapons and military ordnance, such as grenades and anti-tank weapons, bystanders are at considerable risk of injury or death,” according to Stratfor.

Cartels are also diversifying their operations. While Mexican drug operations of the past have focused on pushing heroin and cocaine, the rise in popularity of synthetic drugs in the United States is a boon for cartels—the profit margin on manufacturing methamphetamine and fentanyl is much higher than peddling traditional drugs. Splintered cartels are also turning to non-narcotics operations for funding, accounting for the rise in kidnapping and cargo theft.

“It is no coincidence that the pilfering of cargo and fuel have reached historically high levels as balkanization blossomed over the past half-decade,” Stratfor notes.

**A new administration.** These trends in cartel violence may be exacerbated by the vacuum that the change in federal leadership creates every six years. Atilano points out that with a new administration come new security policies and approaches, but until those are established there is no one method to combat the growing numbers of murders, kidnappings, and cargo theft.

Indeed, advocates have been calling for the reinstatement of a national plan...
UNDERSTAND THE RISKS,
MINIMIZE THE DISRUPTIONS
Managing a globally distributed supply chain is no easy task, especially with rising threats from both natural disasters and human conflict. Confronted with increasingly complex supply chains, tighter production windows, and limited supply reserves, the stakes have never been higher for businesses. Given the sheer scale and risk exposure of most manufacturers, risk managers often jump from one crisis to another—never truly getting ahead of the threats. Recently, a senior supply chain risk manager for a global automotive manufacturer took a wiser approach. He discovered that to proactively mitigate against costly disruptions, businesses need to holistically understand the multitude of threats throughout their production cycles.

A series of devastating storms had forced the automotive manufacturer to halt production in a highly competitive market. Realizing that a single day without production could result in losing millions of dollars in potential earnings, the company knew it needed a way to better forecast the impact of emerging events and implement countermeasures. The risk manager, tasked with enhancing the company’s resiliency, set off to holistically analyze the risk of each facility in the end-to-end supply network, down to tertiary suppliers.

The risk manager quickly discovered that the greatest challenge was finding a way to intuitively visualize the complexity of the supply network, given the sheer number of parts and production facilities involved in creating a finished product. “[Every] vehicle has hundreds of thousands of unique parts that are sourced from global suppliers operating on nearly every continent,” he says. “It doesn’t matter if production is halted because of a hurricane or because a subtier supplier went out of business—the effects are the same.”

“We needed a way for us to avoid costs associated with disruptive events in the supply chain,” the manager continues. “We’ve been in a position where even an hour’s worth of downtime at a production facility can have a significant impact on schedule.” Utilizing a “single-pane-of-glass” approach, the risk manager leveraged Esri technology for location intelligence to visualize the location of the company’s key suppliers, monitor emerging threats in near real time to quickly forecast their potential impact, and better communicate the manufacturer’s overall risk to decision-makers.

Through the use of location intelligence, the risk manager was able to effectively streamline the manufacturer’s response efforts at a crucial, early moment and reduce the overall cost of an event. The manager says, “With Esri, we’ve reduced the amount of time on two key metrics when it comes to crisis management: the speed of discovery of an event that has the potential to affect our supply, [and] the speed of understanding the impact.” This framework has empowered him and his company’s other executives with mission-critical insights to better reroute, reallocate, and reschedule production plans to minimize downtime during crises.

To learn how location intelligence can empower your corporate security and business resilience teams to mitigate threats, visit esri.com/ASIS.
to combat kidnapping—there is currently no strategy because the last plan expired at the end of December. According to Mexican kidnapping prevention advocacy group Alto el Secuestro, at least 317 people were kidnapped within the first two months of Obrador’s presidency, representing a 51.6 percent increase from last year’s rates.

“Every president wants to take his own approach. But until new programs are set up, there are no protections in place,” Atilano says.

The differing approaches to violence and corruption in Mexico are evident when comparing confiscation of drugs and weapons under previous administrations. Under President Felipe Calderon, who served from 2007 until 2012 and was known for his ruthless pursuit of cartels using the national military and intelligence arms, more than 163,000 weapons were confiscated from criminal organizations. When President Enrique Pena Nieto became president at the end of 2012, he focused more on reducing violence by establishing a National Gendarmerie instead of attacking the country’s cartels with military might. During his six-year term, some 46,500 weapons were confiscated. The number of drug-related arrests and confiscations dropped in a similar manner.

Obrador is expected to employ his own unique approach to the cartel violence. He campaigned to continue the demilitarization of law enforcement—undoing the controversial tactics Calderon used to combat the drug war—and instead address the social issues that cause the violence. However, two months into his governance, Obrador has proposed the creation of a new 60,000-person Mexican National Guard that would replace current armed forces fighting the cartels.

Regardless of the president’s approach, it will be some months before a National Guard or other security measures are enacted, and Atilano says it’s important for corporate security leaders to foster the continuity of security best practices within their organizations and communities.

“We have been dealing with a lot of cargo theft, where criminals will steal or hijack our goods in transit,” Atilano says. “We were able to address it with armed escorts. We didn’t want to address fighting with fighting, but it was the best approach and now our cargo theft is down to zero.”

Atilano says he is emphasizing corporate security training to address the crime that has crept up following Obrador’s inauguration.

“For corporate security, we’re working on our awareness programs; I’ve stepped them up over the past few months,” he says. “We are increasing our executive protection and kidnapping training.”

Atilano says he has been through this before—until a new national security approach is established, corporate security leaders have to fill the gap the best they can. The consequences of this trend were made clear in a recent report from Mexico’s Sistema Nacional de Seguridad Pública—between December 2018 and January 2019, the rate of kidnappings, extortion cases, and robberies all rose. The report also found that during this past January alone, 2,452 people were murdered, making it the deadliest January since the organization began collecting data in 1997.

“The statistics show that crime is getting worse over the past few months,” Atilano says. “I don’t think that’s going to change any time soon, until the new administration puts new security programs in place and they start working. Until then, we just have to enforce security best practices.”

**IMMIGRATION AND CRIME**

Individuals from European countries were polled about whether immigrants are causing crime in their country. Below is the percentage of respondents who believe immigrants are more culpable for crime than other groups.

<table>
<thead>
<tr>
<th>Country</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>France</td>
<td>22%</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>22%</td>
</tr>
<tr>
<td>Poland</td>
<td>23%</td>
</tr>
<tr>
<td>Spain</td>
<td>29%</td>
</tr>
<tr>
<td>Hungary</td>
<td>33%</td>
</tr>
<tr>
<td>The Netherlands</td>
<td>42%</td>
</tr>
<tr>
<td>Italy</td>
<td>44%</td>
</tr>
<tr>
<td>Germany</td>
<td>52%</td>
</tr>
<tr>
<td>Sweden</td>
<td>55%</td>
</tr>
<tr>
<td>Greece</td>
<td>59%</td>
</tr>
</tbody>
</table>

**SOURCE:** Around the World, More Say Immigrants Are a Strength Than a Burden; Pew Research Center, March 2019

@To read the Stratfor cartel report, visit SM Online.
THE SECURITY OF IP BASED CONTROL & COMMUNICATION

HUBBCOM™ IP DEVICES

Tomorrow’s technology for today’s connected world.

- ALARMS
- DOOR/GATE ACCESS
- VIDEO MONITORING

www.GAI-TRONICS.com  1-800-492-1212

For product info #12 securitymgmt.hotims.com
Time to up your selfie game

AND WIN BIG!

Take a selfie showing you with the back side of the postcard attached to the next page. Post it on Facebook, Twitter, LinkedIn, or Instagram using the hashtag “#GSX19Contest” no later than 16 August and be entered into a drawing to win a $100 gift card to Rosebuds Restaurant in Chicago.

Card not attached? Visit GSX.org/selfie to download a version you can use.

Early-bird rates end on 14 June.

REGISTER TODAY AND SAVE >> GSX.org/selfie

ENHANCE YOUR CAREER STATUS AND EARNINGS

GSX pre-conference programs help you prepare for the prestigious ASIS International certification exams. Already certified? GSX is the best place to earn CPE credits to help you maintain your APP, CPP, PCI, and PSP credentials.
Xperience Something

XTRAORDINARY

Join 20,000 registered attendees from 110+ countries to:

**LEARN**

300+ sessions and dozens of security topics compose an immersive and interactive learning environment, offering insights and best practices to security professionals at every stage in their career.

**NETWORK**

The Opening Night Celebration—Chicago on the Silver Screen, ASIS Happy Hour, and the President’s Reception—the can’t miss event of GSX 2019—allow you to relax, sit back, and get to know other attendees and exhibitors.

**XPLORE**

Engage with 550+ exhibitors and experience 1000s of emerging technology solutions—all part of an interactive learning lab. Multiple learning stages; the D3 Xperience: Drones, Droids, Defense; and the Career HQ and headshot studio are designed to offer the security practitioner something unique.

**SPECIAL 11 SEPTEMBER KEYNOTE**


*Free one day pass for military, law enforcement professionals, and first responders. Use the promo code THANKS when registering.

GSX

GLOBAL SECURITY EXCHANGE

FORMERLY ASIS ANNUAL SEMINAR & EXHIBITS

8-12 SEPTEMBER 2019

McCORMICK PLACE | CHICAGO, IL

GSX.ORG  |  #GSX19
Each acquisition and location brought with it a new—and separate—antivirus solution for that facility’s network. And when Zack Moody, CISSP®, joined AVX as information security manager two years ago, he was tasked with facilitating a singular network security approach that could protect the organization’s 29 facilities in 16 countries.

“The job was much larger than AVX knew, but this was an opportunity I was willing to accept,” Moody says. “I wanted to create a program from scratch.”

Through his experience in both the private and public sectors, Moody says he knew there were many ways to approach the challenge at hand—either through a compliance or risk perspective.

“It was hard—there’s lots of noise from the compliance standpoint, but there was also a lot of risk to take into consideration,” Moody explains. “How do you find that balance? A good security professional is going to understand that as long as you’re implementing security correctly, compliance falls into place. It took a long time to figure out the business side, because AVX is such a massive organization and spread throughout the world.”

The first thing Moody did in the decision-making process was conduct a global security assessment to identify the biggest risks and gaps.

“For me, when I looked at what was the biggest risk, endpoints obviously came to mind,” he explains. “One way attackers enter your organization is typically with malware, so how does it get in? It’s either through a USB or email. And if it gets onto the machine, that’s where it’s going to execute from, so we have to strengthen that.”

The security assessment revealed that AVX’s facilities were running five or six different antivirus solutions worldwide. Moody says he knew that finding one effective solution that would stop malware execution at the endpoint was imperative for AVX’s systems.

“Throughout AVX facilities there were different price ranges, even with the same vendor, because people purchased things separately from the next facility,” Moody explains. “There was no central view into the influence, no central control—and if a fix or change needed to be pushed out, you’re not just pushing one patch, it was one patch to this vendor, one patch to another vendor.”

