

SOLUTIONS FOR ENABLING AND ASSURING BUSINESS

SEPTEMBER 2020

SECURITY

THE

Most Influential People in Security

2020

INSIDE

Goodbye and Thank You p. 10

Securing Houses of Worship p. 50

You've Been Hacked – Now What? p. 58



SecurityMagazine.com

@SecurityMag

A bnp Publication
media



Wisenet 7

System on Chip (SoC).

— Excellence Through Innovation.



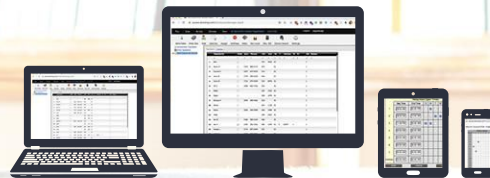
At the heart of Hanwha Techwin's new product development is the Wisenet 7 System on Chip (SoC). Designed in-house and built in Korea, Wisenet 7 is our most technology-intensive and feature-rich chipset. From its enhanced image quality and total cybersecurity to unprecedented user convenience and operational efficiency, Wisenet 7 delivers end-to-end intelligent video surveillance capabilities today...and tomorrow.

HanwhaSecurity.com

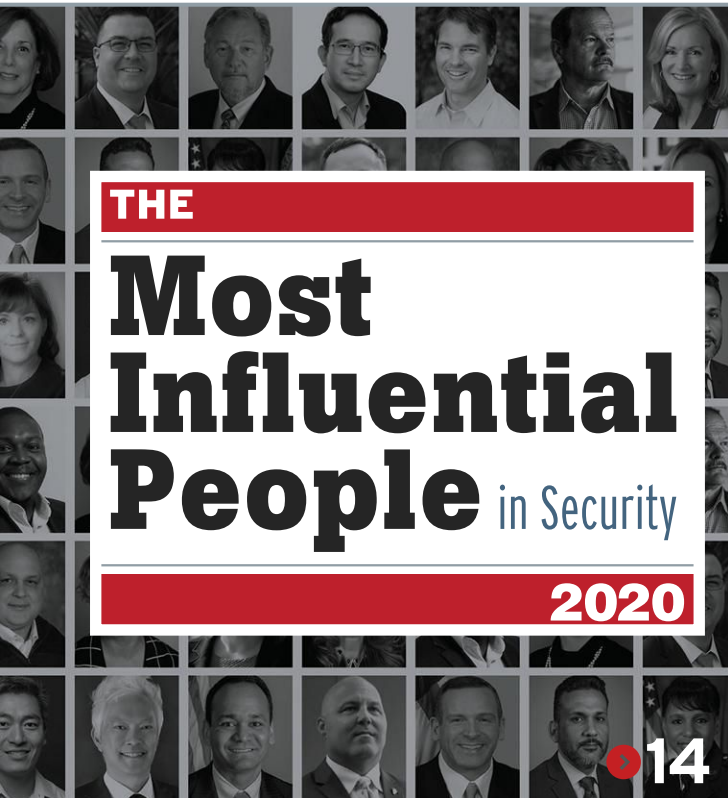
Cloud Programming Designed to Fit Your Life, (and whoever you're working with these days)

DKS Cloud Programming gives you the ability to program, manage and control your DKS Entry System on any computer, tablet, or smartphone from anywhere you have an internet connection. The way the world works is changing, and so have we. Discover work freedom with Doorking's Access Solutions.

Works across all devices
and operating systems.



FIND YOUR SOLUTION AT doorking.com/cloud



THE

Most Influential People in Security

2020

14

14 SPECIAL REPORT The Most Influential People in Security 2020

Security magazine announces 22 top security executives and industry leaders who are positively impacting the security field, their organization, colleagues and peers and the national and global security landscape. What are their career paths, goals, accomplishments and how can others follow in their footsteps?

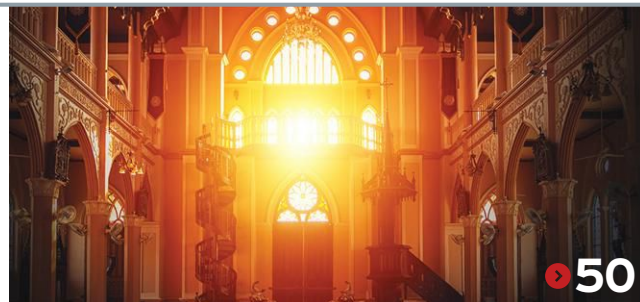
By Maria Henriquez

FEATURES

50 ENTERPRISE SERVICES Communal Efforts are the Way to Better House of Worship Security

Faith-based institutions need to be welcoming and inclusive with their duty of care to provide a safe space for worship, even with constraints on safety and security budgets in a non-profit environment.

By Robert Graves



50



58

58 CYBERSECURITY

You've Been Hacked - Now What?

If you're reading this article because of the headline, you're in trouble my friend. But, if you've done your job correctly, you will never ask "now what?" when such an incident occurs, because you'll already have an incident response plan in place that prescribes exactly what you need to do.

By Brian Wrozek

62 CYBERSECURITY

Get to Know the Standards Advancing Cybersecurity

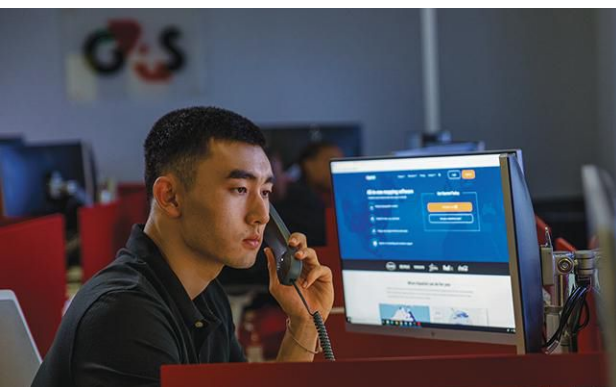
There are currently a multitude of different standards and regulations to address the urgent need to secure our connected world, yet it's time to create a unified global conformance assessment.

By Max Wandera

67 PRODUCT SPOTLIGHT

Surveillance for Airports/Seaports

Enhanced analytics, intrusion detection, broad surveillance, access control, facial recognition – are a few of the solutions explored here to help with airport and seaport applications.



You're working 6 feet apart. We're working around the world.

As social distancing changes the way we live and work, G4S can help. Whether you need to secure an empty facility or building, manage the flow of visitors and employees to your office, or need the additional support of security officers, we are committed to working closely with you.



Your trusted security advisor. | 888-645-8645 | www.G4S.us

RISK CONSULTING

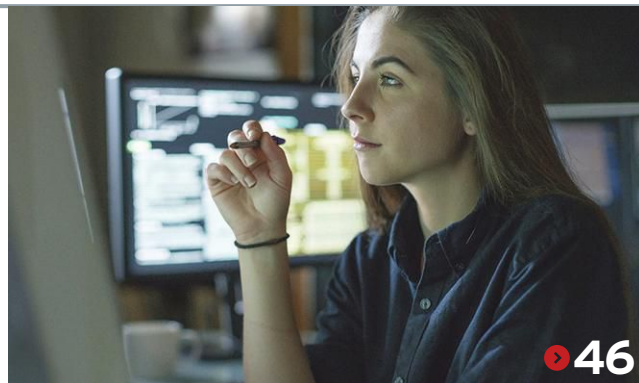
SOFTWARE & TECHNOLOGY

SYSTEMS INTEGRATION

SECURITY PERSONNEL

© 2020 G4S. All Rights Reserved.

Inside



► Columns

10 Security Talk

Goodbye and Thank You

By Diane Ritchey

46 Career Intelligence

Security Careers in Investigations

By Jerry Brennan

48 Leadership & Management

The Unifying Power of Security

By Michael Gips

56 Cyber Tactics

It's Coming: National Cybersecurity Awareness Month

By John McClurg

65 Education & Training

Derailing Ransomware 2.0 Requires a Little Trickery

By Carolyn Crandall

► Departments

12 Global News & Analysis

Security executives on the move!

Which industry leaders have recently begun new roles?

69 Classified Advertising

69 Advertising Index

69 Calendar of Industry Events



GET SOCIAL / with *Security Magazine*



Are you following *Security* on Facebook, Twitter, YouTube, and LinkedIn?
It's the easiest way to stay in touch with us and to see what we are doing.

SECURITY ADVISORY BOARD

Advising editors on topics and trends.

Dean Alexander

Professor of Homeland Security
Western Illinois University

Guy Grace

Manager, Security and Emergency
Planning Littleton (Colo.) Public
School District

Jeff Hawk, MSA, CPP, PEM

Director, Public Safety
and Police Authority Services
Memorial Healthcare

Jeff Karpovich, CPP & CHPA

HPU Security Chief &
Transportation Director

W. Barry Nixon, SPHR

Executive Director
National Institute for the
Prevention of Workplace Violence

Karl Perman

President
CIP CORPS

Jim Sawyer

Director, Security Services
Seattle Children's

Bryan Warren

Director of Corporate Security
Carolinas HealthCare System

MORE CONTROL, LESS CONTACT

50% Off
First-Year
Subscription
of Mobile IDs



LEADING AN ECONOMIC RECOVERY REQUIRES A FASTER AND SAFER RETURN TO THE WORKPLACE

As people return to their workplace, they will expect to see more rigorous cleaning and disinfection routines, frequent hand washing and sanitizing, minimal use of shared surfaces, and **increased use of touchless access control technologies.**

REDUCE ANXIETY AND ENABLE A SAFE RETURN WITH 50% OFF YOUR FIRST-YEAR SUBSCRIPTION OF MOBILE IDS.

- Minimum order increment of 20 Mobile IDs
- Promotion ends December 31, 2020 (not valid for renewals)

Learn More or Request a Free Consultation
hidglobal.com/mobile50



➤ **Publisher/Sales Team**

Gary Merrill, Publisher, East Coast U.S.
(248) 786-1247 • Fax: (248) 502-2104
merrillg@bnpmedia.com

Kent Beaver, Regional Sales Manager
(310) 927-4475 • Fax: (310) 474-8970
kent.beaver@verizon.net

Ben Skidmore, Regional Sales Manager
(972) 587-9064 • Fax: (972) 692-8138
ben@partnerspr.com

Jackie Bean, Regional Sales Manager/
Classified Sales Manager
(215) 939-8967
beanj@bnpmedia.com

India, Shivaji Bhattacharjee, Information
and Education Services Pvt. Ltd
iesdelhi@bol.net.in,
bh.shivaji@gmail.com

Israel, Asa Talbar, Talbar Media,
talbar@inter.net.il

Korea, Young-Seoh Chinn,
JES Media Inc., jesmedia@unitel.co.kr
Pacific Rim (except Korea), Arlen Luo,
NewSteel Media, nsmchina@126.com

**For subscription information or service,
please contact Customer Service at:**
Phone: 800-952-6643 or Fax: 847-763-9538
Email: security@omeda.com

➤ **Editor in Chief**

Diane Ritchey • (248) 833-7342
ritcheyd@bnpmedia.com

➤ **Associate Editor**

Maria Henriquez • (847) 405-4079
henriquezm@bnpmedia.com

➤ **Art Director**

Mike Holmes • (248) 786-1712
holmesm@bnpmedia.com

➤ **Production Manager**

Lyn Sopala • (248) 786-1641
sopala@bnpmedia.com

➤ **Reprint Manager**

Stacey Hurley
hurleys@bnpmedia.com

➤ **Directory/Buyers Guide**

Carolyn Perucca • (248) 244-6474
peruccac@bnpmedia.com

➤ **Trade Show Coordinator**

Gina Gjonaj • 248-244-1286
gjonajg@bnpmedia.com

➤ **Audience Marketing**

Christina Roth - Audience Marketing Manager
Lauren Atsalakis - Senior Integrated Media Specialist

➤ **List Rental**

Please contact your sales rep.