In Moody’s search for a standardized solution, he focused on the need for endpoint protection, detection, and response capabilities, which would provide multiple ways to handle malware threats. He also looked for something that would allow him to manage the system from one platform and provide the tools needed to actively detect threats.

AVX found its solution in SentinelOne’s Endpoint Protection A GLOBAL MANUFACTURER UNIFIES ITS ENDPOINT PROTECTION, DETECTION, AND RESPONSE INTO ONE PLATFORM TO MITIGATE CYBER RISK IN DISPARATE LEGACY SYSTEMS. BY LILLY CHAPA

AVX CORPORATION MANUFACTURES and supplies sensors, antennas, and other electronic components that make up phones, computers, medical devices, and more. For many years, the firm faced various company acquisitions, managed multiple facilities, and used numerous security systems.
It's going to pick up on older endpoint solutions. Moody puts it, “some of the oldest known to man” and don’t work well with newer systems, so when we turn on the detect mode, there are fewer false positives.

Moody says he was also impressed by SentinelOne’s reliance on its customer base, which often informs what new features are developed—in fact, AVX played a part in SentinelOne’s development of its firewall and USB controls, he notes.

Implementation of the platform was seamless, Moody explains, and AVX ran the program in detect-only mode for the first two weeks so AVX could teach it what programs or actions to whitelist—including the legacy antivirus software that facilities had in place.

“During that period, we could see what they were identifying as good, bad, and ugly, and had the opportunity to compare it to what rules are currently in place with the existing antivirus systems the site was using,” Moody explains. “We could start whitelisting those known systems, so when we turn on the detect mode, there are fewer false positives.”

One challenge AVX faced was one many manufacturers are familiar with—the computers, programs, and code used in manufacturing are, as Moody puts it, “some of the oldest known to man” and don’t work well with newer endpoint solutions.

“Throwing SentinelOne on these systems, it’s going to pick up on older applications that may not be digitally signed or seem to appear malicious, but in reality are old applications that we’ve been using for years,” Moody says. “You can whitelist an application, but the good thing about SentinelOne is it will pick up on any strange activity that an application does, even though it’s whitelisted. It can still get blocked if it starts changing files or does something malicious.”

AVX implemented SentinelOne’s solution in June 2018, and the process took about six months because of the number of disparate and isolated systems throughout the organization, Moody explains.

But now that it’s up and running, it has streamlined the malware detection and response process. Previously, if an AVX employee encountered a potential malware issue with his or her computer, he or she would report it to the company’s IT department, which would investigate and run scans—often with the same software that didn’t detect the malware in the first place, Moody notes. Depending on the results of the scan, it would reimage the computer and inform the security department of the potential breach. With the SentinelOne solution, security is the first to address a potential hack.

“There was a lot of wasted time with the legacy products,” Moody says. “So why not invest in tools that were going to be more proactive on the security side? They give the security team reach into those endpoints and free up our IT professionals. We need to be in control of what’s on our network and what’s happening. Business continues to go on, people can continue to work—the majority of the time, SentinelOne is taking care of things in the background and blocking what it needs to be blocking. But if something happens, we’ll be notified immediately, and we’ll have all the tools to react.”

Moody says that he is pleased with SentinelOne’s innovative approach to detecting and responding to malware. “We wanted to get away from the traditional signature-based detection systems and go towards something more proactive to these threats,” he says. “It’s very important, especially in manufacturing where there’s so much machine code that is old or might change a lot. You have to make that decision—do I trust a company that built their entire organization off legacy antivirus, or a company that is fresh and inventive in today’s world and threat landscape? When I take a step back, we want someone who is going to be with us for the next 40 to 50 years and has a vision of threats today and beyond. I want someone new in the game, and for us, that was SentinelOne.”

“SentinelOne provides the capability of rolling back the operating system in case there is a ransomware system on a computer,” Moody notes. “There’s the argument that you shouldn’t have to have that, but for me it’s better to have, because you never know.”


“The good thing about SentinelOne is it will pick up on any strange activity that an application does, even though it’s whitelisted. It can still get blocked if it starts changing files or does something malicious.”

AVX implemented SentinelOne’s solution in June 2018, and the process took about six months because of the number of disparate and isolated systems throughout the organization, Moody explains.

But now that it’s up and running, it has streamlined the malware detection and response process. Previously, if an AVX employee encountered a potential malware issue with his or her computer, he or she would report it to the company’s IT department, which would investigate and run scans—often with the same software that didn’t detect the malware in the first place, Moody notes. Depending on the results of the scan, it would reimage the computer and inform the security department of the potential breach. With the SentinelOne solution, security is the first to address a potential hack.

“There was a lot of wasted time with the legacy products,” Moody says. “So why not invest in tools that were going to be more proactive on the security side? They give the security team reach into those endpoints and free up our IT professionals. We need to be in control of what’s on our network and what’s happening. Business continues to go on, people can continue to work—the majority of the time, SentinelOne is taking care of things in the background and blocking what it needs to be blocking. But if something happens, we’ll be notified immediately, and we’ll have all the tools to react.”

Moody says that he is pleased with SentinelOne’s innovative approach to detecting and responding to malware. “We wanted to get away from the traditional signature-based detection systems and go towards something more proactive to these threats,” he says. “It’s very important, especially in manufacturing where there’s so much machine code that is old or might change a lot. You have to make that decision—do I trust a company that built their entire organization off legacy antivirus, or a company that is fresh and inventive in today’s world and threat landscape? When I take a step back, we want someone who is going to be with us for the next 40 to 50 years and has a vision of threats today and beyond. I want someone new in the game, and for us, that was SentinelOne.”

SentinelOne’s innovative approach to security is the first to address a potential threat. Moody says he is pleased with SentinelOne’s innovative approach to detecting and responding to malware. “We wanted to get away from the traditional signature-based detection systems and go towards something more proactive to these threats,” he says. “It’s very important, especially in manufacturing where there’s so much machine code that is old or might change a lot. You have to make that decision—do I trust a company that built their entire organization off legacy antivirus, or a company that is fresh and inventive in today’s world and threat landscape? When I take a step back, we want someone who is going to be with us for the next 40 to 50 years and has a vision of threats today and beyond. I want someone new in the game, and for us, that was SentinelOne.”

“For more information: Daniel Bernard, Vice President, Business and Corporate Development, SentinelOne, DB@sentinelone.com, 816.668.3472.

“For more information: Daniel Bernard, Vice President, Business and Corporate Development, SentinelOne, DB@sentinelone.com, 816.668.3472.

“This is a wonderful initiative. There’s now no distance between ASIS members.”

McLean Essiene, CPP, PCI, PSP
MD/CEO Essimacs International Security LTD

Join the conversation
community.asisonline.org
Despite the measures implemented by Google, the infringements observed deprive the users of essential guarantees regarding processing operations that can reveal important parts of their private life since they are based on a huge amount of data, a wide variety of services, and almost unlimited possible combinations,” CNIL said in a press release. The commission added that the violations are “continuous breaches of the regulation as they are still observed to date. It is not a one-off, time-limited infringement.”

Two associations—None Of Your Business and La Quadrature du Net—filed complaints with CNIL in May 2018. They claimed Google did not have a valid legal basis under the GDPR to process users’ personal data for ad personalization purposes.

CNIL then began investigating Google and found that when users created Google accounts using Android smartphones, the tech company’s practices violated the GDPR in two ways: transparency and legal basis for ads personalization processing.

CNIL’s analysis found that the notices Google provided to users about what information it sought to collect were not easily accessible. “Essential information, such as the data processing purposes, the data storage periods, or the categories of personal data used for the ads personalization, are excessively disseminated across several documents, with buttons and links on which it is required to click to access complementary information,” CNIL explained. “The relevant information is accessible only after several steps, sometimes requiring up to five or six actions.”

And when users were able to access this information about Google’s data practices, it was not always “clear or comprehensive,” CNIL said. “Users are not able to fully understand the extent of the processing operations carried out by Google,” the regulator added. This was because the terms Google used were “too generic and vague in manner, and so are the categories of data processed for these various purposes...the information communicated is not clear enough so that the user can understand that the legal basis of processing operations for the ads personalization is consent and not the legitimate interest of the company.”

CNIL also found that Google violated the GDPR because it does not validly obtain users’ consent to process their data for ad personalization. This is because Google does not sufficiently inform users about the company’s data practices, and when users go through the process to make changes to what data is collected

THE FIRST BIG FINE

A FRENCH REGULATOR ISSUED THE FIRST MAJOR FINE FOR VIOLATIONS OF THE EU’S GENERAL DATA PROTECTION REGULATION. OTHER ORGANIZATIONS ARE TAKING NOTE. BY MEGAN GATES

IT WAS THE MOMENT the global data privacy world had been waiting for. A regulator fined Google €50 million ($56.7 million USD) on 21 January for violating the European Union’s General Data Protection Regulation (GDPR)—the first major fine against a company following the regulation’s compliance deadline.

The fine amount was justified, France’s National Data Protection Commission (CNIL) said, because of the “severity of the infringements” it observed of the principles of the GDPR—transparency, information, and consent.

“Despite the measures implemented by Google, the infringements observed deprive the users of essential guarantees regarding processing operations that can reveal important parts of their private life since they are based on a huge amount of data, a wide variety of services, and almost unlimited possible combinations,” CNIL said in a press release. The commission added that the violations are “continuous breaches of the regulation as they are still observed to date. It is not a one-off, time-limited infringement.”

Two associations—None Of Your Business and La Quadrature du Net—filed complaints with CNIL in May 2018. They claimed Google did not have a valid legal basis under the GDPR to process users’ personal data for ad personalization purposes.

CNIL then began investigating Google and found that when users created Google accounts using Android smartphones, the tech company’s practices violated the GDPR in two ways: transparency and legal basis for ads personalization processing.

CNIL’s analysis found that the notices Google provided to users about what information it sought to collect on them were not easily accessible.

“Essential information, such as the data processing purposes, the data storage periods, or the categories of personal data used for the ads personalization, are excessively disseminated across several documents, with buttons and links on which it is required to click to access complementary information,” CNIL explained. “The relevant information is accessible only after several steps, sometimes requiring up to five or six actions.”

And when users were able to access this information about Google’s data practices, it was not always “clear or comprehensive,” CNIL said.

“Users are not able to fully understand the extent of the processing operations carried out by Google,” the regulator added. This was because the terms Google used were “too generic and vague in manner, and so are the categories of data processed for these various purposes...the information communicated is not clear enough so that the user can understand that the legal basis of processing operations for the ads personalization is consent and not the legitimate interest of the company.”

CNIL also found that Google violated the GDPR because it does not validly obtain users’ consent to process their data for ad personalization. This is because Google does not sufficiently inform users about the company’s data practices, and when users go through the process to make changes to what data is collected.
about them for ad personalization, the options are prechecked.

This violates the GDPR, CNIL explained, because “consent is ‘unambiguous’ only with a clear affirmative action from the user—by ticking a non-pre-ticked box, for instance.”

Google responded to the fine with a statement that users expect transparency and control from it and that it is “deeply committed to meeting those expectations and the consent requirements of the GDPR,” according to the BBC.

At a February 2019 event in Dublin, Ireland, Google’s Chief Privacy Officer Keith Enright said the company will appeal CNIL’s finding. (It had not filed an appeal by Security Management’s press time.) Google did not respond to requests for comment on this article.

While Google plans to appeal the finding, the initial fine marks a turning point in the first year of the GDPR compliance enforcement. The regulation—drafted in 2012 and approved in 2016—went into effect on 25 May 2018.

The GDPR was designed to give EU citizens greater control of their personal data and rights to what data they choose to share and have retained by organizations. It required organizations that collected EU citizens’ data to obtain “clear and affirmative consent” for data collection, have privacy policies in clear and understandable language, inform citizens when their data was compromised, allow citizens to transfer their data to other organizations, and request to have their data deleted—commonly known as “the right to be forgotten.”

Despite the two-year time frame companies were given to comply with the regulation, many were not compliant by the deadline. Others made only limited efforts to become compliant, preferring to wait instead until the first major fine was issued to see how serious regulators were about enforcement.

“One year after enforcement began, many companies are still not compliant with the GDPR,” says Andrea Little Limbago, chief social scientist at Virtru, who gave a presentation at the RSA Conference 2019 on privacy laws.

A core challenge many companies face in achieving compliance is meeting the Right of Access requests, she explains in an interview with Security Management.

“As consumers are increasingly wary of how data is collected and used, the number of data requests is increasing and many companies may not be able to respond securely within the deadline with data in a readable format,” Limbago says.

Companies are also struggling with the GDPR’s consent requirements, especially when it comes to transparency and accessibility.

“Under the GDPR, companies can’t bundle multiple uses of data within a single consent form, which had been the standard in many industries,” she adds.

This practice was one of the reasons that Google was found to be in violation of the GDPR, and Limbago says she was not surprised that CNIL focused on consent—and that Google
was using data for practices other than those users had consented to—for its first major fine.

To avoid similar fines, Limbago suggests that companies review how they obtain consent to collect users’ personal information.

“Each data use requires its own consent, and it must be very clear to the user exactly what they are opting into,” she explains. “This transparency is essential and requires shifting away from those standard business practices, such as auto-populating boxes to assume consent, that are not considered compliant as the user must actively confirm their consent.”

And while companies continue moving towards compliance with the GDPR, California-based companies will soon face new data privacy challenges. In June 2018, then-California Governor Jerry Brown signed the California Consumer Privacy Act (CCPA), which goes into effect in 2020.

The CCPA applies to for-profit organizations that collect and process California residents’ personal information or do business in the state. Organizations must also meet one of three additional criteria for the CCPA to apply to them: generate an annual gross revenue in excess of $25 million, receive

A majority of respondents in a March 2019 poll said that the most dangerous type of insider threat is a negligent end user.

INSIDER THREAT

Compromised
Those exploited by outsiders through compromised credentials

Malicious
People who intentionally cause harm for personal or financial gain

Negligent
Well-meaning workers who accidentally expose sensitive information


HIGH SECURITY PERIMETER SOLUTIONS

Protecting what MATTERS MOST.

For product info #15 securitymgmt.hotims.com
or share personal information of more than 50,000 California residents each year, or obtain at least 50 percent of its annual revenue by selling California residents’ personal information.

The CCPA shares some similarities with the GDPR, such as requiring companies to demonstrate after a data breach that they took reasonable steps to protect that data from a breach, but it also differs from the European regulation.

“The CCPA ignores certain categories of personal data that are covered by the GDPR because they are covered under other U.S. regulations, such as HIPAA,” Limbago says. “The penalties are also a bit different, with the GDPR focused on up to 4 percent of annual global turnover, whereas the CCPA focuses on a per violation fine.”

Unlike the GDPR, the CCPA does not require organizations to hire data protection officers or conduct impact assessments—in some cases.

“The good news is that for companies that are GDPR compliant, it will be much easier to be compliant with the various patchwork of laws coming into effect in the United States,” Limbago adds. “In fact, the lack of harmonized data privacy laws across the United States may pose the biggest compliance challenge given how quickly these policies are emerging.”

Vermont recently passed data privacy measures that apply to data brokers, Colorado passed a consumer data protection law, and Massachusetts is considering privacy legislation. The U.S. Senate Committee on Commerce, Science, and Transportation also held a hearing earlier this year on creating a federal data privacy framework.

“In an age of rapid innovation in technology, consumers need transparency in how their data is collected and used,” said Committee Chairman U.S. Senator Roger Wicker (R-MS). “It is this committee’s responsibility and obligation to develop a federal privacy standard to protect consumers without stifling innovation, investment, or competition.”

However, Limbago says she thinks the United States will work to federally harmonize data breach laws before adopting federal privacy provisions, which are likely to meet more resistance.

“There are currently over 50 data breach notification laws in the United States, each with slightly different provisions and requirements,” she says. And in the international arena, nations will likely move in one of two directions—embracing the GDPR with similar regulations or adopting a more authoritarian view. Vietnam, for instance, recently enacted a law that requires Internet companies to remove content that communist authorities contend is against the state.

Companies that collect data on Vietnamese citizens are also required to have an office in the country.

India is also considering data privacy legislation that would require companies that collect Indians’ user data to store that data in the country, and for personal data to be processed in the interest of the state.

“These new laws tend to limit free speech and mandate government access to data,” Limbago explains. “While China and Russia best exemplify this competing framework, Vietnam’s recent data law and the one under debate in India both reflect aspects of authoritarian versions of data protection, and it is a model that continues to spread globally.”

Consumers need transparency in how their data is collected and used.

New or transitioning into the security management profession?

Make our new Associate Protection Professional (APP) certification the first rung on your security management career ladder!

Find out if you qualify!
Land O’Lakes, Inc., hired a security leader to build a program from the ground up. Here’s how he did it.

Starting From Scratch

Defining and introducing functional security improvements into a 90-year-old company with worldwide operations and a well-established organizational culture is, at best, a challenging task.

This was the reality that presented itself when I was hired as global security director for Land O’Lakes, Inc., in 2012 and given a clear mandate to design and implement an enterprisewide security program from scratch.

Over the past few years, the business had transitioned from a holding company to an operational enterprise. In the past, each operating entity was responsible for its own security. But under the new model, security would become a centralized support function—along with other headquarter functions that would become standardized across the enterprise.
This new approach would make Land O’Lakes better prepared to protect itself and its employees, and to respond adaptively to the dynamic environment of a 21st century organization. As security risks become ever more complex, threats like terrorism, crime, and cyberattacks are asymmetric and networked, making them more difficult to manage.

I considered it a once-in-a-lifetime opportunity to go into a Fortune 500 company with a clean slate to establish a corporate security function—without inheriting dated policies or overcoming a predecessor’s established vision.

Founded in 1921 by 320 dairy farmers in St. Paul, Minnesota, the Minnesota Cooperative Creameries would eventually become what is known today as Land O’Lakes, Inc.

Since 1981, Land O’Lakes, Inc., has supported Land O’Lakes International Development, a 501(c)(3) nonprofit that has led nearly 300 programs in almost 80 countries that help communities around the world build economies by strengthening agriculture from farm to fork. These initiatives are designed to improve farmers’ agricultural productivity and food security while also creating stable market systems.

Land O’Lakes has approximately 10,000 employees and does business in more than 50 countries and in every U.S. state. The organization has 3,963 members, including 1,959 dairy producers, and had $14 billion in net sales in 2012.

In 2012, Land O’Lakes was looking to hire a security leader. I understood the company to be an agricultural enterprise that in a few years grew from $7 billion to $15 billion in sales. With this growth, there were acquisitions, mergers, and joint ventures—both domestic and internationally.

With increased global business activity, a fast-expanding international workforce, and a diverse international development portfolio in higher threat locations such as Yemen, Lebanon, and Egypt, the company leadership was well aware of the risks.

During the interview process, I quickly discovered that leaders at the senior level of the enterprise genuinely understood the need for a new skill set to help them manage the day-to-day threats that they were not equipped to handle. Leadership was receptive to allowing for adjustments to what the function of the position would embody, and what it would not.

Before accepting the position, I was able to negotiate a rewrite of the position description of a security manager to that of a global director of security to embrace the following responsibilities: physical security, investigations, international risk management, travel risk management, liaison with law enforcement and the U.S. Department of State, as well as other ancillary functions, such as event security and executive protection.

My new job would be to create a security program that would be standardized across the enterprise from headquarters across the globe. It would involve building a program that would make the company better prepared to protect itself and its employees.

First Steps

When I reported for duty in February 2012, I was given a simple direction: learn the business and meet the leaders. So, I did.

I started with conducting research on Land O’Lakes and spoke to a senior sales manager, who gave me an insider’s perspective about what it is like to work for one of the most recognizable branded companies in America.

I discovered that, in addition to dairy foods, Land O’Lakes is a major player in agriculture, primarily through its Purina Animal Nutrition and WinField United divisions—both domestically and internationally. However, the riskiest undertakings for the company were with its International Development group.

Land O’Lakes International Development has applied an integrated approach to international economic development, with funding from USAID, the U.S. Department of Agriculture, and the Bill and Melinda Gates Foundation.

The employees associated with this nonprofit segment use their practical experience and in-depth knowledge to facilitate market-driven business solutions that generate economic growth, improve health and nutrition, and alleviate poverty. They live and operate in some of the riskiest places in the world—meaning security is at the forefront.

During my learning phase, I quickly identified my many principal business partners within the company. The most significant ones included human resources, the legal department, internal auditors, the risk management team, and the real estate and facilities group. Early on, I realized that the security function could not succeed without support from those and other key leaders.

I got to know the many partners and made certain that they understood what the security function would do and how I intended to integrate security.
into their day-to-day operations. For example, it was essential to meet with other leaders to review existing practices on how facilities are leased or built, then partnering to reshape or tweak those procedures to include security in the internal planning process. Establishing early mutual respect, and learning about how each function adds value, was a critical step. I also traveled to meet with as many company leaders as possible, from plant shift leaders to plant managers to members of the C-suite.

This process included several meetings with the CEO, board members, and the chairman of the board. I asked detailed questions about what each one considered to be important from a security perspective, and also took the opportunity to present my vision for the future of the security function at Land O’Lakes. Knowing my communication had to be direct, simple, and memorable, I developed an elevator speech for these interactions. I gave a quick introduction of myself—what I do, where I report within Land O’Lakes—and used my parting tag line: “Asset protection equals bottom line on the balance sheet.” I then followed up with, “Can we meet for 30 minutes so I can learn more about you and your team?”

This approach was generally successful. And one of my first indispensable early partners was the director of internal audit. During my first year, through collaborative investigative effort, we discovered internal control weaknesses that allowed us to implement new process controls and enhancements to prevent future fraud.