➤ **Editorial Offices**

155 Pfingsten Road, Suite 205, Deerfield, Illinois 60015
(847) 205-5660
security@bnpmedia.com

➤ **Corporate**

Chief Experience Officer: Darrell Dal Pozzo
Human Resources & Information Technology Director:
Rita M. Fournia
Production Director: Vincent M. Miconi
Finance Director: Lisa L. Paulus
Creative Director: Michael T. Powell
Clear Seas Research Director: Beth A. Surowiec
Chief Event Officer: Scott Wolters

➤ **Single Copy Sales**

www.securitymagazine.com/scs

www.SecurityMagazine.com

SECURITY



*Helps People Succeed in
Business with Superior
Information*

Learn & Earn

Earn free CEUs at ce.securitymagazine.com

Earn all of your continuing education credits free online through *Security's* Continuing Education Center at ce.securitymagazine.com.



Workplace Violence Prevention in Ambulatory Care Centers & Physician Offices

- *Develop a meaningful violence prevention education program*
- Sponsored by Accent Distributing, Dataminr, Everbridge, Hanwha, HID, and Johnson Controls

Earn: 0.1 IACET CEU; 1 EDAC CEU; may be eligible to receive Continuing Professional Education credit or CPEs toward ASIS re-certification



Mitigating Human Trafficking in the Hotel and Hospitality Industries

- *Best practices for creating an environment that is inhospitable to human trafficking*
- Sponsored by Accent Distributing, dormakaba, Everbridge, HID, and Salient Systems

Earn: 0.1 IACET CEU; may be eligible to receive Continuing Professional Education credit or CPEs toward ASIS re-certification

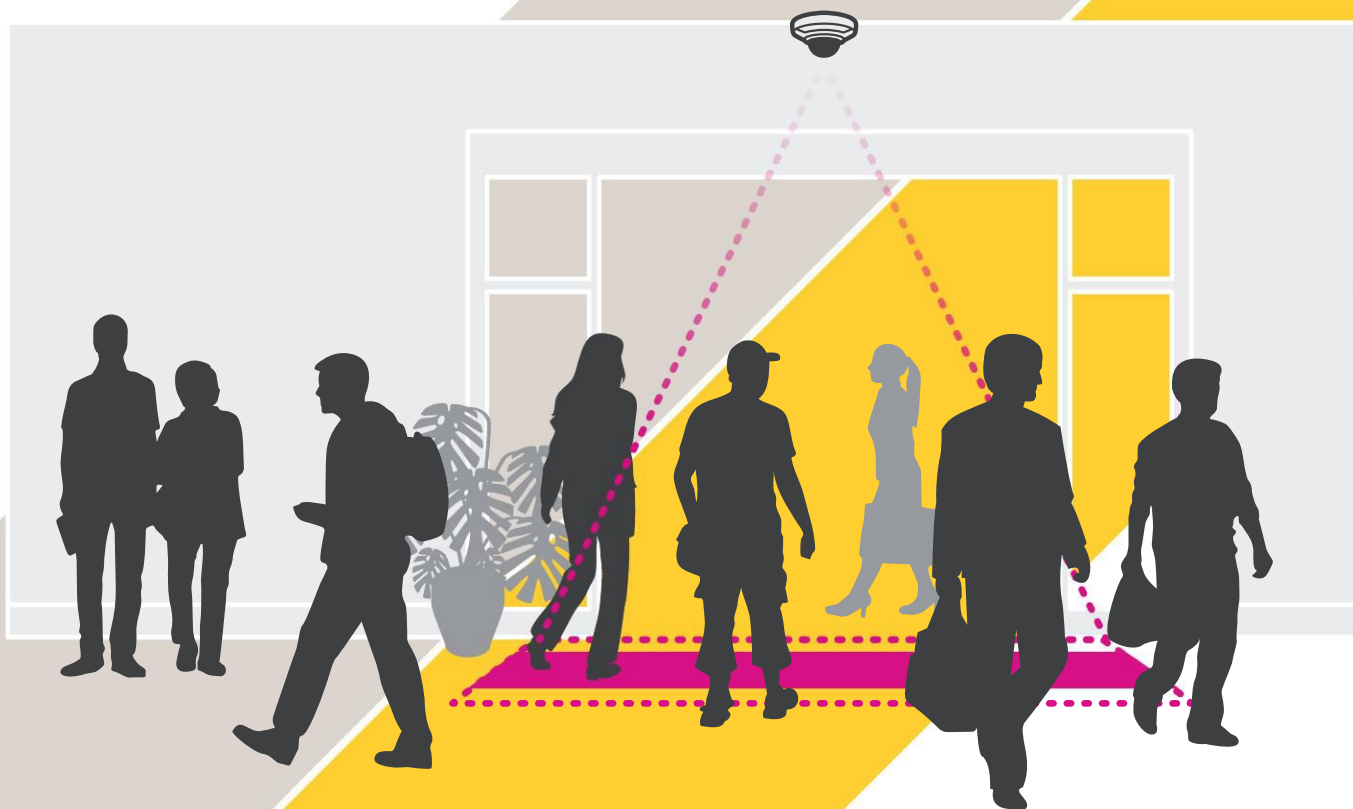
Courses are approved by the International Association for Continuing Education and Training (IACET) to offer continuing education credit participants completing these courses may be eligible to receive Continuing Professional Education credit or CPEs toward ASIS re-certification. Simply view the webinars or read the articles and complete the short quizzes to earn your credits. Most states accept IACET credits for professional continuing education requirements. Check your state licensing board for all laws, rules and regulations to confirm.

You can access these and many other continuing education courses on the Engineering + Mechanical Systems Continuing Education Center at ce.securitymagazine.com.

CONTINUING
EDUCATION
C E N T E R
ENGINEERING + MECHANICAL SYSTEMS



Participants completing these courses
may be eligible to receive Continuing
Professional Education credit or CPEs
toward ASIS re-certification.



Accurately estimate occupancy levels at your premises.

AXIS Occupancy Estimator

How many is too many? As some facilities operate at a limited capacity, there is a need to know exactly how many people are present so social distancing guidelines can be followed. AXIS Occupancy Estimator is an edge-based solution that can (when coupled with Axis network cameras) provide facilities with real-time data on occupancy levels to help them better understand visitor patterns and maintain customer safety.

Check out all the features at:

www.axis-communications.com/sm/occupancy

Goodbye and Thank You

After 11 years, 135 columns and more than 250 feature articles and cover stories...it is time for me to say goodbye as Editor-in-Chief of *Security* magazine.

Eleven years in one role is a long time, yes, but I never really thought about it that way – I was busy pushing forward each day to deliver stories and content that I hope have helped you to mitigate risk in your organizations.



As an Editor-in-Chief, I have learned how to handle just about anything. In any given day, I've jumped from writing a cover story to posting on social media, to responding to emails from PR agencies, to consulting with my art director about the next print or digital edition, to moderating a webinar, or organizing a conference.

One thing I never learned, though, was how to write about myself, which includes any deep reflection about what the past 11 years have meant to me. Even as I write this, in early August, my thoughts are consumed by all of the things still left to do before I leave.

Each day at *Security* magazine, for me, has been filled with a sense of purpose, and it has been a privilege to live that commitment for the past 11 years. I have always placed much thought and importance on the work that we do and the words that we publish. There has never been a day when I have not felt the weight of the impact that our writing and reporting can have on your roles and the security industry as a whole. I have always strived to publish content that you could use to do your job better, and I hope that I have achieved that goal.

This year, especially, with COVID-19 affecting us all professionally and personally, I have

never been more proud of what you do each day to mitigate risk and to keep people, property and assets safe.

I want to thank all of you – every *Security* magazine reader who has taken the time to read my stories and to share your views and successes with me. What an honor it has been for me to communicate with you and the security industry at large the passion that you all have for your roles, why you do what you do and why you enjoy doing it.

Another reason that I've stayed in this role for so long is because of my colleagues – past and present. They include former publishers Mark McCourt and Chris Ward, current publisher Gary Merrill, former Editor-in-Chief Bill Zalud and current Associate Editor Maria Henriquez. Mike Holmes, my Art Director, and Lyn Sopala, my Senior Production Manager, are extremely talented individuals who made my

job easier every day. My sales team is the best in the industry – Jackie Bean, Kent Beaver and Ben Skidmore. It has also been a pleasure to work with the editorial team from sister publication *SDM* – Karyn Hodgson, Maggie Shein and Courtney Wolfe.

Thank you to all of the talented individuals at PR agencies who respected my deadlines and who sent me creative pitches, some that resulted in fun pieces to write and to share.

The good news is that I am staying in the security industry, as Marketing Director for Zenitel USA, which is a provider of intelligent communications systems, specifically, fully integrated communication platforms that include Intercom, Public Address and two-way Radio Systems. I am looking forward to seeing all of you at future ISC West, Security 500 and other industry conferences and events!

Goodbye, take care and see all of you soon! **SECURITY**

3 REASONS YOU SHOULD BE EXCITED ABOUT YOUR **NEW & IMPROVED** SECURITY DIGITAL EDITION!

1

BEAUTIFULLY RESPONSIVE READING EXPERIENCES

Enjoy our intuitive interface that allows you to read *Security* on your desktop as a digital replica or in our new Contents View, and on your phone as a scrollable series of articles.



2

INSTANT AUDIO

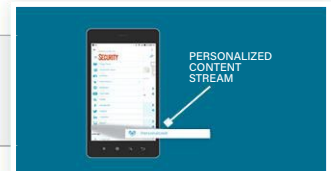
While our digital edition has always supported audio in numerous ways, never before has audio been put front and center in the reading interface – think instant audio! With Audio Articles, you can open your digital edition on your phone and simply click on the speaker icon to the right of an article to listen to it.



3

PERSONALIZED CONTENT STREAM

Using artificial intelligence, our digital edition can deliver a personalized stream of suggested content based on your reading behavior and preferences. In the Menu Bar of the digital edition you can find your own personalized content channel!



ON THE MOVE

5 New Security Executives Announced

Security executives on the move!