For example, we cross-referenced the company’s employee database against its accounts payable, which revealed that employees were receiving illicit payments at their home addresses. We then took action to address this fraud that took advantage of our formerly weak internal controls. Where appropriate, we had dishonest employees prosecuted and recouped stolen funds through restitution. This incident taught me that if I do not know the corporate and supply chain business leaders, I will never learn the business. And if I do not know the business, I cannot hope to effectively prevent losses.

**Strategic Planning**

Besides learning the business and the prevailing culture, my other initial task was to develop and communicate an effective strategic plan that could be accepted by key leaders. The early priorities were to pinpoint clear objectives for the new global security function, to ensure alignment with various broader corporate objectives, and to execute the plan to achieve those objectives. The strategic plan became the ultimate guide to decision making within the team. It helped with several decisions, guided me in implementing my vision, and influenced senior management’s expectations.

To create the strategic plan, I started with setting internal benchmarks within several areas. I identified key initiatives (policies, processes, and people); costs and timelines for these initiatives; an alignment matrix with other functional areas (touch points with internal audit, communications, human resources, real estate and facilities, the legal department, and regulatory compliance); and identified domestic versus international priorities derived from discussions with C-suite leaders. Using those considerations, I was able to work with other stakeholders to direct effort and resources towards initial operating challenges the security function needed to address. These included being unable to determine the total security expenditure within the company; the lack of uniform enterprise technology standards for access control and monitoring; decentralized guard operations; lack of understanding about what security does; the absence of centralized reporting of security-related incidents; lack of insight into who was traveling globally; a scarcity of professional competence for fraud, theft, and workplace violence incidents; and no defined jurisdiction or strategy for preventing or responding to workplace violence concerns.

With my energy focused on people, process, and relationships, I assessed what could be adjusted, improved, fixed, or otherwise put into action quickly and at a low or no cost. **Contracting.** For example, streamlining guard contracting by centralizing the decision making was a necessary improvement. Previously, each location contracted for security guards, and other related services, autonomously with disparate providers with varying degrees of success. The local agreements were not properly examined by security professionals, which hampered...
Guiding Principles

To better prepare Land O’Lakes to protect itself and its employees, its security program was designed around these guiding principles:

PROTECT YOUR HOUSE
Achieve a safe and secure workplace with innovative management and actionable solutions.

EMPOWER YOUR PEOPLE
Embolden operating business units and sites to safeguard their own assets within a realized risk-based framework.

AIM TO INFLUENCE
Adopt a philosophy where the Global Security Department’s primary role is to influence business partners to deliver security through their everyday actions and decisions.

BE A CHANGEMAKER
Recognize that security is in the business of change management, rather than enforcement.

LOOK FORWARD
Understand that the security function cannot stand still or become a fixed entity because its responsibilities will change over time.

NARROW THE VISION
Focus more on overall corporate resilience and less on traditional security.

UNIFY THE SCOPE
Recognize that security is both a strategic and an operational activity.

COMMUNICATE EFFECTIVELY
Security delivers influence and legitimacy derived not from professional knowledge, but from business acumen, people skills, and the ability to communicate security principles.

would own the relationship with the vendor to maintain operational control. This change in management process required consultations with stakeholders throughout Land O’Lakes to review and modify the prevailing policies. Then, the company moved to implementation with a single nationwide contract to a vetted security provider that would be managed locally.

Standards. I used a similar process to establish uniform security technology standards for the enterprise. The past practice had multifarious legacy systems that could not be interconnected. To replace them, we selected a single security technology platform for all new access control and video systems.

As a result, in 2016 the company approved funding for the construction of a Global Security Operations Center (GSOC), which became fully functional in the summer of 2018. It operates on a 24/7 basis with two contract employees at all times. Future staffing levels will expand as Land O’Lakes grows.

In addition to live monitoring our enterprise access control system, the GSOC operators can access security video feeds at any location by calling up a respective IP address for any camera at any company location. This move to a fully integrated modern security technology system will support Land O’Lakes’ operations across the globe.

Investigations. The investigation function was another area where the Global Security Department was able to add value, early on, by solving complex cases that sometimes resulted in prosecutions.

For instance, by partnering with the internal audit team, we were able to detect unexplained inventory shortages. Further investigation uncovered a sophisticated conspiracy by several employees to divert premium Purina animal feed. The employees were fired, and the information was turned over to local authorities, who prosecuted the thieves. They were convicted and sentenced to six years in prison.
A flawed strategy can undermine our ability to operate.

More recently, in January 2017, during an active shooter incident at the Fort Lauderdale Airport, 56 Land O’Lakes employees were in or around the airport. They were traveling home following a previous day’s company marketing event when shots rang out in a baggage terminal.

Instantly, we went into crisis mode and were able to quickly account for all employees and update leadership that everyone was safe. However, it took longer than desired to find contact phone numbers for all employees that were traveling.

After both incidents, we reviewed our response protocols and made appropriate adjustments to our internal processes.

One change made after the Fort Lauderdale shooting was to require that employees provide a cell phone number when they are issued an airplane ticket for travel. This is so that employees can be contacted—in the event of an emergency—while traveling. We also established a 1-800 informational number for employees to call in to during an emergency.

Getting Feedback

Throughout the process of creating a Global Security Department, I’ve received valuable feedback. The most significant feedback, however, has come during the budget planning cycle in the form of authority to hire security staff as full-time employees.

By this measurement, the security function at Land O’Lakes is clearly up-and-coming because the security budget has trended up each year since it came into existence in 2012 with the addition of three full-time security professionals on staff and prospects to hire more. When scarce resources are allocated, security has a seat at the table alongside other business functions. This type of feedback demonstrates that the function is adding value to the company.

My intent from the beginning was to use a “baby steps” approach while building a well-integrated security program. This was best accomplished by depending on my personal credibility, while always remembering that security must have the support of management at all levels of the business.

It is not sufficient to understand the technical aspects of security; I must also be well versed in the business aspects of operating within a global enterprise and appreciate that security, like other business functions, contributes to the bottom line.

At Land O’Lakes, there is now a greater appreciation of the interdependence between the company’s risk appetite and the way it does business. It’s recognized that a flawed strategy can undermine our ability to operate, and, in some cases, can generate risks that would not otherwise be present.

As a result, security has a higher profile within the company today than it did six years ago. Land O’Lakes is constantly looking for new ways to manage both domestic and international risks, and the portfolio of the Global Security Department has widened to include shared responsibility for corporate reputation, governance and regulation, social responsibility, and information assurance as a result.

First, let’s start with a few big picture questions. What effects will the continued rise of the gig economy have on the security industry? Will it mean more opportunity for consultants and security service providers, or more competition?

A. The rise of the gig economy is the logical outcome of the quick win business era that we live in. In this era, businesses focus on cost savings and cost avoidance, and are oriented toward quick profits and short returns of investment.

This has also changed the once strategic nature of security by transforming it into a quick win, project-based service. Unfortunately, security is the usual suspect in nearly every cost-saving equation. The moment security becomes the subject of a quick cost-cutting move, it transforms from a complex process to a simple product. This does not leave much space for deep strategy, sustainability, and consistency.

On one hand, the rise of the project-based economy does provide more job opportunities for security consultants. However, many consultants without a clear and unique niche, and without enough experience, often try to go global instead of focusing on the local. This is a mistake. While the number of prospective clients usually increases with geographic expansion, competition grows, too. Moreover, as the expansion radius increases, competition grows proportionally faster than opportunities.

Security performance is linked to local knowledge and understanding of the cultural nuances and specific place variables, and the overall ability to

In these times of overwhelming security risks, it would be naive and irresponsible to neglect the need of people to feel safe.
incorporate this knowledge in the comprehensive security calculus. It also relies on a strong local network and resources. Additionally, distance increases the cost of the service, which makes it less attractive for clients. It also makes customer support following the completion of the project more difficult.

Instead of diluting their chances of landing gigs by spreading their focus all over the crowded global marketplace, consultants without a clear universal advantage should primarily focus on suitable and financially viable local opportunities.

Is the development of the gig economy changing the nature of security consulting, and the nature of security services, in fundamental ways?

A. Yes, and I believe that it is the small and medium-sized businesses (SMB) that are benefiting the most from the emerging models of security consulting. Traditionally, it has generally been larger enterprises that were privileged enough to be able to afford a security setup, whether in house or outsourced. Smaller businesses didn't always have the resources or the need for full-time security management professionals on their team. However, these smaller companies still have security issues, experience occasional incidents, and encounter recurring losses. Although they might not justify the cost of adding additional full-time staff, the inconveniences are still significant enough to create the need for a dedicated part-time security function. Until recently, such companies had three bad choices: overpay, compromise on the quality of service, or simply leave issues unaddressed.

Now we have security consulting companies that are completely devoted to offering viable security management solutions to SMBs based on a specific time-sharing business model. Such consultancies typically have a back office composed of professionals who specialize in different aspects of security (investigations, executive protection, intelligence, or engineering) and a front office with generalist field chief security officers. Each of the chief security officers is responsible for the security of several businesses and is physically present in each of them during one or more days per week, depending on the assessed need and the agreed pace. The “back office” is always on standby to provide specialist support for more complex issues.

This model allows a business to have a CSO and a team of specialists performing a service that is specifically tailored to its actual needs while paying only a fraction of the actual cost. I believe that similar models of consulting will grow and expand as
security professionals start to fully understand the opportunities that lie in the SMB market.

**In your book, you mention one potential drawback of outsourcing, through the example of the hospitality industry, which requires security “to be both a presentation and a performance.” Is it advisable for security consultants to promote themselves as adept both at delivering top-shelf security services and marketing?**

**A.** I don’t believe that any commercial process, service, or product can currently survive without having both functionality and appeal. In the past, security and marketing were always regarded as complete opposites. The function of marketing was to create attraction; security was seen as an unattractive distraction to that, an unavoidable obstacle.

Although it has been more than 70 years since Abraham Maslow, in his Theory of Human Motivation, suggested that safety is the second most important human need, right after the basics of air and food and water, only recently have marketing experts started to realize that security is a concept that positively influences the perceptions and decisions of consumers and, as such, actually promotes products and supports commercial agendas.

Moreover, security could be the prevailing factor in ruling out the competition. Many studies that analyze the motivation of consumers put security at the top of the list of human needs that are essential to all selling, whether face-to-face or in advertisements. It is emotions that sell, and the feelings of being at risk and of being safe are even more successful than sex or desire in triggering emotions.

The shrinking of distance as a product of globalization suddenly brought a variety of security risks right to the living rooms of ordinary people. Crimes and terror can now be committed from a distance using the Internet, while fear as an instrument of terror marketing spreads instantly through new information and communication channels. Moreover, political violence around the globe and intolerance between different ethnic and religious groups have probably reached the highest point in history.

In these times of overwhelming security risks, it would be naïve and irresponsible to neglect the need of people to feel safe. The hospitality industry is the perfect example of missed opportunities. Paradoxically, even in regions where terrorist attacks are extremely frequent and where hotels are continuously targeted by terrorists and have suffered devastating attacks, hotels still base their marketing campaigns on the apparent and latent desires of customers by advertising ocean view, food, location, and comfort. Hoteliers completely “forget” to mention security, which is a fundamental concern of guests, and even go the extra mile to hide their security measures.

**Will the growth of online platforms cause more end users to turn to more generic security services?**

**A.** Everything we do in security, starting from the creation of policies and down to executing hands-on tactics, is based on a combination of specific circumstances. Even companies that are seemingly identical in every aspect—such as location, size, product, and agenda—might experience some very different issues.

The only advantage of freelance platforms is the possibility to staff and execute projects remotely which, in my opinion, has no application in security. I believe that assessments as well as the design and management of any security-related process or project require actual physical presence. Also, because trustworthiness and reliability are crucial when hiring security consultants and service providers, word of mouth and reputation will continue to outrun convenience and accessibility in hiring calculations.

**What other advice would you give to consultants and service providers who want to thrive in the current—and future—security marketplace?**

**A.** Things that we believe give us an edge aren’t necessarily our competitive advantage. So, devote time and energy to understanding what it is that can help you gain an actual advantage over the competition. Expect to be surprised by the result. But also remember that these competitive “X” factors by themselves aren’t enough to ensure success in the marketplace. Apart from strengths, we must also clearly assess our weaknesses and work diligently on finding the missing pieces and adding them to the puzzle.

Many security consultants and service providers in business settings don’t understand that their true mission is not helping the security of the business but helping the business by improving its security. Before rolling up our sleeves and getting our hands dirty, we must devote time and effort to fully understanding the client’s business, including its culture and goals.

Competing on price alone degrades the profession and leads to a race to the bottom by placing us among countless similar, anonymous, cheap consultants and service providers. On the other hand, competing on quality advances the trade, gives us an identifiable differentiator, and simultaneously lifts us toward niche markets.

From first to last: be fair to yourself, the client, and the profession.

**MARK TARALLO** is senior content manager at Security Management. Contact him at MarkTarallo@ASISOnline.org. Connect with him on LinkedIn.
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 | New program
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:
3 April  Turnstiles 101 – Designing & Implementing an Entrance Control System
4 April  How to Prove the Value of Corporate Security Investments
9 April  Building a Business Case (for members only)

FIND DETAILS ON ALL PROGRAMS AT ASISONLINE.ORG/JUNECLASS
The U.S. Department of Homeland Security (DHS) issued a binding operational directive in September 2017 to remove all Kaspersky Lab information security products, solutions, and services from all federal government departments and agencies. It was the first time DHS issued an order to remove all of one manufacturer’s software from government systems.

“This action is based on the information security risks presented by the use of Kaspersky products on federal information systems,” DHS said in a statement on the directive. “Kaspersky anti-virus products and solutions provide broad access to files and elevated privileges on the computers on which the software is installed, which can be exploited by malicious cyber actors to compromise those information systems.”

DHS also issued the order because it was concerned about ties Kaspersky, a Russian company, might have to Russian intelligence agencies.

“The risk that the Russian government, whether acting on its own or in collaboration with Kaspersky, could capitalize on access provided by Kaspersky products to compromise federal information and information systems directly implicates U.S. national security,” DHS explained.

The department gave federal agencies and departments 30 days to identify all Kaspersky products on their systems. The agencies had to create plans to remove and discontinue use of those products within 60 days, and discontinue and remove those products within 90 days of the notice.

Following the directive, the U.S. National Defense Authorization Act was enacted in December 2017 to outlaw the use of Kaspersky products within federal agencies and departments.

Kaspersky denied allegations of ties to the Russian intelligence community and also challenged the U.S. government’s ban of its product in U.S. federal court. The D.C. Circuit Court dismissed Kaspersky’s lawsuit, but CEO Eugene Kaspersky said in a statement that the company would remain committed to “providing the best cybersecurity solutions for our customers globally and saving the world from cyberthreats.”

After the Kaspersky directive, other companies’ products have come under scrutiny for posing possible security threats to governments and private companies alike. The U.S. government, Japan, and others have also put restrictions around the use of Huawei and ZTE products—both manufactured by Chinese companies—citing security concerns.

The moves also renewed focus on the need to address the supply chain security of information technology products. A lack of such security here could create major risks for end users who install those products in their systems.

“Traditionally, most organizations have been focused on the hardware and physical aspects of the supply chain—does it have counterfeit parts, was it compromised in
The fifth generation of wireless networking technology, dubbed 5G, is predicted to transform the way users work and live because of its increased connectivity benefits.

“One way to quantify the difference is in terms of download speeds,” according to a Verizon fact sheet. “5G will deliver speeds roughly 20 times faster than what is possible with 4G.” This enhanced data transfer speed will allow more technology to connect to each other, including vehicles, the Industrial Internet of Things, and Smart City networks. The first 5G networks, however, will not be available nationwide in the United States until 2020, according to WIRED’s “Guide to 5G.” And only if there is a major investment in the technology between now and then.

To reach the goal of nationwide 5G by 2020, the government must open more wireless spectrum to carriers; the carriers must rapidly expand their infrastructure, and hardware makers need to create a new generation of devices ready to ride the 5G waves,” WIRED explained.

**What is 5G?**

The fifth generation of wireless networking technology, dubbed 5G, is predicted to transform the way users work and live because of its increased connectivity benefits.

“One way to quantify the difference is in terms of download speeds,” according to a Verizon fact sheet. “5G will deliver speeds roughly 20 times faster than what is possible with 4G.” This enhanced data transfer speed will allow more technologies to connect to each other, including vehicles, the Industrial Internet of Things, and Smart City networks. The first 5G networks, however, will not be available nationwide in the United States until 2020, according to WIRED’s “Guide to 5G.” And only if there is a major investment in the technology between now and then.

To reach the goal of nationwide 5G by 2020, the government must open more wireless spectrum to carriers; the carriers must rapidly expand their infrastructure, and hardware makers need to create a new generation of devices ready to ride the 5G waves,” WIRED explained.

**Response**

Shortly after the GAO published its report, DHS announced the creation of its National Risk Management Center.

“It will employ a more strategic approach to risk management born out of the re-emergence of nation-state threats, our hyperconnected environment, and our survival and its need to effectively and continually collaborate with the private sector,” said former DHS
REACH NEW HEIGHTS in Professional Excellence

ASIS accredited certifications can help you reach your career goals.

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

–Nicholas Santillo, Jr., CPP, PCI, PSP, Vice President, Chief Digital Infrastructure & Security Officer, American Water
Secretary Kirstjen Nielsen in a speech at the department’s Cybersecurity Summit in July 2018. “...the center will bring together government experts with willing industry partners so that they can influence how we support them. Our goal is to simplify the process—to provide a single point of access to the full range of government activities to defend against cyberthreats.”

One of the center’s first major efforts would be bringing together government and industry to address supply chain risk. In November 2018, the center launched the Information and Communications Technology (ICT) Supply Chain Risk Management Task Force to develop consensus recommendations that identify and manage risk to the global ICT supply chain.

“This is a moment when we need increased effort countering strategic risks that we see from—particularly—foreign adversaries in the cybersecurity space, including supply chain,” says Bob Kolasky, director of the National Risk Management Center and task force cochair. “There is an urgency of government and industry coming together to take this threat seriously and come up with solutions to address the threat and reduce risk.”

The task force consists of 60 representatives from the private sector and government, including members of the intelligence community. Kolasky co-chairs the task force with John Miller, vice president of policy and law at the Information Technology Industry Council (ITI), and Robert Mayer, senior vice president for cybersecurity at the USTelecom Association.

Mayer, who is also the chair of the DHS Communications Sector Coordinating Council, says that the range of representatives on the task force means there will be broad conversation to generate real progress on supply chain security.

“Given the recognition now that the supply chain represents a major vector for attacks, especially when you consider the nation-states behind them, there’s a great deal of urgency to have a coordinated strategy and plan to mitigate the risk,” he adds.

The task force, which has a two-year charter, held an initial meeting after it was created in November 2018. To get the ball rolling, the task force created an inventory of both government and private sector initiatives to address supply chain security to prevent duplication of previous efforts.

The partial U.S. government shutdown in December and January delayed the database initiative, but Mayer says the task force was on track to have both segments of the inventory completed in March 2019.

The task force will then use this inventory to inform its future work, which it divided into four initial workstreams that it announced in the spring. One workstream is devoted to developing a common framework for bi-directional sharing of supply chain risk information between government and industry. DHS already has a variety of information sharing channels in place to communicate between government and industry, so the task force intends to identify any gaps in sharing about supply chain vulnerabilities.

“Private entities are constantly evaluating whether there’s risk in things they put in their supply chains or understanding their own risk, and as they’re making their own risks, we want to understand why those decisions are being made so that we can help push that message out that other companies might want to be making similar decisions,” Kolasky adds.

Another workstream focuses on identifying processes and criteria for threat-based evaluation of ICT supplies, products, and services. This workstream will provide organizations with an understanding of what the criteria are and what the dimensions of supply chain oversight might look like, Mayer says.

Threat criteria are often based on the party that is assessing the technology, which will make this workstream’s assignment slightly daunting.

“Somebody in an acquisition role may have one set of parameters they’re interested in from a supply chain perspective; if it’s the end user, they might have another,” Mayer says. “Views change.”

The information the second workstream identifies on criteria will likely help inform the third workstream: identifying market segments and evaluating criteria, establishing qualified bidder and manufacturer lists. Ideally, this workstream will inform companies about what standards they will need to meet to qualify as a white list bidder.

The fourth workstream is focused on producing policy recommendations to incentivize purchasing ICT from original manufacturers or authorized sellers. The consensus is that “if you purchase equipment from the original manufacturer or an authorized reseller, instead of buying it” from an unauthorized seller, “you have a better likelihood that the security protocols have been adopted, implemented, and verified,” Mayer says.

To get companies and agencies to adopt this purchasing pattern, the workstream will look at which incentives will help users make decisions “based on good cyber supply chain risk management,” he adds.

The task force met several times this spring and plans to release information to the public about its progress beginning this summer. Mayer says. It will also continue looking at the scope of its work and addressing the workstreams’ assignments as the task force evolves.

“I think what we’ll see is an ongoing process of evolving of the scope, adding new efforts into the equation,” he adds.

“There is a desire here to produce products that are actionable and that can actually move the needle.”
In addition to the workstreams, the task force will also work with the Supply Chain Security Council that was created by the 2018 U.S. Federal Acquisition Act.

The council focuses on the federal government, tasked with mitigating security risks that could arise from information technology, telecommunications services, and other services the federal government buys.

The council is responsible for creating criteria to assess threats and vulnerabilities to the supply chain, issuing guidance on risks to the supply chain, as well as publishing guidance on how to address those risks.

The council must obtain input from the private sector on supply chain risk, and Kolasky says that the task force will be the primary venue for that dialogue.

Overall, Mayer says it’s important that these conversations are happening and that the private sector—through the council—is included in the process.

“When the Department of Homeland Security comes to industry and says that they want to partner with industry on making improvements on a critical national security consideration, that’s music to our ears,” Mayer adds. “That’s what we want to see in the public-private partnership collaboration with government.”