Which industry leaders have recently begun new roles?



Rodney Bond – Denmark Tech’s New Chief of Public Safety

Rodney Bond brings to Denmark Tech a wealth of experience as a law enforcement professional with more than 18 years of service in public safety on college campuses. Bond will be working closely with students to share his experiences and perspectives, while creating cooperative working relationships within a safe and secure campus. Congrats!



Sgt. Willie Halliburton – Portland State University’s New Chief of Campus Public Safety

Sgt. Willie Halliburton has worked for PSU since February 2016, following a 32-year police career. A graduate of Kansas State University, he’s held a variety of patrol and special assignment positions. He is active in the community and continues to promote the philosophy of community policing — the foundation of his entire career.

Halliburton served as a contributing member of the University Public Safety Oversight Committee. Congrats!



Steve Krameisen – American Portfolios Financial Services’ New CISO

Steve Krameisen has more than 35 years of FinTech experience. Early in his career, he served as the CIO and managing director for Nathan & Lewis Securities and Insurance General Agency to MetLife / New England Financial.

In his role as CISO, Krameisen leads information security and directs security initiatives around strategy, opera-

tions and the budget in the protection of AP’s enterprise information. Congrats!



Ben Carr – Qualys’ New CISO

As CISO of Qualys, Ben Carr is responsible for providing cybersecurity guidance and security strategies, leading the CIO/CISO Interchange and internal risk and security efforts and ensuring compliance across the world.

Previously, Carr was the CISO of Aristocrat and held executive strategic leadership roles at Cyberbit and Tenable. From 2012 to 2016, he was the senior director of Global Information Security for Visa, where he developed and led Visa’s global Attack Surface Management team. Congrats!



John A. Wilson – MITRE’s New VP and CISO

John A. Wilson is now vice president and chief information and security officer at MITRE. In this role, he is responsible for advancing MITRE’s intelligent enterprise and a broad, multi-year effort to transform MITRE’s business operations and systems.

Prior to joining MITRE in 1983, Wilson was director of consulting technology for Kana Software. Wilson is a member of the Gordon Institute’s Industry Advisory Council at Tufts University. He has served as an advisor or faculty member at Boston University, Daniel Webster College, New Hampshire College, and the Worcester Polytechnic Institute. Congrats! **SECURITY**



Have you recently changed roles?

We’d like to know! Email Editor-in-Chief Maggie Shein at sheinm@bnpmmedia.com or Associate Editor Maria Henriquez at henriquezm@bnpmmedia.com. For this month’s complete list, please visit www.securitymagazine.com

THE CHALLENGES OF YESTERDAY ARE NOT THE CHALLENGES OF TOMORROW

Allied Universal® is There for you™,
keeping you secure by staying
one step ahead of tomorrow's
growing and evolving threats.

Because it is when we are
fearless, humanity thrives.

aus.com



©2020 Allied Universal

ALLIED UNIVERSAL®
There for you.

THE

Most Influential People in Security

2020

Who is leading the way for enterprise security professionals? These 22 thought-leaders are making a difference.

By Maria Henriquez, Associate Editor

Security magazine is pleased to announce our 2020 Most Influential People in Security - 22 top security executives and industry leaders who are positively impacting the security field, their organization, their colleagues and peers, and the national and global security landscape.

These security leaders have been nominated by their colleagues and associates, and were chosen based upon their leadership qualities and overall positive impact on stakeholders, enterprises, colleagues, constituents and the general public.

This year's Most Influential is organized by the following categories: Corporate Security Executives, Cybersecurity, Government, Special Recognition and Associations.

Here you will find brief overviews of each honoree's career path, goals and accomplishments - often across both the public and private sectors - as well as advice for those security professionals looking to follow in their footsteps, including being a security generalist, investing in lifelong education, seeking mentors and more.

Our special appreciation goes to Jerry Brennan, who was a project partner on this report and provided subject matter expertise and research.

For a listing of past Most Influential People in Security honorees, please visit:
www.SecurityMagazine.com/MostInfluential



William P. Woods

Senior Director of Security
Intelligence
McAfee

CORPORATE SECURITY

As Senior Director of Security Intelligence at McAfee, William P. Woods leads the organization's Security Fusion Centers worldwide. The centers provide physical security for all McAfee employees, contractors and facilities; network security for all McAfee networks and cyber activities; proactive threat hunting teams; McAfee's Industrial Security programs; the Insider Threat Program; and Cyber Security Incident Response Teams. He also provides guidance to McAfee's global security teams who are responsible for protecting people, property, assets and critical data.

Prior to joining McAfee in 2017, Woods had a career lasting over 22 years as a Special Agent in the U.S. Federal Bureau of Investigation (FBI). He finished his career as an FBI Executive responsible for leading the St. Louis, Mo. Field Office, where he spearheaded multiple investigations, while supporting multiple cyber, counter-terrorism, counter-intelligence and criminal investigations.

With the FBI, he led technical investigations in the Operational Technology Division and was the Chief Security Officer for the Washington, D.C. Field Office. He also spent five years in the Critical Incident Response Group, where he hired, trained, assigned and coordinated special deployments for surveillance teams and worked investigations throughout the U.S.

According to Woods, a project he is most proud

of during his career at the FBI is the large-scale crisis and investigation involving the law enforcement shooting of Michael Brown in 2014, which led to the Ferguson, Mo. unrest, and thus sparked vigorous debate in the U.S. about the relationship between law enforcement officers and African Americans and the use-of-force law in Missouri and nationwide.

"This investigation was extremely sensitive with highly charged emotions from people with different views on what occurred and why," Woods

notes. "It became a highly publicized investigation with scrutiny up to the White House. Ultimately, I ensured the FBI investigation was thorough and unbiased, following the evidence regardless of the politics."

Before joining the FBI, Woods served as an Army National Guard pilot and officer; a former New York State Police - State Trooper; and

Company Commander in the U.S. Army Reserve. He is a graduate of the State University of New York at Buffalo. He has been married for over 20 years and has three children.

"Some of the best career advice I have received from mentors and friends, especially as it pertains to leadership in security/investigations, which often demands leadership under stressful circumstances, [is] be tough but kind, be confident but humble," Woods says. "These may sound contradictory, but they are not. Set high expectations for yourself and your teams and be honest about results. When dealing with people use common sense and common courtesy. My father told me, 'Treat people with the same courtesy and respect you would want them to show your mother.'"

"Some of the best career advice I have received from mentors and friends, especially as it pertains to leadership in security/investigations [is] be tough but kind, be confident but humble."



Mike Wanik, CPP, CBCP

Senior Director,
Corporate Security
United Therapeutics
Corporation

CORPORATE SECURITY

In 2013, Michael W. Wanik became the first Security Director for biotechnology company United Therapeutics Corporation, a firm that develops products and solutions for patients with chronic and life-threatening diseases. The company is headquartered in Silver Spring, Md., with additional facilities up and down the East Coast as well as other global locations.

At United Therapeutics, Wanik built a security program and culture from the ground up. He standardized, unified and created an identity provisioning system across all company physical locations in concert with the collapse of several different access control platforms into one, supported by two security operation centers.

As part of a continual improvement process, Wanik is now leading an interoperability initiative at Research Triangle Park (RTP) campus in Durham, N.C. in concert with the RTP Foundation, businesses within the 7,000-acre science park, and public sector partners. "I began reviewing calls for service to the park by law enforcement, EMS, Fire and others in 2018 after noting degradation in response times. We learned through our partnership with the public sector that their assets were stretched and thus that the park was not routinely patrolled or familiarized with by responders," Wanik says.

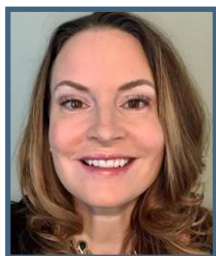
Shortly after he began his tenure at United Therapeutics, he became Chairman of "Security@RTP," a committee of RTP Foundation's Owners and Tenants Committee that shares knowledge and information between companies and law enforcement, regarding possible threats and related responses.

As Chairman, Wanik facilitates the communi-

cation to, coordination with, and response of Park companies and emergency management when safety for RTP's roughly 55,000 employees may be of concern. The initiative just launched is the RTP-Communications Network (CN), and it's currently in its pilot phase. The RTP-CN will bring select RTP security organizations together with public source partners through interoperability software that allows them to securely and privately share video, communications and mapping. Since the 7,000-acre park has no dedicated public safety resources yet, the platform will help in an easier transfer of data in an emergency situation between partners.

Previously, Wanik held executive roles at SSC Inc.; United Health Group; served in the U.S. Army; and taught law enforcement courses for Central Texas College Overseas in Stuttgart, Germany to armed forces members.

When asked what career advice he has for future security/law enforcement professionals, Wanik states that the current security landscape is one that is changing quickly. He explains, "Public and private organizations are experiencing extreme culture change, and this and ever-advancing technology will directly impact how we, in public and private organizations, will provide protective and investigative services. Law enforcement and the security professions will need to continue to strive to provide safe environments, deter criminal elements and act upon need as requested by others (to protect, detect, recover). Those that think rationally and critically, as well as utilize all the tools that are available to them will be the most successful. These tools don't singularly reside in a police or corporate security department but are in our extended community of relationships as well. These relationships always pay dividends and help solve issues in ways we don't instantly think of."



Kristine Raad

Director, Global Security
Owens Corning

CORPORATE SECURITY

Kristine Raad is the Director of Global Security for Owens Corning, a global building and industrial materials leader. She is responsible for developing and implementing Owens Corning's enterprise security strategy and has been a leader in transforming security operations across the organization. She has been pivotal in driving continuous improvement through technology innovation, business alignment and project delivery.

Raad previously worked in a variety of roles in both engineering and security during her more than 20 years of experience with General Motors (GM). During her tenure at GM, she was responsible for North American Regional Security, including oversight of security at more than 75 manufacturing and office sites throughout Canada, Mexico and the U.S. She also led the company's global security intelligence center, travel security, whistleblower hotline and global reporting programs. Raad had an assignment in Mexico, where she lived and worked for three years, implementing a security compliance program and managing investigations for the South America region.

Due to her success in security, Raad was selected for an inaugural leadership program at GM focused on developing skills to drive improvement and long-term change in organizational culture. She attributes this program with enhancing her ability to leverage problem-solving and leadership skills to drive continuous advancement of business objectives.

In addition, she is an active member of a number of security organizations including the International Security Management Association

(ISMA) and the Women in Security (WIS) Common Interest Council of OSAC. Raad serves on the ISMA Education and Benchmarking Subcommittees and is also a member of the WIS benchmarking team.

"Throughout my career, I have been presented with pivotal decision points that have had a profound effect on my career. The key for me has been to acknowledge the uncertainty these created, and to allow myself to embrace the opportunity and believe in my ability to succeed," she says.