And this partnership is critical for addressing supply chain security and ensuring that the United States has a path forward to make the acquisitions process for private and public entities. In the RSA appearance with Eoyang, Managing Director of the Cyber Readiness Institute Kiersten Todt said it was vital for the United States to address this issue.

“We don’t want to find ourselves in the position where we’re in the environment that China has defined for us,” she said.

MEGAN GATES IS SENIOR EDITOR AT SECURITY MANAGEMENT. CONTACT HER AT MEGAN.GATES@ASISONLINE.ORG, FOLLOW HER ON TWITTER: @MGNGATES.
A DAY IN THE LIFE OF
ELIZABETH MOSLANDER, CPP

COMPANY: CAPITAL ONE  POSITION: MANAGER, PHYSICAL SECURITY OPERATIONS–GLOBAL SECURITY  YEARS WITH THIS COMPANY: SIX

5–8am
Elizabeth Moslander, CPP, rises bright and early to check email on her phone to alert her of any pressing matters she might have to face during the day. She tends to the family cat and dog before getting her 12- and 15-year-old daughters ready for school. Prepared to face the day, she then embarks on her hour-long commute to worksites in the Chicago area.

8–11am
“We have a desperate need to bring the importance of this industry to the attention of the younger generation,” she adds. “Young people know about cybersecurity, but we have a lot of work to do to educate them about the many other diverse aspects of our industry.”

11am–5pm
Business as usual for Moslander involves incident and robbery response, developing enterprise life safety initiatives, resolving any security equipment breakages, reviewing facility security, and designing, implementing, and validating project system design.

“You’ve critical to maintain health, motivation, and perspective,” she says. “Don’t sacrifice so much to work that, at the end of the day, you find yourself asking if it was worth it. No one ever looks back at the end of their career and wishes they’d spent more time at work.”

5–10pm
Beyond splitting daughter chauffeuring duties with her husband David, Moslander loves baking, crafting with her girls, and watching a good comedy. She’s also trying her hand at Super Team tennis in 2019—a form of socialized tennis where the participants gather to play, eat, and socialize.
Have you updated your ASIS profile?

To optimize engagement with ASIS—and to ensure that you receive content most relevant to your needs—please take 5 minutes to complete these 3 easy steps:

1. Visit asisonline.org and log into your ASIS profile.
2. Click “my information” and then go to “my account” to review your profile details.

We also encourage you to review our privacy policy at asisonline.org/privacy.

THANK YOU
He will offer a first-hand look into the trends, risks, and potential rewards amid hot spots around the globe, and the role the United States should play on the global stage.

Kelly’s address will kick off Military and Law Enforcement Appreciation Day, which honors those who make communities and the world a safer place. All law enforcement, military, and first responders are entitled to free one-day admission to GSX on 11 September. To learn more and register, visit GSX.org/MLEAD.

CREATING A CERTIFICATION

The Associate Protection Professional (APP) early career certification is almost ready for its worldwide debut. But what makes a certification? How does a certification come into existence?

Overall, it takes months of hard work from many dedicated security professionals over several phases to ensure that the exam accurately tests the knowledge and skills a security professional needs to be successful in his or her career. For the APP, it was critical that the test focused on skills and knowledge for those relatively new to the security profession, because the certification is designed for those with one to four years of experience in the industry. It tests competencies in four broad domains:

- Security management fundamentals
- Business operations
- Risk management
- Response management

First, ASIS conducted a job analysis, consulting a global panel of subject matter experts to determine the body of knowledge professionals need to excel in their careers. In the case of the APP certification, the panel identified the four domains listed above.
ASIS surveyed almost 10,000 security management professionals to validate the panel’s work and evaluate how important each domain is relative to the others. This determined how many questions on the final exam would address each domain.

Next, a volunteer panel gathered to write the questions that appear on the APP exam. Every question must have four answer choices—three plausible wrong answers, called distractors, and one correct answer tied to a specific reference from the exam’s recommended reading material. For the APP, the recommended reading material includes three volumes from the Protection of Assets set and various ASIS Standards and Guidelines.

“I thought taking the CPP exam was tough, but now I realize that creating an exam is even tougher,” said one APP item writer from The Netherlands. “Formulating the questions—not too simple, but also not too complicated—and then finding a balance between the right answers and good distractors is quite a challenge.”

More than 230 security professionals beta-tested the APP between December 2018 and February 2019. Based on test takers’ performance, a panel of volunteers determines the passing score and makes any necessary adjustments to the questions. Once these final updates are complete, ASIS will officially launch the APP program, scheduled for June 2019.

Learn more at asisonline.org/APP.

ASIS makes sure its certification programs remain current by repeating the job analysis and item writing processes every few years. In 2019, ASIS is seeking volunteers to participate in the Certified Protection Professional (CPP®) job analysis study or item writing panels for the Professional Certified Investigator (PCI®) and Physical Security Professional (PSP®) exams. If you are interested in any of these volunteer opportunities, contact the Certification team at certification@asisonline.org.

UPCOMING CLASSROOM PROGRAMS

ASIS is bringing top-notch security classroom programs to Atlanta, Georgia, in June and to Madrid, Spain, in July. Don’t miss these opportunities for hands-on training to stay informed on the latest trends in the profession.

Implementing Enterprise Security Risk Management (ESRM)
24–25 June
Atlanta, Georgia, USA
ESRM is a strategic security program management approach that ties an organization’s security practice to its mission and goals using globally established and accepted risk management principles. Learn how to develop a security program in the ESRM model.

Executive Protection
24–25 June
Atlanta, Georgia, USA
This comprehensive program covers the fundamental skills and procedures required to provide effective personal protection. Case studies reinforce the techniques and teach best practices. Ideal for those interested in executive protection as a career or who are looking for a solid refresher.

ASIS Assets Protection Course: Practical Applications (APC II)
24–26 June
Atlanta, Georgia, USA
Through real-life case studies, explore various perspectives and gain insights on current methodologies for successfully mitigating risks. The program addresses key areas of concern that every security expert must comprehend to be successful.

Risk, Threat, and Vulnerability Assessment
24–26 June
Atlanta, Georgia, USA
This program examines all aspects of planning and implementing a risk assessment program in any type of organization, large or small, public or private. Hands-on exercises and a site visit illustrate practical applications.
**ASIS/IE Business School: Effective Management for Security Professionals**

**2–5 July**
Madrid, Spain

Today’s organizations face complex challenges where every business decision affects the bottom line. To be successful, security managers must have a strategic understanding of security’s function to ensure adequate budgetary and organizational support for security initiatives. This custom-designed program will facilitate a deep dive into the central areas of management. Enhance your effectiveness in the corporate environment and align your expertise with the organization’s security requirements.

**LIFE MEMBERS**
ASIS congratulates its newest Life Members: Chris A. Hertig, CPP, and Hugh A. Palmer, CPP.

Chris Hertig, CPP, has been an ASIS member for 38 years and earned his CPP in 1982. Over the years, he has been a supporter of education in the security field, and he currently serves on the Professional Development Council and the Young Professionals Council. Hertig has written many articles and book reviews for *Security Management*. He has also been active in his local chapter, previously serving as chapter chair.

An ASIS member for 27 years, Hugh Palmer, CPP, earned his CPP in 1992. He is a recognized expert in pipeline and infrastructure security. He was a member of the ASIS Petrochemical, Chemical, and Extractive Industries Security Council and served as its chair. He was also active in his local chapter, taking on the roles of treasurer and secretary.

**MEMBER BOOK REVIEW**

Author Michael E. Goodboe, CPP, takes aim at a problem that plagues the security industry, as well as other service industries. *Reducing Turnover in the Services Sector: Lessons from the Security Industry* explores the causes of employee turnover and offers some commonsense solutions.

Personnel turnover is a normal component of business and can at times be healthy for an organization. However, excessive turnover leads to excessive costs, reduced profits, and inefficiency, while it degrades operational effectiveness. Churning of the employee pool is not conducive for team cohesiveness and the acquisition of individual experience necessary to provide a basic service level or an effective emergency response.

Unfortunately, as the author points out, the security industry for too long has accepted turnover as a normal part of doing business. Goodboe challenges that assumption and encourages managers to address the problem within their organizations by finding out why the situation exists and correcting it. Managers must recognize that a good number of employees leave their employers because of poor leadership, perhaps more than any other reason. Competent supervisors are critical to performance and retention of employees.

Among his solutions are delivering leadership skills for first-line supervisors and senior managers and using mentoring and coaching techniques to develop all levels of personnel. Quality training for security officers and supervisors using adult learning strategies is crucial. Goodboe discusses his training research and introduces the Meyers-Briggs Type Indicator assessment for understanding and identifying a successful match between the individual applicant and employment with an organization. There is also discussion of a seven-level leadership energy model based on measurements from the Energy Leadership Index.

Goodboe spent 30 years at G4S Secure Solutions USA as a senior vice president in human resources, so he...
CERTIFICATION PROFILE

MYRON LOVE, CPP, PCI, PSP

As director of security services for the Ann & Robert H. Lurie Children’s Hospital of Chicago, Myron Love, CPP, PCI, PSP, is responsible for all physical security operations protecting the hospital’s patients, employees, and guests.

Love is one of fewer than 200 professionals in the world who are ASIS Triple Crown holders, meaning he has all three ASIS certifications. While he serves as a mentor for aspiring ASIS security professionals today, at the onset of his security management journey he looked to ASIS International as a source for mentorship and guidance.

Love left the U.S. Army in 2004 and planned to start a career in law enforcement. Attending a police academy by day, he worked night shifts as a security guard in a retirement community. When he earned a promotion to supervisor, he interacted with clients more directly and quickly grew to appreciate the significant impact the security team made in the residents’ lives.

“I was hooked,” he says, “and I’ve worked in healthcare security ever since.”

He knew he had to educate himself about his new role for the future. He took online courses in security management and joined ASIS International in 2006 as a student member.

“My ASIS membership was beneficial from day one,” he says. “As a student attending local chapter meetings, I met several people that provided me with mentorship and even interviewed me for future security positions. I demonstrated my interest in growing in the field and showed that by getting more involved with ASIS, asking questions, and seeking out advice.”

He pursued the Physical Security Professional (PSP®) certification in 2012, inspired by his ASIS board-certified mentors and by what a certification meant in the industry.

“They were extremely competent, confident in their decisions, knowledgeable in security, and they were high-level contributors to our ASIS chapter and councils,” he explains. “I was motivated to gain similar knowledge and also establish myself as a subject matter expert in security.”

Despite a full calendar and a never-ending to-do list, he scheduled a firm date for his exam and studied hard—and his preparations were rewarded when he successfully attained his PSP. Driven to further develop his security qualifications, he added the Certified Protection Professional (CPP®) credential to his résumé in 2014 and the Professional Certified Investigator (PCI®) in 2019.