Raad adds, "I began my career with General Motors as an engineer; however, when the opportunity arose to make a transition from engineering to corporate security, I jumped at the chance and embraced the challenge. At the time I didn't have experience in security, but I had raw ability, and the desire to dedicate myself to becoming a true security professional. To this day, I consider this decision to be amongst the best I have ever made. Similarly, when I made the move from General Motors to Owens Corning, I had a highly successful career but recognized the opportunity to challenge myself and grow professionally. I asked myself, 'If not now, when?' and knew the right answer was now."

Raad is most proud of leading a cross-functional team to develop and implement a Corporate Crisis Management program at Owens Corning. She says, "The timely development of the program, completed just prior to the 2020 global pandemic, positioned the organization to effectively respond to the crisis and to prioritize key actions to protect our employees and the business. While the circumstances that required the implementation of the plan were unfortunate, it has been gratifying to see the plan implemented successfully to the benefit of our workforce."



Mike Matranga

Executive Director
of Security and School Safety
*Texas City Independent
School District*

CORPORATE SECURITY

Mike Matranga is the Executive Director of Security and School Safety for the Texas City Independent School District (ISD), a public school district based in Texas City, Texas, serving 9,000 students.

Though there are many things he is proud of in his career, Matranga is most proud of developing the safety and security protocols at Texas City ISD. “I was hired fresh off the heels of the Parkland and Santa Fe Shootings, which I believe were the pivotal point in our society where the people of this great country started to rally together and demand answers, accountability and action, not only from their school officials, but our elected officials as well,” he notes.

“Thankfully, at Texas City ISD, Superintendent Dr. Rodney Cavness had the foresight to know education and security are separate and should always be constructed and applied by professionals in their respective fields. Though we need to understand the needs of educators and adapt to their environment when applying security tactics, techniques or procedures, they too should understand and value what we as security practitioners bring to the table.”

As a result, Matranga has forged a new path for school security, taking things further than any other Texas school district to mitigate security threats. Matranga and the security team have increased the ability to identify students or staff who may be in crisis; deployed threat assessment/CARE teams, based upon the National Threat Assessment Centers' guidelines; trained staff in tourniquet application; built an entire security computer-based training; and designed a robust access control system. In addition to installing

a mass notification system, Matranga installed a camera system using analytics and a biometric facial recognition system to use proactively.

“Of all the measures and initiatives we implemented, the absolute most important thing we have is our staff, who have the ability to make real change which no camera system will provide,” he says. “Simply teaching our staff how to identify pre-attack behavior, self-harm behavior and a person in crisis will always be what is most important. Secondly, having the resources and courage to intervene once those things are identified will keep individuals off the path to violence. We must never discredit the human element.”

Previously, Matranga served as a Special Agent with the U.S. Secret Service. He is the Owner and CEO of M6 Global Defense Group.

He says, “The law enforcement and security professions are among two of the most rewarding careers a service-minded person can enter. However, those who choose this path must understand by doing so, they accept being held to a higher standard. Their values, morals and ethics are what separate them from the rest of the civilian population; therefore, they must always lead. However, leading and being held to a higher standard does not mean being a doormat for those who would choose to weaponize another's commitment to being a public servant by thinking one should not have a voice because they wear a uniform. We must stand tall, be proud, always seek justice, righteousness, be unbiased, exercise fairness, and remember we must be the refuge others seek but can't find in themselves. At times in your life and career you'll be given a choice to be heard or be silent. Be the voice for coworkers who don't have the courage to speak up. That's what leaders do, lead!”

SPECO OFFERS 3 FACTOR AUTHENTICATION **THREE** ARE BETTER THAN **ONE.**

Factor #1
Facial Recognition

Factor #2
Credential & Reader

Factor #3
Temperature Reading
Panel with Face &
Mask Recognition

 **Access Granted!**

Your All-In-One Security Solution


speco technologies®
Giving You More.

Learn more at specotech.com



FOLLOW US AT
SpecoTechnologies



Jeff Hawk, MSA, CPP
Director, Public Safety and
Police Authority Services
Memorial Healthcare System

CORPORATE SECURITY

At Memorial Healthcare System in the City of Owosso, Mich., Jeff Hawk has laid the foundation and established a vision that guides the members and standards of the nationally recognized department, creating a “gold standard” in healthcare security. Prior to his arrival, Memorial Healthcare did not have a Public Safety Department.

Since Hawk joined, he has constructed the Public Safety department from the ground up and has been instrumental in the implementation, growth and development of Memorial Healthcare’s security risk management approach, along with their regimented training processes and technological capabilities. “Of all the training programs that we have developed, it is our firearms program that I believe is one of the most innovative and comprehensive around; and of creating leadership development and career ladder programs for my staff, including the impact they have had in driving recruitment, talent development and compensation strategies to modernize and make the security profession not just a job, but an actual career path,” Hawk says.

One of Hawk’s biggest passions is in protecting and serving others. “The security industry as a whole is one of the fastest moving, demanding and ever-changing arenas. It offers the opportunity to have a truly meaningful impact on others. It is a dynamic and exciting career path for the right person. For success, you must be passionate about being of service to others, resilient and tenacious in your approach, enjoy the challenge of change and have the ability to both inspire and influence others,” he says.

Over the years, he has developed a reputation for strong leadership; organizational development; a consistent ability to effectively deal with emerging security challenges; creativity in employing leading industry practices; and a knack for developing critical public and private partnerships. Hawk has accumulated numerous certifications and awards, including 2019 IFPO’s “Bill Zalud’s Memorial Award for Professional Excellence” special runner-up; 2017 *Campus Safety* magazine’s Director of the Year-Healthcare and runner-up in 2019. He is a former ASIS Chapter Chair, current ASIS Leadership, and management council member.

Previously, Hawk was a District Risk Manager for the Natrona, Wyo. County School District, where he built a security risk awareness culture to include overall direction of all loss control and prevention, emergency preparedness, fire and life safety, security operations, and an SRO program. He has also held executive CSO roles at the El Paso Water Utilities and Emergent BioSolutions, where beyond developing the program from its infancy stages to national recognition, he is most proud of driving and implementing a convergence strategy for an ever-expanding global operation. Hawk states, “the program’s growth, along with the organization’s trajectory during that same time, was truly monumental and will likely never be duplicated.”

He adds, “It is rewarding to be an ambassador, advocate and thought leader for our industry, as well as a leader of and mentor to the next generation of security professionals. I am especially proud of the men and women that I have had the privilege to lead, coach and mentor along the way. I have been fortunate to see many of them go on to positions of increased responsibility and become outstanding security ambassadors in their own right.”

Incredible!

ASTM M50 ***Portable*** Barriers & Bollards



Available now, you can set up certified ASTM M50/P3 rated portable barriers and bollards on concrete, asphalt, compacted soils or vegetation in 15 minutes or less to provide M50 stopping power. Your people are now protected from damage by a 15,000 pound (6804 kg) medium-duty truck going 50 mph (80.4 kph). Quick deployment, multiple configurations and, best of all, unrivaled security at the highest level!



See our full line of certified crash tested portable and fixed line of vehicle access control products at www.deltascientific.com.



Link M50 rated TB150 bollards together to create immediate protection for spans of 20 feet (6 m) or greater. TB150's contain and stop 1.2 million foot pounds of medium-duty truck.



Visit www.deltascientific.com for details and specifications.

GSA 47QSWA18D003B ▲ 1-661-575-1100 ▲ info@deltascientific.com



Kirsten Provence

Senior Manager, Supply Chain Security, Program Execution & Organizational Executive Strategy & Business Operations
*The Boeing Company,
Security & Fire Protection*

CORPORATE SECURITY

As the Senior Manager of Boeing's Supply Chain Security program, Kirsten Provence leads the team responsible for maintaining the security of Boeing's global supply chains and ensuring compliance with federal and international security requirements.

In addition, Provence leads Boeing's Security and Fire Protection (S&FP) Program Execution team, which ensures the deployment of standardized security services across the enterprise. She is also executive strategy leader for the S&FP organization and leads the development and delivery of the organizational strategic direction to enable cross-functional success.

Provence graduated from Western Washington University with a degree in Political Science – International Policy and obtained her MBA in Global Management. After spending time in the international trade industry and obtaining her U.S. Customs Brokerage License, she joined Boeing in 2001.

In addition to serving as a Governance Board member for the Supply Chain Risk Leadership Council, she also chairs the OSAC Women in Security Benchmarking subcommittee and is a member of the U.S. Department of Homeland Security (DHS) Critical Infrastructure Sector Coordinating Council. There, she aids in the identification, assessment, prioritization and protection of nationally significant manufacturing industries within the sector that may be susceptible to manmade and natural disasters.

"I have had the opportunity to work with many industry groups to identify and develop best practices of which I'm incredibly proud of. One area in particular was the U.S. Customs and Border Protection (CBP) Customs Trade Partnership Against Terrorism (C-TPAT) Program's recent initiative to revise the minimum-security criteria in order to ensure its members were responding to relevant and current threats. I was part of the subcommittee that was pulled together to work on these updates," Provence says. "This was

a massive effort, and I have applauded the program frequently for their commitment to engaging the community on this endeavor. The opportunity to work with experts from all aspects of the supply chain to identify current and future risks was nothing short of inspirational and innovative.

I feel like the outcome of that effort has had an astounding and positive impact on securing global supply chains and enabling the protection of the Homeland."

Throughout her career, Provence has learned that pursuing new opportunities outside of her comfort zone and seeking new ways to solve challenges has resulted in professional and personal growth. "During these times, I have found that I have built on each experience and have learned the most as a leader and security practitioner," she explains. "There have been many times where I may not have had all of the bandwidth I thought I needed to 'lean in,' but once I started, I was so energized by the innovation and connecting with new people that more bandwidth just seemed to appear."

Provence resides in Woodinville, Wash., with her family and their three-legged rescued Labrador retriever, Rebel.

"I have had the opportunity to work with many industry groups to identify and develop best practices of which I'm incredibly proud of."

THE ONLY THING YOU NEED TO IMPLEMENT YOUR NEW **MOBILE** **ACCESS CONTROL** SOLUTION



Just your smartphone's phone number.

(No post-credential management requirements.)

No portals. No private information. No unsecured credentials.
No jerry-rigged implementation. No hassles.

Made by Farpointe Data, the CONEKT® solution—potted,
mobile-ready RFID readers and companion credentials—is
only available through your favorite integrator.

1-408-731-8700
www.farpointedata.com


Farpointe Data®
Readers • Credentials

The OEM's global partner for premium RFID solutions



© 2020 Farpointe Data, Inc.



Mark Reed

Director of Support Services
*Martin Luther King Jr.
Community Hospital*

CORPORATE SECURITY

Mark Reed embodies the spirit of a security leader. Since he joined the Martin Luther King Jr. Community Hospital, he has fostered a collaborative team environment in support of operations and infrastructure. He spearheaded changes to the Hospital Preparedness Program and implemented a Quality Control Preparation Plan; coordinated Workplace Violence Program revisions; as well as established certification programs for the Security Department, resulting in a International Association for Healthcare Security and Safety (IAHSS) Program of Distinction Designation.

Reed says, "I am most proud of our Public Safety team being selected for the IAHSS Foundation Lindberg Bell for demonstrating outstanding healthcare security. We have been successful in implementing leading-edge security technologies while significantly improving our training and certification programs for staff which has shown a significant reduction in incidents."

As Director of Support Services, Reed's primary responsibility is to ensure a safe and secure environment for patients, staff and visitors. In addition, he oversees the security services, PBX, workplace violence prevention program, parking, investigations, emergency management program, and the Safety and Environment of Care departments.

Previously, Reed was security manager at Huntington Hospital, responsible for development and oversight of the security management program for the main campus, immediate surrounding properties and off-site facilities.

There, he oversaw inspection of the hospital and grounds to ensure safety and secu-

rity was maintained at all times; and evaluation, planning and development recommendations regarding facility access control and alarm systems, infant security monitoring, and safety procedures to eliminate or reduce unsafe and hazardous conditions.

He was also chief of security and shift supervisor/unit manager at CoreCivic and served in the U.S. Army Reserve as a Telecommunications Specialist and on Active Duty state in support of the Operation Iraqi Freedom in 2003.

Reed possesses a plethora of certifications and designations demonstrating excellence, such as Terrorism Liaison Officer Joint Regional Intelligence Center, FEMA Professional Development Series Certification, Disaster Preparedness for Hospitals and Healthcare Organizations, InfraGard Infrastructure Liaison Officer, IAHSS Supervisor Certification, and ACA Certified Correctional Manager.

In addition to his responsibilities, Reed is involved in several community and professional organizations, locally and across the nation, including Chair of the Safety and Security Committee for the Hospital Association of Southern California Security; as Board Member and LA/OC Chapter Chair of the International Association Healthcare Security and Safety; and as ASIS International Greater L.A., Calif. Chapter Vice-Chair. In 2019, he was recognized with an Outstanding Security Team OSPA award, presented at ASIS Global Security Exchange (GSX).

"For future security professionals, I would encourage them to always work towards learning and staying engaged. Professional associations offer valuable training, education and networking opportunities. They have been a key factor to staying innovative and allow the ability to discuss important technology, best practices and training with peers," says Reed.



The *FUTURE* of Multi-Tenant Security

You can now offer property owners a single, powerful system that combines the feature-rich benefits of an IP intercom with the versatility of a multi-tenant solution.

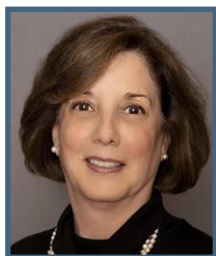
The IXG Series IP Multi-Tenant Video Intercom helps solve security communication challenges beyond any other intercom.



- *Easy to start small, expand at any time*
- *Cloud-based app (service fee will apply)*
- *All stations are PoE*
- *Touchscreen entrance panel*
- *Updates can be programmed remotely*
- *Physical video guard station (Sept 2020)*
- *Compatible with IX Series stations*

We encourage you to try before you buy! Look for the orange DEMO button on our website and fill out the brief form. Once you get the chance to demo—and adore—the IXG Series, you'll see firsthand how this system will impress your customers.

aiphone.com/SecMag_Sept



Margaret Levine

Vice President,
Corporate Security
Bridgestone Americas, Inc.

CORPORATE SECURITY

For the past 12 years, Margaret Levine has been VP of Corporate Security at Bridgestone Americas, a leader in tire and rubber technologies, in Nashville, Tenn. In addition to leading an enterprise-wide security program in identifying risks, reducing vulnerabilities and responding to crises across national and international locations, she also chairs Bridgestone Corporation's Global Working Group on Risk Management and Business Continuity.

At Bridgestone, the C-suite relies on Levine and the Corporate Security team to be an integral part of enhancing the company's brand and protecting its employees, as well as physical and intellectual assets. To meet those expectations, Levine relies upon in-house resources, in addition to outsourcing in areas such as her guard force, technology design and certain investigative work. She also relies on colleagues and data from the State Department's Overseas Security Advisory Council (OSAC) and the FBI's Domestic Security Alliance Council.

Outside of Bridgestone, Levine is a board member of the International Security Foundation and Chairs OSAC's Women in Security Council. She is the first woman to have served as president of the International Security Management Association.

Levine has had previous roles as deputy director of the Commission on Accreditation for Law Enforcement Agencies, and as senior advisor, Business & Operations Support and technical services manager at Mobil Oil. There, she managed executive protection, crisis management, risk and threat assessment, and security support to operations in high-risk non-U.S. locations.

After Mobil Oil, she moved on to Capital One

as director of global security and also led corporate security at Georgia Power Company, focusing on business strategy and proactive risk management. While there, she designed and implemented the company's first enterprise crisis management program.

From redesigning the FBI's Uniform Crime Report to building a global security department to leading security for Bridgestone Americas at the Rio Olympics, Levine has been part of many initiatives that have made a difference in the profession and the well-being of teammates and corporations where she has worked.

"One that stands out in particular is my role leading the design team for Mobil Oil's Shared Services business strategy for expertise functions. Our team created the process through which the security, medical, aviation, EHS, legal and government relations departments sold and delivered their services to company business units worldwide. At the time, I had worked at Mobil for only a couple of months – this was my first job in the private sector," Levine notes. "The assignment forced me to quickly learn the oil and gas industry, understand how Mobil operated its business and run a staff function like a business. I'm proud to have been a part of the effort that put Mobil in the forefront of companies transitioning to a shared services operating model."

To be successful, she believes that security professionals should understand the culture and the C-Suite of their organization, now and as it evolves, and have the flexibility to adapt. "It doesn't matter how talented you are, how much experience you have or how successful you've been. If you don't have the awareness and ability to change, your credibility and track record may be tarnished because the programs, problem-solving and communication style that worked in one organization or under the leadership of one CEO may not work in the new paradigm," she says.



Eric Sean Clay

Chief Security Officer
CoxHealth

CORPORATE SECURITY

Eric Sean Clay is Chief Security Officer at CoxHealth, a not-for-profit healthcare system based in Springfield, Mo., that comprises six hospitals and primary and specialty care providers in more than 80 clinics.

Under Clay's leadership, CoxHealth had the first three hospitals in Missouri to secure the IAHS's Program of Distinction recognition, the first in the state to issue NARCAN to its officers, to have a K-9 unit and to open a POST-certified law enforcement/healthcare security training center. He has increased the number of female and minority officers, as well as started a uniform allowance for officers, increased wages, created a succession plan with clearly defined expectations, and looked for ways to increase the caliber of officers.

Clay created CoxHealth's training academy, which offers more than 140 POST-certified classes for the organization's officers and law enforcement officers. He mandates all CoxHealth's officers to take IAHS basic, advanced and or supervisory level classes. Another area Clay has made an immediate impact is in the area of workplace violence on hospital staff and employees. Clay sent 21 employees to a defensive tactics instructor school, where de-escalation, team tactics and individual defense skills are taught. He also sent 60 officers to Crisis Intervention Team training to better assist staff and patients in emergency departments and psychiatric units.

During his career, Clay has worked for the St. Charles, Mo. Police Department, the Orlando, Fla. PD and the U.S. Federal Air Marshal's Service.

His career advice for future security and law

enforcement professionals is, "We currently live in a distressing time where people seem polarized and quick to express their outrage. People's unwillingness to treat others with respect and civility make the role of security and law enforcement professionals more difficult and all the more important. Nice matters, more than ever. As the first line of defense for your organization or community, you will have people question you. How you respond to this behavior is a choice. Try to accommodate others by putting yourself in their shoes. This will help you understand and appreciate their point of view. You don't have to agree with their position, or even like it, but understanding it will definitely benefit you as you carry out your responsibilities. In our field, there is a tendency for self-isolation. It's easy to develop an 'us vs. them' mentality. Try to avoid this. Rather than seeing problems as impediments to success, I would encourage you to view them as opportunities – to grow, improve things, or simply learn. Problems are inevitable. Changing your perspective forces you to constantly adapt and strengthen your problem-solving abilities."

Clay adds, "Albert Einstein famously said, 'I have no special talent. I am only passionately curious.' As a lifelong learner, I would encourage future security and policing leaders to have a natural curiosity. If you're always expanding your perspective and skills, you're going to be successful. That's not to say you have to know everything. Things change too rapidly for that. What worked yesterday won't always work tomorrow. However, you can take what you have learned and build upon that to help develop ideas that build upon what previously worked."

Editor's Note: At the time of publication, Clay will be VP of Security for Memorial Hermann in Texas.

**Paul Lanois**

Director, Technology,
Outsourcing and Privacy
Fieldfisher

CYBERSECURITY

Paul Lanois is Director of Technology, Outsourcing and Privacy at Fieldfisher, a European law firm with practices in many of the world's dynamic sectors. Lanois provides guidance on information governance, data protection, privacy, cybersecurity and digitalization. In particular, he advises businesses on a wide range of domestic and international privacy compliance matters. He is a subject matter expert on cybersecurity matters, including data breaches and incident response, risk assessments, policy development and compliance with industry standards, such as the Payment Card Industry Data Security Standard (PCI DSS).

Before joining Fieldfisher, Lanois was vice president and senior legal counsel at a leading international bank, Credit Suisse, at its headquarters in Switzerland and later at its Hong Kong office. As in-house senior legal counsel, he advised the bank on various matters and spearheaded several initiatives, to include a global compliance program, cross-border matters, the bank's digital transformation initiatives and the launch of new online services and products.

In addition to being a cybersecurity professional, he is also an attorney, qualified in California, New York and D.C., meaning he can advise both on cybersecurity requirements and on legal requirements such as the European General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).

"I have had the privilege to work on a wide range of different projects and initiatives, including privacy and cybersecurity issues related to autonomous vehicles, new AI-enabled devices

and applications, virtual reality (VR) and augmented reality (AR) projects, blockchain initiatives, digital banking solutions and contact tracing apps," he says.

Throughout his career, one of the projects Lanois is most proud of was in an area he did not expect: videogames. "I advised a game developer from a privacy and cybersecurity law perspective in relation to the implementation of an anti-tamper and anti-cheat solution for an online multiplayer game," he says. "I enjoy playing games and know how cheating can be an issue in today's games, so it was interesting to help a game developer in their fight against tools designed by hackers to inject a game with specialized code that changes how the game works and gives the user an unfair advantage over other players."

Lanois is a member of the International Association of Privacy Professionals' Education Advisory Board and CIPT Exam Development Board. In addition to holding several certifications, Lanois has received a number of awards, including the Association of Corporate Counsel's Top 10 30-Somethings award and the ACC Advocacy Award.

"My advice for future security professionals is to always read and keep learning. There are many resources readily accessible online to help new security professionals get started on their journey. Never stop the learning process: getting a cybersecurity job is not the end, but only the beginning of the journey. Cybersecurity is an area which is ever-changing, with the emergence of new technologies and new threats constantly arising or evolving, so it is important to always keep abreast of such new developments. Also, never assume that a shiny new tool acquired by your company can or will do your job for you and that you can just sit back and relax. A determined attacker will just find another way to get through," Lanois says.