“Having earned all the ASIS certifications, I can be a better mentor for everyone on my team,” he explains. “I have oversight of 75 security officers and administrative staff, with managers reporting to me who are specialists in physical protection and electronic security systems, threat and risk management, and investigations for workplace violence and loss prevention. The topical expertise I gained while preparing for my board certifications has made me a much more effective guide for them all.”

Love now relishes the opportunity to serve as a leader in the security industry. He is currently vice chair of the ASIS Healthcare Security Council and previously served as vice chair of the Cincinnati Tri-State Chapter.

PROFILE BY STEVEN BARNETT, ASIS COMMUNICATIONS COORDINATOR
CENSUS. The justices of the U.S. Supreme Court will review a challenge to the Trump administration’s decision to add a citizenship question to the 2020 census. The Court scheduled oral arguments in late April, bypassing the usual procedure where a federal appeals court first issues a decision.

The challenge concerns the March 2018 decision from U.S. Secretary of Commerce Wilbur Ross to include a citizenship question in the upcoming census. According to the administration, answers to the question would assist the U.S. Department of Justice’s efforts to better enforce voting rights. State and local governments, civil rights groups, and other plaintiffs in the case claim that households with undocumented residents are less likely to respond to the question, resulting in inaccurate data.

The Court previously agreed to review an evidence dispute with the case and

CORRUPTION. Pakistan’s National Accountability Bureau indicted the country’s opposition leader, Shahbaz Sharif, on corruption charges related to a housing scheme. On 18 February, the corruption tribunal indicted Pakistan Muslim League President Sharif and nine others in connection with a scam in Lahore. The Ashiyana Iqbal housing project began in 2010 in the Punjab province, where Sharif served as chief minister from 2013 to 2018. The tribunal accused Sharif of abusing his authority as chief minister to award the contracts to unqualified businesses of people associated with his party, causing the loss of millions of rupees to the national treasury. Sharif denied the charges.

DISCRIMINATION. The Iowa District Court for Polk County ordered the state to pay a transgender nurse $120,000 in damages due to gender-related discrimination. On 11 February, the court found that the state discriminated against Jesse Vroegh by forcing him to use female restrooms at the Iowa Correctional Institution for Women and that the state’s employee medical insurance plan specifically denied him coverage for transition-related surgeries. Claiming he was treated differently compared to other male employees because he is transgender, Vroegh successfully sued Iowa’s Department of Corrections, the Department of Administrative Services, and Patti Wachtendorf, a former warden at the prison. The state added gender identity protections to its Civil Rights Act in 2017, which now protects transgender Iowans from discrimination in education, employment, housing, and public accommodations. (Vroegh v. Iowa Department of Corrections, et al., Iowa District Court for Polk County, No. LACL38797, 2019)

Bribery. A former Atlanta mayoral official was sentenced to 21 months in prison, three years of supervised release, and a fine of almost $15,000. Katrina Taylor-Parks pleaded guilty in August 2018 of accepting bribes as the mayor’s deputy chief of staff, as well as lying to the FBI and using her position to force other city employees to behave unethically. (U.S. v. Taylor-Parks, U.S. District Court for the Northern District of Georgia Atlanta Division, No. 1:18-CR-299-SCJ, 2018)
barred the plaintiffs from questioning Ross. The Court did allow questioning of then-head of the civil rights division for the Justice Department, John Gore.

In January, the Trump administration asked the Supreme Court to review the trial court’s decision without requiring the government to appeal first to the U.S. Second Circuit Court of Appeals.

The deadline for finalizing the questions for the census is 30 June 2019.

**SEXUAL HARASSMENT.** The U.S. Fourth Circuit Court of Appeals ruled that under Title VII of the Civil Rights Act, employers may be liable for not effectively addressing and stopping rumors of an alleged sexual relationship between a female employee and a male supervisor. The ruling maintains that sex discrimination includes entertaining the stereotype that women’s sexuality is of greater value than their merit.

The case was presented to the federal appeals court in Richmond, Virginia, after Evangeline Parker sued her former employer for sex discrimination and retaliation after a competing male subordinate started a rumor that her promotion was due to a sexual affair instead of her hard work.

Although the rumor was false, it spread throughout the warehouse where Parker worked for six weeks—sometimes with assistance from the highest-ranking manager at the warehouse, Larry Moppins. Moppins allegedly treated Parker with hostility and less respect, while coworkers were openly hostile because of the gossip.

Parker filed sexual harassment claims with Reema’s human resources department against both Moppins and the rumormonger.

In mid-May, the rumormonger complained to human resources that Parker was creating a hostile work environment. The department ordered Parker to stay away from the employee without issuing similar restrictions on the rumormonger, allowing him to remain in her work area to distract the employees she managed while he allegedly stared and laughed at her.

Although Parker complained to her superior and human resources about the rumormonger’s continuing hostile behavior, the behavior was not addressed, “exacerbating Parker’s experience of a hostile work environment,” according to court documents.

Approximately one month after that last complaint to human resources, Parker was fired in May 2016 during a meeting with Moppins, human resources, and Reema’s in-house counsel.

Disagreeing with the Fourth Circuit’s ruling, the federal court found that Parker adequately alleged a hostile work environment for sex discrimination. “These facts in combination—the spreading of a rumor rooted in base stereotypes about female professionals, plus Parker’s disparate treatment compared with members of the opposite sex—fairly permit the inference that Parker was treated with less dignity because she is a woman,” Judge Albert Diaz wrote in his decision.

---

**ISSUE:** Sexual Assault  
**BILL:** Senate Bill S2440 (19R)  
**VENUE:** New York  
**STATUS:** Enacted  
**SIGNIFICANCE:** Pauses the statute of limitations for criminal and civil prosecution for sexual offenses committed against children, so the clock does not begin to run until the victim turns 23.
Judge Paul Niemeyer added that Parker’s allegations supported her harassment claim since her experience “was severe or pervasive such that it altered the conditions of her employment and created an abusive atmosphere.” He also noted that the harassment was at times “physically threatening.”

“That this harassment came from Parker’s supervisor made it all the more threatening,” Niemeyer wrote. (Parker v. Reema Consulting Servs., U.S. Fourth Circuit Court of Appeals, No. 18-1206, 2019)

H.R. 1140, or the Rights for Transportation Security Officers Act, would offer TSOs not only full collective bargaining rights, but also chances to effectively raise issues in disputes to an independent third party for an impartial resolution. It would also make the officers subject to the General Services Administration’s wage system, which is the primary wage system for federal employees. TSOs comprise more than 70 percent of the administration’s workforce. They have labor union representation but due to limitations imposed by the TSA are denied certain privileges. The bill also includes protections so officers’ pay is not decreased due to the transition of the personnel system.

The bill was reintroduced after the latest partial U.S. government shutdown, during which TSOs—considered “essential” personnel and required to work without pay during lapses in appropriations—worked for 35 days.

Due to missed paychecks during the lapse in appropriations, some officers took second jobs, relied on food banks and charities, or left the TSA for paid employment.

According to Lowey, the legislation would aim to not only grant additional workplace rights, but also improve the nation’s security by retaining experienced officers with better morale.

New York City RACIAL DISCRIMINATION. The New York Commission on Human Rights issued new guidelines on 18 February, outlining that segregating people based on their hair or hairstyles is a type of racial discrimination.

The New York City Human Rights Law (NYCHRL) safeguards people dealing with racism, especially through hair-based discrimination. “Anti-Black bias also includes discrimination based on characteristics and cultural practices associated with being Black, including prohibitions on natural hair or hair-styles most closely associated with Black people,” the commission said.

Employers cannot legally discriminate or dictate how New Yorkers style their hair, according to the new guidance. Instead, such employees can maintain natural hair or other hairstyles linked to their cultural, ethnic, or racial identities. “Grooming or appearance policies that generally target communities of color, religious minorities, or other communities protected under the NYCHRL are also unlawful,” the commission wrote.

The guidance allows that employers might have legitimate health or safety concerns regarding hairstyles; however, alternative methods to addressing these concerns should be considered before levying a ban or restriction on hairstyles.

The law closely follows an investigation into discrimination accusations
from employees of several businesses in Manhattan, Queens, and the Bronx.

Recent guidance from the Equal Employment Opportunity Commission runs parallel to the NYCHRL, explaining that “hair texture” is a protected racial attribute and that related restrictions are a kind of prohibited discriminatory stereotyping.

REGULATIONS

SEXUAL MISCONDUCT. The Nevada Gaming Commission fined casino magnate Steve Wynn’s former company a record $20 million for failing to investigate sexual misconduct claims against Wynn.

The gaming regulators penalized Wynn Resorts Ltd. at the conclusion of an investigation into misconduct claims made prior to Wynn’s resignation from the company in 2018. Wynn reportedly harassed or assaulted several women. Regulators allowed the company to retain its gambling license.

The commission froze Wynn’s state casino license.

One of the commissioners said the issue concerned the failure of a “corporate culture.” Wynn denied all allegations made against him, and sold his company shares. However, Wynn Resorts confirmed that several former board members and executives were aware yet failed to investigate the claims, including one where Wynn paid $7.5 million to a former employee who alleged he raped her, resulting in a pregnancy.

Massachusetts gambling regulators opened a similar investigation into Wynn Resorts, looking into whether to permit the company to operate a roughly $2 billion casino resort scheduled to open in June 2019. The Massachusetts Gaming Commission is not evaluating the truth or falsity of the allegations against Wynn, but the company’s response to the allegations, as an indicator of corporate governance. A company settlement is pending in the state.

This column should not be construed as legal or legislative advice.
SEGCOL SCHOOL GUARD BOOTHs

B.I.G. Enterprises, Inc., recently manufactured new enclosures for St. Mary’s, a K-8th grade private school, providing perimeter security and access control as well as a secure location for school security guards. The booths present a visual deterrent for would-be attackers and are placed at every entry to the campus. These prefab units are built to meet all state codes, include the most recent energy codes, and ship as a complete one-piece unit ready for an easy installation. The booths include modern features such as all galvanized steel construction and a coated roof that offers a solar reflective index of 95 or greater.

MERGERS & MOVES

NSI Industries, LLC & Platinum Tools
NSI, an electrical and control products provider, merged with the datacom producer to expand its product portfolio and market reach.

NTT Security Corporation & Whitehat Security
NTT signed a definitive agreement to acquire the privately owned application security provider.

DOYLE SECURITY SYSTEMS & COMMERCIAL INSTRUMENTS & ALARM SYSTEMS (CIA)
Doyle, a regional provider, purchased CIA customer accounts, expanding the company’s scope in New York state.

FLIR SYSTEMS & ENDEAVOR ROBOTIC HOLDINGS, INC.
FLIR becomes a leading provider of unmanned aerial and ground solutions to support military, public safety, and critical infrastructure missions.

AWARD
The Hazardex Awards program, part of the annual Hazardex Conference and Exhibition, awarded the Personnel Protection Technologies (PPT) Innovation Award to Oncam’s Evolution ExD Explosive Environment Camera Range for the best innovation in PPT equipment to improve safety within the process and high hazard industries.