Kurt John

Chief Cybersecurity Officer,
Siemens USA

CYBERSECURITY

As Chief Cybersecurity Officer, Kurt John is responsible for overseeing the development and implementation of cybersecurity strategy in Siemens' largest market, the U.S. In this role, he oversees the coordination of cybersecurity for the enterprise's products, solutions, services and infrastructure utilized to deliver value to Siemens USA's customers.

John serves as a member of the Siemens Cybersecurity Board, working alongside international colleagues to set strategy, address global challenges and evaluate actions to secure new cybersecurity opportunities. John is a member of the Virginia Chamber of Commerce's Innovation & Technology executive committee and was recently appointed to Governor Northam's Virginia Innovation Partnership Authority.

John has shared his expertise with many external bodies and consortiums including the National Institute of Standards and Technology (NIST), contributing to the cybersecurity standard used by U.S. Government agencies. He has also provided guidance on key metrics that help track and improve cybersecurity to the U.S. Government Accountability Office and provided input on cybersecurity legislations. He has informed the UN Under-Secretary-General's office on the industry's perspective in addressing global cybersecurity policy challenges, and worked with other large organizations including the Council on Foreign Relations and the University of Pennsylvania in communicating the importance of cyber norms for society.

John is a proponent of engaging sections of the workforce that are uniquely positioned to help

address the cybersecurity skills gap. As a result, he has mentored several individuals and groups including Waukegan High School Students in the Chicago, Ill. area, teaching the importance of staying the course and how to face adversity. He has mentored Columbia University Masters students on applying what they have learned to the private sector and also mentored students from a variety of universities through the Atlantic Council on how to apply cyber policy to multinational and geopolitical challenges. He also holds several professional certifications in the field of cybersecurity.

His advice to future security professionals is to think big, then think bigger. "All of our workstreams today are becoming more interconnected, and it is inevitable that a ripple in one area will impact another. We learn the skillsets and tools we need to approach our discipline methodically; however, your mindset should attempt to take in the broadest context with a predisposition to collaboration across multiple domains. Security, both cyber and physical, will always have overarching business impacts. The sooner we can anticipate and understand those impacts, the better off the business will be."

Throughout his career, he is most proud of driving and implementing a collaborative culture that prioritizes proximity to his customers and responsiveness to needs. He says, "Technology and other aspects of our lives are moving so fast that we can sometimes feel overwhelmed. Strong cross-functional teamwork with an eye to the future is how we navigate the technological and ethical challenges we face. I believe that leaders in the field of cybersecurity need to emphasize collaboration, not only in their teams, but across all business functions to ensure we bring a myriad of perspectives to the table when taking on new challenges."



Joyce Hunter

Executive Director
*The Institute for Critical
Infrastructure Technology*

CYBERSECURITY

Joyce Hunter is the Executive Director of the Institute for Critical Infrastructure Technology (ICIT), a nonprofit cybersecurity and technology think tank. There, she is responsible for building and executing ICIT's mission of improving national security, increasing public and private sector cyber resiliency, and modernizing critical infrastructures.

U.S. President Barack Obama appointed Hunter as the deputy chief information officer for Policy and Planning at the Department of Agriculture (2013-2017) and as the acting chief information officer from March 2016 to July 2016. An MBA holder from the Wharton School of Business, Hunter is a strategic-doer who oversaw the Department's IT investment portfolio of \$4.1 billion and provided executive leadership in IT governance, portfolio management, IT policy, workforce planning and enterprise architecture.

With more than 30 years' experience in the information technology industry, Hunter demonstrates a strong ability to build and sustain relationships with public and private stakeholders, and to develop and lead innovative projects and inter-agency initiatives. Prior to her federal appointment, Hunter was the CEO of Vulcan Enterprises, a strategic management consulting organization, where she also provides executive coaching and IT advisory services.

Hunter has been honored numerous times as a technology executive, receiving the Joseph A. Wharton award and the Roy L. Clay Sr. Technology Pinnacle Award for being one of the 50 most important African-Americans in technology. She is on the Dean's Advisory Council for Villanova University, sits on multiple

industry boards and is active in several philanthropies focused on advancing STEM and data science education. She is also published in *The Handbook of Federal Government Leadership and Administration: Transforming, Performing and Innovating in a Complex World*.

She is passionate about advancing a digital future. She says, "It's a significant issue for educators, cyber experts and our future cyber leaders. The rapidly evolving challenges are what makes it such an exciting time to work in our fields of data protection and cybersecurity. Cybersecurity professionals have never been in more demand, and training and capabilities are essential. By understanding the information lifecycle, from collection to storage, to destruction; by taking a privacy and security and testing by design approach; and recognizing the human element in how we interact with data, future cyber leaders will be well equipped to help take us into a safe and people-centered digital future."

Hunter is most proud of the creation of the Data Science Camp in 2014 while she was the Deputy CIO for Policy and Planning at USDA for underserved and underrepresented youth. "Science Technology Engineering Agriculture and Math (STEAM) has just completed its sixth year and is designed to deliver an immersive, two-week-long, design thinking, project-based and team-focused learning experience for high school students. The program's goal is to help these students build familiarity and hands-on competence with the approaches, tools and analytical techniques relevant to harnessing the power of open data on critical issues related to food and agriculture in the Washington, D.C. and Sacramento, Calif. areas," she says. There are additional camps forthcoming with concentrations in energy, athletics and architecture.

GLOBAL SECURITY AS A SERVICE

T-0 LIFT OFF

GLOBAL SECURITY AS A SERVICE (GSaaS): THE DISRUPTION SHAPING THE FUTURE OF SECURITY



SEPTEMBER 30, 2020 AT 2 PM EDT

SPEAKERS



Rob Kay
Global Director of
Professional Services
Northland Controls



Pierre Trapanese
CEO
Northland Controls

Not since the introduction of IP cameras and NVRs has the security industry seen the amount of change that is coming. In the way that Netflix toppled Blockbuster, GSaaS is taking off and poised to take over the industry. GSaaS holds the promise of proper consistent global configuration of security systems, more reliable integrations to other systems across the enterprise, more efficient responses, easier scalability, and more reliable hardening because of one holistic ecosystem. Join this webinar to understand why people are making the shift, what it takes to make it happen, how to avoid common pitfalls, and why those that do it quickly will be better off for it.

LEARNING OBJECTIVES:

1. Identify the benefits and challenges of security on premise, in the right cloud, and the wrong cloud.
2. Assess and vet the performance of a GSaaS provider.
3. Explain the concepts needed to transition into working with an IT world and move to a GSaaS model.
4. Assess whether GSaaS is the right model for your organization.



NORTHLAND
CONTROLS



Earn: 0.1 IACET CEU – BNP Media is authorized by the IACET to offer 0.1 CEU for this program. Participants completing this course may be eligible to receive Continuing Professional Education credit or CPEs toward ASIS re-certification.

Watch live on September 30, 2020 or anytime On-Demand at
SecurityMagazine.com/Webinars



Jinyu (Gene) Sun

Corporate Vice President,
Information Security - Chief
Information Security Officer
FedEx Corporation

CYBERSECURITY

Since being named FedEx CISO in January of 2018, Gene Sun has been guided by the principle that the most important factor in any cybersecurity program is trust. He has found that this trust has given him a license to operate with the FedEx C-Suite, his business peers, the Global Information Security team and the 500,000 FedEx team members around the world. Sun is responsible for securing digital assets and ensuring business continuity for the \$69 billion global transportation and logistics company. He provides global leadership and strategic direction for information security, risk management and regulatory compliance.

Sun has expanded the influence of the CISO role at FedEx by initiating quarterly briefings with his executive peers throughout the FedEx enterprise. He knows how important it is for business and IT executives to work collaboratively to create more transparency and understanding throughout the company about the technologies and processes that are most effective for protecting critical business information. He uses this collaborative approach to convene business and IT leadership, along with subject matter experts, to develop and launch enterprise programs such as Zero Trust and the Global Segmentation of Enterprise Networks.

The trust the FedEx enterprise has in Sun is key as the cybersecurity landscape continually changes and requires constant evaluation of threats, new technologies and emerging innovations to protect the company. FedEx leadership has empowered Sun to deliver bold, game-changing solutions. Sun in turn empowers his team to do the same. For his organization, Sun has a singular vision,

and he sets aspirational goals that challenge his team members to “stretch their security muscles” to meet the escalating trajectory of cyberattacks and threats. He regularly makes time for mentoring team members, and encourages his organization to learn and develop opportunities.

Sun has a vast knowledge of FedEx through his work in various areas, and he encourages his team members to do the same. To be successful within the cybersecurity profession, Sun says, “Go outside of your comfort zone by broadening your career experience beyond the cyber expertise. Before I moved to information security, for instance, I gained experience as a sales engineer, network administrator/web master and application developer. It is important to be able to speak ‘other languages’ and look at the larger picture beyond security to establish personal credibility. Those experiences will enable you to see how security should be integrated within the business and to make better risk decisions.”

Sun is a thought leader in the areas of cyber defense, digital transformation, the evolving CISO role, risk management and the importance of public-private partnerships. He is also a founding member of a cross-industry private sector collaborative group that focuses on global privacy and technology regulations.

Throughout his career, Sun is most proud of gaining support for the FedEx global cloud strategy. “This large, multi-year program enabled the company to take advantage of rapid innovation, agility, economic value and reduce our information risks at the same time,” he says.

Sun is a member of the Google CISO Advisory Board, a board member of the Open Networking User Group (ONUG) and an advisory member for Herf College of Engineering at the University of Memphis. He is a four-time recipient of the FedEx Five Star Award, the most prestigious award an employee can receive.

Join the Mission 500 Club Virtual Fundraising Drive



Open enrollment for Mission 500's 500 Club is now open. Join us to raise funds via virtual events for children and families in need across America.

It's easy! Participate in one of the virtual events already organized online or create your own. Then set up a personalized fundraising page you can send to friends and family to get their support, and promote through your own social media channels. And if you require assistance, we are here to help.

Visit Mission500.org for more information. #M500Club



Choose or create
an event

Here are some ideas:

Running Cycling
Walking Jump Rope
Karaoke Etc.



Set-up a
fundraising page

Customize a fundraising page
with your story and goals!



Get friends and
family to participate

Promote your event via
social media. We'll help too!



Supporting Families Across America

MISSION 500

**Sounil Yu**

CISO-in-Residence
YL Ventures

CYBERSECURITY

As the CISO-in-Residence of YL Ventures, a cybersecurity-focused venture capital firm, Sounil Yu provides entrepreneurs first-hand insights into product development, customer needs and how global enterprises evaluate cybersecurity vendors and their solutions pre- and post-investment.

Previously, Yu served as Bank of America's chief security scientist, where he led a cross-functional team of experts dedicated to driving cybersecurity innovation. There, he pioneered the organization's adoption of FAIR, a quantitative cyber risk analysis methodology, to enable the team to understand and evaluate risk more effectively. He also served as the University Dean for Bank of America's internal training and education program and served as the executive sponsor for DevCon, an internal Bank of America conference.

Yu's most influential business accomplishment is the creation of his Cyber Defense Matrix, a framework for understanding and navigating the cybersecurity landscape. He has developed use cases that make the Cyber Defense Matrix practical for many purposes, such as rationalizing technology purchases, defining metrics and measurements, and identifying control gaps and opportunities. Elements of the Cyber Defense Matrix have been incorporated into the Center for Internet Security's (CIS) Top 20 Critical Security Controls and has also been adopted by the OWASP Foundation. He also developed the DIE Resiliency Framework (a.k.a. DIE Triad), which advocates for three paradigms (Distributed, Immutable and Ephemeral) to replace the CIA Triad. Yu is also a board member for the FAIR

Institute and SCVX; a co-chair of Art into Science: A Conference on Defense; IANS faculty member; and a visiting fellow at the National Security Institute.

Previously, Yu led the FS-ISAC Measurements and Metrics Working Group to develop a unified corpus of measurements to consistently measure security posture and derive useful cyber risk metrics for executive level reporting. He co-chaired OASIS OpenC2 (a security standards group) to support interoperability of defensive technologies enabling machine-level speed for response actions.

"My career advice would be to have a security mindset that is intensely curious and willing to poke holes in the status quo. However, this must be done in the name of improvement. For every hole that you poke, don't just point it out, but be ready to roll up your sleeves and take concrete steps to make it better. It is easy to throw a brick through a window and blame the window engineer for bad design or for its inherent vulnerabilities. It's much harder to help the engineer build a better window that can withstand that brick and still let in light," Yu says.

Yu is most proud of the cybersecurity internship programs that he led over the last decade. "Through these efforts, I had the opportunity to shape the career trajectories of over 500 interns and equip them with skills to tackle the many challenges we face in the cybersecurity industry," he notes. "We often lament that we do not have enough qualified and diverse cybersecurity professionals to fill the hiring pool. I take pride in making meaningful contributions to this long-term talent pipeline and helping future cybersecurity experts find solid footing in cybersecurity."

To do his part during the pandemic, Yu is a volunteer for Project N95, an organization connecting healthcare providers with manufacturers and suppliers of critical equipment. When he is not helping his community, he enjoys playing board games and video games with his children.



How to Leverage Multi-Layered Time Series Data for Improved Security

OCTOBER 8, 2020 AT 11 AM EDT

SPEAKER



Craig Johnston
VP of Business
Development & Sales
Live Earth

SPONSORED BY



Organizations and agencies must adopt new technologies to keep their most important assets safe. For security professionals, filtering through the massive amounts of disparate data is overwhelming. Detecting critical events, uncovering patterns, and then communicating action is a clear challenge.

Currently, most organizations are not taking advantage of time series data using a multi-layered platform approach. Analyzing real-time data from disparate layers is greatly enhanced using advanced geo-temporal techniques.

In this webinar, we will show a variety use cases to help you understand how easily you can enhance the safety and security of your most important assets.

LEARNING OBJECTIVES:

- Improve the physical security of your organization with anomaly detection and pattern recognition.
- Leverage your current data streams through a multi-layered operational view.
- The benefits of using secure cloud technology as a data warehouse.
- How to provide operations and security staff a complete operational picture to reduce response time.



Watch live on October 8, 2020 or anytime On-Demand at
SecurityMagazine.com/Webinars



Tyne Truong

Assistant Special
Agent in Charge
*U.S. Department of Homeland
Security, Homeland Security
Investigations*

GOVERNMENT

Tyne Truong is an Assistant Special Agent in Charge for the U.S. Department of Homeland Security (DHS), Homeland Security Investigations (HSI) National Security, Counterterrorism and Counterproliferation/Export Control Investigations Division. He is a proactive security leader with experience across law enforcement, government operations, defense and intelligence, working with stakeholders in private and public sectors for the delivery of innovative security solutions.

The best advice he can give is to know the important difference between a “leader” and a “manager/supervisor,” he says. “Understanding that although both aspects are important for the success of the enterprise, it is good leadership that will have the most profoundly positive influence on that organization’s culture and its long-term effectiveness. Once you realize that you lead people and you manage ‘things and processes,’ you can accordingly frame the challenges that you’ll encounter, no matter how adverse, to achieve the best business-aligned security outcomes for your organization. I truly believe the consequences of positive or negative leadership styles are that much more amplified for security and law enforcement personnel tasked with protecting people, assets and organizational reputation.”

After entering the DHS post-9/11, and serving in HSI, the U.S. Department of the Treasury, and U.S. Customs Service, Truong deployed project management methodologies on an enterprise level, and created and implemented national policy with an enterprise-wide grasp on threat and vulnerability.

This is something Truong is proud of.

“Architecting and authoring new global policies from the ground up for DHS shortly after its founding, I’m proud of having transformed disparate legacy agency policies governing global security, investigations and strategies into new, cohesive and operationally effective ones that have facilitated thousands of successful law enforcement operations, investigations and security outcomes for the newly formed department. I’ve had the honor of leading some of the best people in law enforcement during the deployment of these new guidelines in operational settings and along the way, managed some of the most successful national security and public safety campaigns for our agency.”

Truong served as a National Program Manager for the agency’s National Undercover Operations Unit and was responsible for being a national policy developer, writer and implementer for enterprise risk, critical incident management, operations security and investigations oversight of the agency’s worldwide undercover operations enterprise. Today, he leads the agency’s counterproliferation and export control program in Los Angeles to ensure robust outreach to community and security industry leadership regarding export violations of controlled technologies and materials, oftentimes within the defense industrial base.

Throughout his career, Truong has paid it forward when it comes to mentoring his colleagues and staff. A number of the individuals whom he has mentored have themselves become executive managers at both the agency headquarters and field levels. Based on his service and accomplishments, he has been honored with the DHS Secretary’s Meritorious Service Award and Director’s Excellence in Law Enforcement Award. He is a Distinguished Homeland Defense Fellow at the National Defense University.

Stay up to date with valuable training materials for security professionals from *Security*



A. Effective Security Management, 7th Edition - \$93.00

Effective Security Management, 7th Edition teaches practicing security professionals how to build their careers by mastering the fundamentals of good management. Charles Sennewald and Curtis Baillie bring common sense, wisdom and humor to this bestselling introduction to security management.

.....

B. Understanding Homeland Security: Foundations of Security Policy - \$154.00

Understanding Homeland Security is a unique textbook on homeland security that blends the latest research from the areas of immigration policy, counterterrorism research, and border security with practical insight from homeland security experts and leaders such as former Secretaries of the Department of Homeland Security Tom Ridge and Janet Napolitano.

.....

C. Cyber Strategy: Risk-Driven Security and Resiliency - \$132.00

Cyber Strategy: Risk-Driven Security and Resiliency provides a process and roadmap for any company to develop its unified Cybersecurity and Cyber Resiliency strategies. It demonstrates a methodology for companies to combine their disassociated efforts into one corporate plan with buy-in from senior management that will efficiently utilize resources, target high risk threats, and evaluate risk assessment methodologies and the efficacy of resultant risk mitigations.

.....

D. GSEC GIAC Security Essentials Certification All-In-One Exam Guide, 2nd Edition - \$63.00

GSEC GIAC Security Essentials Certification All-in-One Exam Guide, 2nd Edition provides learning objectives at the beginning of each chapter, exam tips, practice exam questions, and in-depth explanations. Designed to help you pass the exam with ease, this authoritative resource also serves as an essential on-the-job reference.



Rebecca Morgan

Chief Insider Threat Division
Center for Development of
Security Excellence (CDSE),
Defense Counterintelligence
and Security Agency (DCSA)

GOVERNMENT

Rebbecca Morgan is the Chief of Insider Threat Division at the Center for Development of Security Excellence, Defense Counterintelligence and Security Agency (DCSA). In this position, she coordinates training, awareness, professional development, education, research outcomes and public outreach efforts in support of the counter insider threat mission for U.S. Government, cleared industry and critical infrastructure sectors.

Morgan established the Insider Threat Division and developed and directed insider threat practitioner training, national public outreach and general workforce awareness campaigns. In addition to successfully initiating the first national Insider Threat Awareness Month, she designed and delivered Insider Threat Program requirements and products resulting in DCSA being named in Department of Defense (DoD) and federal policy, directives and memoranda. She implemented the program by leading a team of technical experts in support of counter Insider Threat efforts throughout the DoD, Intelligence Community and federal agencies.

She is proud of her efforts to develop public outreach for insider threats, leading to creation of the mobile application Insider Threat Sentry, which provides training, awareness and resources to support security practitioners.

“We’ve been able to educate the general public and federal and private industry workforces on the true role of insider threat programs, which are designed to deter, detect and mitigate risk of trusted insiders, while protecting the privacy and civil liberties of the workforce,” Morgan says.

Previously, Morgan served as a special agent and counterintelligence specialist with the Defense Security Service; an intelligence operations specialist with the DoD Counterintelligence Field Activity; the senior Intelligence Analyst of Foreign Supplier Assessment Center; and an instructor at the Joint Counterintelligence Training Academy.

In addition, Morgan is a mentor for Girl Security, an organization that is building a pipeline for girls and young women in national security through learning, training and mentoring support. She also mentors new security and counterintelligence practitioners.

To anyone that is starting out in their career, Morgan recommends being open to new experiences, cross-training and opportunities for joint duty or short-term assignments. “Having a strong base of knowledge in multiple areas provides individual career flexibility and improves the efficacy of national security programs. Throughout my career, I have held a number of positions in a variety of discipline areas. I have supported personnel security, industrial security, counterintelligence, research and technology protection, critical infrastructure protection, supply chain risk management and insider threat in positions ranging from investigations to analysis to operations to program management. Having this breadth of knowledge has helped me to be a more effective practitioner within the intelligence and security communities and develop a broad network of reliable professionals whose support has been critical in the implementation of various initiatives.”

Morgan's was named the CI Educator of the Year by the Director of National Intelligence and honored as a DoD “Unsung Hero” by Secretary of Defense William Cohen.



Chief Carmen Best

Chief of Police
Seattle Police Department

GOVERNMENT

Carmen Best will retire as Chief of the Seattle, Wash. Police Department (SPD) on September 2, 2020. As Police Chief, Best managed 1,400 police officers and was in charge of maintaining court-ordered reform to limit excessive police use-of-force and improve relationships with the local community. She was the first African-American woman to lead Seattle's police department.

Born and raised in Tacoma, Wash., Best graduated from Lincoln High School in 1983. After high school, she attended Eastern Washington University, then joined the U.S. Army and served three years in South Korea. In 1989, Best left the Army to work as Account Processor at Aetna Insurance, where she then enrolled in the police academy.