ANNOUNCEMENT
IXP Corporation authored a new industry white paper, NG911 & FirstNet: Emergency Communication Centers Provide the Critical Link. The report explores how 911 communication centers can successfully navigate Next Generation 911 technologies and the FirstNet public safety broadband network and its users.

PARTNERSHIPS
CYBERSECURITY
AbedGraham and BridgeHead Software coauthored a white paper, Legacy Applications: A Healthcare Cybersecurity Nightmare, which outlines the cyber risks and consequences of running vulnerable legacy systems.

CLOUD SURVEILLANCE
The South Grand Community Improvement District in St. Louis, Missouri, is using Genetec Inc.’s Stratocast cloud surveillance to reduce license plate theft and collaborate with the local police department.

INTERNET OF THINGS
The Kudelski Group’s IoT security platform will integrate into IDEMIA’s DAKOTA IoT and other solutions for combined network connectivity management and IoT security.
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>
<th>CIRCLE #</th>
<th>PAGE #</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>Ameristar Security Products</td>
<td>07</td>
<td>Detex Corporation</td>
</tr>
<tr>
<td>05</td>
<td>AMICO</td>
<td>06</td>
<td>G4S</td>
</tr>
<tr>
<td>09</td>
<td>Avigilon</td>
<td>12</td>
<td>GAI-Tronics Corporation</td>
</tr>
<tr>
<td>17</td>
<td>Brownyard Group</td>
<td>01</td>
<td>SecurAmerica</td>
</tr>
<tr>
<td>07</td>
<td>Detex Corporation</td>
<td>10</td>
<td>Special Response Corporation</td>
</tr>
<tr>
<td>24</td>
<td>DSX Access Systems, Inc.</td>
<td>08</td>
<td>TSCM America</td>
</tr>
</tbody>
</table>

ADVERTISERS ONLINE

<table>
<thead>
<tr>
<th>Ameristar Security Products</th>
<th>esri</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMICO</td>
<td>G4S</td>
</tr>
<tr>
<td><a href="http://www.amicosecurity.com">www.amicosecurity.com</a></td>
<td><a href="http://www.g4s.us">www.g4s.us</a></td>
</tr>
<tr>
<td>Avigilon</td>
<td>GAI-Tronics Corporation</td>
</tr>
<tr>
<td><a href="http://www.avigilon.com">www.avigilon.com</a></td>
<td><a href="http://www.gai-tronics.com">www.gai-tronics.com</a></td>
</tr>
<tr>
<td>Brownyard Group</td>
<td>SecurAmerica</td>
</tr>
<tr>
<td><a href="http://www.brownyard.com">www.brownyard.com</a></td>
<td><a href="http://www.securamericallc.com">www.securamericallc.com</a></td>
</tr>
<tr>
<td>Detex Corporation</td>
<td>Special Response Corporation</td>
</tr>
<tr>
<td><a href="http://www.detex.com">www.detex.com</a></td>
<td><a href="http://www.specialresponse.com">www.specialresponse.com</a></td>
</tr>
<tr>
<td>DSX Access Systems, Inc.</td>
<td>TSCM America</td>
</tr>
<tr>
<td><a href="http://www.dsxinc.com">www.dsxinc.com</a></td>
<td><a href="http://www.tscmamerica.com">www.tscmamerica.com</a></td>
</tr>
</tbody>
</table>
MARKETPLACE

Adding another critical weather intelligence product to its portfolio, BARON announced Telematics for Public Safety, which uses accurate, patented technology to help organizations keep employees, students, patients, or customers safe. The product can generate highly accurate road weather condition data using basic weather information, cross-referenced with proprietary algorithms and other data inputs. This technology allows organizations to access advanced weather forecasting tools, delivering alerts tied to their immediate location, and makes staying informed easy and quick, using pre-interpreted information. Telematics for Public Safety is tailored for public schools, hospitals, government agencies, and outdoor venues, ready to integrate into any company’s apps or software.

BOON EDAM, INC., announced the launch of an updated Turnlock full-height turnstile that offers increased performance and an improved experience for users and installers. The update focused on the design of the speed control mechanism and the overall construction of the turnstile’s top channel, providing improved rotation action while minimizing the force needed to push the rotor, resulting in a quiet and smooth user experience. The optional emergency backup battery lasts twice as long as before, keeping a turnstile working in case the power goes out; the coverage period has doubled from two hours to four hours of protection.

PRINCETON IDENTITY INC. announced the deployment of its Biometric Conex, designed to assist customers with quick and accurate personnel authentication for campuses and facilities. The Conex—a 20-foot-long standard shipping container outfitted with on-the-move facial, iris, and fingerprint biometric capture technology—can be operational in less than 24 hours. The container’s combination of patented authentication technology and portable configuration gives organizations flexibility to deploy these authentication units anytime, anywhere. The multimodal biometric, high-throughput system offers more secure rapid personnel authentication, with features including rapid enrollment of personnel, mobile multimodal personnel identification, self-contained or networked configurations, support for large personnel database configurations, and more.
PERSONAL PROTECTION

SENSTAR CORPORATION introduces the Flare personal protective device (PPD) compact, ideal for support and administrative staff in institutional environments. A new, more compact version of its Flare Real-Time Locating System (RTLS) PPD, Flare provides a sleeker option for staff in high-threat environments, offering a smaller device that can be worn in several ways, including on a lanyard, while still determining a user’s location. When the user activates the PPD, it emits an RF signal detected by a sensor network concealed throughout the facility and immediately locates duress alarms, displaying the location, status, and identity of the PPD. Flare operates in protected frequency bands that use dedicated spectrum, avoiding potential interference.

VISITOR KIOSK

VISITOR PASS SOLUTIONS launched a time-saving kiosk version of its visitor management software, eVisitorPass. The touchscreen application enables visitors to self-register into an organization’s building using a driver’s license reader, which automatically captures the name and photo; those lacking a license can instead type in their name and take a photo. The kiosk then sends the information to a printer, where an administrator issues the badge. The eVisitorPass Kiosk comes in two models—free-standing and tabletop—and both include a one-year software subscription, a driver’s license reader, a thermal printer, and a supply of visitor badges that change color when they expire to prevent unsanctioned reuse.

DVR ENCLOSURE

VIDEO MOUNT PRODUCTS announced its DVR-LB1 DVR Lockbox, designed to protect DVRs in settings that may be prone to theft or vandalism. As expensive technologies and equipment, including DVRs, find homes in more commercial and professional settings, additional security measures are required to ensure these electronics are not harmed or stolen. Features of the 21 x 21 x 8-inch lockbox include a fan for additional ventilation, interlocking lift-off lid, key locked hinging front door, and a black powder-coat finish.
SECURITY MANAGEMENT

VANDERBILT INDUSTRIES is partnering with ALLEGION US to enhance facility protection. Integration of Vanderbilt Security Management System software with Allegion’s Von Duprin remote undogging and remote monitoring options allows improved lockdown and remote monitoring functionality, especially for schools. Users can now remotely monitor and lock down secondary perimeter doors with the touch of a button in the event of an emergency. The Vanderbilt SMS system can manage alarms, photo ID badging, visitor management, elevator control, offline and online locks, advanced reporting, and lockdowns from its intuitive platform.

PASSWORD MANAGEMENT

Expanding its portfolio to include a self-service password management solution, IVANTI announced its Password Director. IT organizations can quickly and easily empower end users to resolve their own password resets by providing them with secure 24/7 access to a number of automated, self-service password reset options. End users can reset their passwords or unlock their accounts quickly and securely from the convenience of their Windows pre-login screen, a self-service Web portal, or a mobile app—without contacting the service desk—and therefore free up a considerable amount of IT’s time for better use, while keeping end users productive.

FIRE COMMUNICATOR

NAPCO SECURITY TECHNOLOGIES, INC., introduced StarLink Fire LTE Universal Commercial Fire Cellular Communicators, which are now available with Verizon LTE service for reliability and longevity. Each unit can replace two FACP POTs landlines for cellular reporting of any brand fire alarm system. Panel-Powered Technology eliminates power supplies to buy, install, and pipe, so the communicators can be installed in less than 15 minutes. Signal Boost circuitry and precision LTE twin antennas ensure greater range and reliability, maximizing signal acquisition and null-avoidance, receiving signals simultaneously on both antennas.

POWER DISTRIBUTION

MIDDLE ATLANTIC PRODUCTS now offers the High Power DC Distribution solution, solving installation challenges posed by powering numerous components with similar voltages. Part of the DC Power Distribution family, the new 200W and 300W models provide high current capacity to up to 24 devices, maximizing the same voltage in a single unit, or splitting between 12V and 24V. Not only do DC Power Distribution solutions remove space-consuming, unreliable wall warts and provide maximum power, they also increase system efficiency, saving energy. The solution’s AC input and DC outputs provide multilevel protection, and built-in individual redundancy ensures maximum uptime, while a supported input voltage range of 100-240VAC, 50/60 Hz provides additional design flexibility for international applications.

SMART BUILDINGS

HONEYWELL launched its Connected Buildings technologies, aiming to minimize response times and eliminate human delays during critical situations. The products help commercial buildings detect threats early, respond to incidents faster, centralize decision making, and allow management from anywhere. These solutions are part of Honeywell’s Connected Buildings portfolio, which includes MAXPRO Cloud and ProWatch, keeping people and property safe. Recent additions to Honeywell’s Commercial Security portfolio include NetAXS 123, Performance Series, VISTA, equiP Series, WIN-PAK, and Vindicator.
FREE PRODUCT INFORMATION

USE YOUR SMARTPHONE AND SCAN THE QR CODE TO REQUEST INFORMATION ON ANY AD IN THIS ISSUE

SECURITY MANAGEMENT
GETTING TO KNOW

JAIME P. OWENS, CPP, IS SECURITY BRANCH SUPERVISOR FOR THE PANAMA CANAL. HE IS A MEMBER OF THE ASIS INTERNATIONAL BOARD OF DIRECTORS AND THE GLOBALIZATION TASK FORCE.

Q. What security issue do you believe is being overlooked?
A. I strongly believe that security is science, art, and philosophy. Perhaps the philosophical part has been overlooked.

Q. A mentor who inspired you?
A. There are many, but Alex Omar Garrido comes to mind. He was the first CPP in Panama and my mentor as I prepared to become a CPP.

Q. What is your proudest moment or accomplishment?
A. When I was elected as the first Latin-American member of the Board of Directors of ASIS International.

Q. Your favorite ASIS moment?
A. There are so many. The foundation of the Panama Chapter, the first certification exam in Panama, and announcing that certification exams would be given in Spanish.

Q. What does ASIS mean to you?
A. ASIS is critical from a security knowledge and networking standpoint. It provides the educational foundation necessary for me to keep building my career.

Q. What book/movie/play title describes your life?
A. I was fortunate to grow up around many books at home. One of the best ones is Og Mandino’s The Greatest Salesman in the World.
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.
INTEGRITY. QUALITY. RELIABILITY.

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

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

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

DSX STANDARD SYSTEMS FEATURES INCLUDE:

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

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

For product info #24 securitymgmt.hotims.com