For 26 years at the police department, Best served in roles, including patrol, school safety and media relations, patrol supervisor, watch commander and operations lieutenant.

Prior to assuming the role of Chief of Police on August 13, 2018, Best was Deputy Chief, where she oversaw the Patrol Operations, Investigations and Special Operations Bureaus, as well as the Community Outreach section. Although there have been nationwide protests against police after the death of George Floyd while in police custody in Minneapolis, Minn. as well as divide over policing and budget cuts to the police departments, Best was one of the first police chiefs to describe Floyd's death as murder.

Recently, the Seattle Police Department created the Collaborative Policing Unit, which encourages community partnerships – something she is

most proud of. "The SPD is not apart from, but a part of the City and its people. We also now focus many of our recruiting efforts on the neighborhoods of Seattle, so that increasing numbers of our new officers come from the diverse communities we serve," Best said.

In addition, Best has completed training at the Senior Management Institute for Police, the FBI National Executive Institute (NEI), the FBI National Academy, the Criminal Justice Executive Leadership Academy and the Major Cities Chiefs Association Police Executive Leadership Institute. She holds a Master of Science in Criminal Justice from Northeastern University.

Best also serves as Chair of the Human and Civil Rights Committee (HCRC) for the International Association of Chiefs of Police (IACP) and the IACP Board of Directors, serves on the National Law Enforcement Exploring Committee, and is a member of the National Organization of Black Law Enforcement Executives (NOBLE) and the National Latino Police Officers Association (NLPOA).

In 2015, Best received the Newsmaker of the Year award from the Seattle Black Press. In 2019, she received the Vision from the Mountaintop award from Urban Impact for her commitment to justice and community. She was also awarded the Ellis Island Medal of Honor, which recognizes individuals for accomplishments in their field and contributions to society.

"Police work is never done," notes Best. "Officers must continuously improve public safety methods and embrace innovation. Law enforcement professionals must also have a growth mindset because new challenges are always being presented. Be as ready as you can be for whatever may be coming, and be willing to pivot."



Paul Abbate

Associate Deputy Director
*Federal Bureau of Investigation
(FBI)*

GOVERNMENT

Paul Abbate currently serves as the Associate Deputy Director, a position in which he is responsible for the management and oversight of all U.S. Federal Bureau of Investigation (FBI) personnel, budget, administration and infrastructure, as well as the inspection and insider threat programs.

Abbate began his FBI career as a special agent in March 1996, assigned to the New York Field Office, where he worked in the Criminal Division and served as a member of the SWAT team. In 2003, he joined the Counterterrorism Division as a supervisory special agent overseeing FBI operations in Iraq. During his career, Abbate has led the counterterrorism program in various positions and has served in leadership roles on the Joint Terrorism Task Forces of the Los Angeles and Newark, N.J. Field Offices. Abbate has also led FBI operations overseas while deployed in Iraq, Afghanistan and Libya.

In 2012, Abbate was appointed special agent in charge of counterterrorism at the Washington, D.C. Field Office and in 2013, the special agent in charge of the Detroit Field Office. In September 2015, he was appointed assistant director in charge of the Washington Field Office, where he served until his appointment as the executive assistant director for the Criminal, Cyber, Response and Services Branch in December 2016. In this capacity, Abbate oversaw all FBI criminal

and cyber investigations worldwide, international operations, critical incident response and victim services.

“From an FBI perspective,” says Abbate, “I’m most proud of the hard work that our people do day in and day out, 24/7, to keep others safe from harm and protect our country – particularly as they’ve worked tirelessly to overcome the challenges present in the current operating environment. They have shown tremendous agility and resilience in carrying out our mission, while everyday life and work have been altered

in unimaginable ways by the ongoing pandemic. From a programmatic viewpoint, one of our most significant strategic advancements has been the development of our Insider Threat Office over the past several years. We have made tremendous progress toward putting in place effective internal measures to protect our people, information and facilities from the myriad of threats we face every day.”

“We have made tremendous progress toward putting in place effective internal measures to protect our people, information and facilities from the myriad of threats we face every day.”

For those aspiring to a career in security or law enforcement, he says it’s essential to always remain vigilant and stay focused on effectively countering the most severe and immediate threats at a tactical level, while never losing sight of the broader strategic horizon. Abbate adds, “These dual objectives are best accomplished through relentless engagement, communication, collaboration and teamwork. The mission is best served by working hard to protect people from the terrorism, cyber, criminal and foreign intelligence threats we face today, while simultaneously adapting, innovating and offering a vision for the future in order to stay ahead of emerging threats and outpace adversaries.”



Paul Goldenberg

CEO
Cardinal Point Strategies

SPECIAL RECOGNITION

Paul Goldenberg is a highly decorated law enforcement and national security professional. He was a co-founder of Secure Community Network, the nation's first Department of Homeland Security (DHS) and ASIS-recognized faith-based information sharing center, which has developed many of the security industries standards for faith-based security. Through his work as a member of the DHS Advisory Council, he has played a key role in setting domestic and international policy for the legislation and investigation of hate crimes, insider threat, countering violent extremism, information sharing, cybersecurity policy and establishing and managing public-private partnerships across the world.

Goldenberg led the efforts of the 2019 Subcommittee for the Prevention of Targeted Violence Against Faith Based Communities. In 2018 and 2019, he co-chaired the National Cyber Security and Foreign Fighter Task Forces. His public career includes more than two decades as a former senior official for the New Jersey State Attorney Generals Office, and commissioner/director of one of the nation's largest social service and juvenile justice systems.

During the 1990s and in the wake of highly publicized incidences of domestic terrorism and hate crimes, Goldenberg was appointed the nation's first statewide Chief of Office for bias crimes, domestic terrorism and state community relations efforts. "What I am most proud of is that enforcement was only a minor part of our mission. We directed much of our efforts towards the advancement of programs focused on building trust between the most

vulnerable groups among us and the police and security professionals who serve them. These included groundbreaking community policing programs based on cooperation and information sharing. Our team traveled to more than 20 states and 12 countries where we shared our works with academia, state and national police services and NGOs. And that, in turn, led me to my work as a senior fellow with the Rutgers University Miller Center for Community Protection and Resilience and as liaison to the University of Ottawa where we continue these efforts today."

Goldenberg has received numerous honors while working as a law enforcement officer in urban Essex County, N.J. In addition, he served as a deep undercover agent for the South Florida Strike Force and was awarded Florida's citation for valor: Officer of the Year.

"Throughout my career, I've had the privilege of working within a variety of roles in the law enforcement and transnational security profession. I had a rare opportunity the last four decades to witness the transformation of American policing and security in all its manifestations," Goldenberg says. "The progression and soul searching underway since George Floyd's death will be difficult for some – nonetheless, galvanizing for others. A successful career is no longer judged on the number of arrests one makes, how many doors you hit in pursuit of the bad guy, or the number of tickets issued. Where most aspiring law enforcement and security professionals may once have been drawn to the exploits of SWAT, anti-Crime and or narcotics enforcement – the newly minted officers will need to be more focused on community policing, building trust, engagement and taking on the role as agents of social change through their actions and commitment to the communities they serve."



Peggy O'Neill

Executive Director
*International Security
Foundation (ISF)*

SPECIAL RECOGNITION

An experienced nonprofit leader who specializes in startups, turnarounds and leadership coaching, Peggy O'Neill has over 35 years of experience working with non-profit boards.

O'Neill began her career in real estate and financial services. Her nonprofit expertise began at the Whitby School in Greenwich, Conn., where she created internal control procedures and new revenue streams to transform the school's financial position and eliminate an operating fund deficit. From 2007 to 2013, she served as executive director of Baltimore's Irvine Center, an environmental education organization. She successfully led Irvine through many difficult transitions including the construction of a new facility and financial challenges to eliminate an operating deficit and create a thriving nonprofit. Now, as Executive Director of ISF, O'Neill is responsible for securing funding from the private sector to support the programs of the Overseas Security Advisory Council (OSAC) of the U.S. Department of State, Bureau of Diplomatic Security. This requires O'Neill to fundraise and raise awareness about how ISF helps promote and market OSAC and the value that OSAC's programs serve. "It is also important to create and maintain a healthy partnership between the ISF and OSAC as this model is unique," she says.

For O'Neill, working in the nonprofit sector allows her to have a mission that guides all of her work and responsibilities. "It's a rallying and a passion point for people to come together to create something for the better good. For the security sector, it's very rewarding knowing that

the ISF is really making a difference in support of the exchange of security information through OSAC, which helps to keep Americans safe overseas. But it's also personal. My late brother, Master Sgt. Patrick J. Mangan, was a Marine, and I always admired his service. When I lost him in 2001 (not in active duty), I really wanted to do some type of work to honor his commitment to our country. Working for the ISF rang true to me," she says.

At ISF, she has spearheaded and created the institution's infrastructure, fundraising program and website and grew its staff. Through successful programs that include a highly anticipated annual fundraising event, the ISF has funded more than 200 OSAC programs.

"My work at Irvine was a challenging experience navigating through the 2008 economic downturn," she says. "But to bring all my experience and skills in fundraising, finances and programming to create something of real value – especially wearing many hats in the ISF's earliest days – is very rewarding. I am quite proud of seeing how the ISF has been embraced so passionately by the community OSAC serves and to see the ISF grow from its founding in 2011."

O'Neill adds she is often surprised by the resiliency of the security community. "OSAC members freely and genuinely share best practices. It's about keeping people safe. The strength of the community and the work that the ISF does to support the OSAC network have been an incredibly strong experience. I would encourage all security and law enforcement professionals to embrace that network and get involved. Reach out to the Outreach and Engagement Unit OSACCCO@state.gov for information."



Paul Timm, PSP
Vice President, Physical
Security Services
Facility Engineering Associates

SPECIAL RECOGNITION

Paul Timm is Vice President of Facility Engineering Associates (FEA), which helps support and provide owners and managers with progressive and innovative solutions to facility lifecycle challenges. He is a national acclaimed expert in physical security, a board-certified Physical Security Professional (PSP), and is a professional dedicated to helping people make their places of employment safer through education and sharing best practices.

In his position at FEA, Timm specializes in school security, campus security, church security, library security, parks and recreation security, school safety, emergency planning, expert witness, crisis management and staff training.

For more than 17 years, Timm was owner and president of RETA Security, Inc., a non-product affiliated, family-owned firm focused on the education market, acquired by FEA in January 2017. At RETA Security, he provided independent physical security assessments, training, and technical assistance to schools, campuses and businesses nationwide. He also assisted administrators with loss prevention, risk management and emergency planning services.

Timm is also a keynote speaker working with Kirkland Productions through Safe and Sound Schools, a national school safety non-profit founded by Sandy Hook parents. There, Timm works to deliver crisis-prevention, response, and recovery programs, tools and resources to educate members of the school community, from students and parents, to teachers and administrators, to law enforcement and local leaders.

In addition to vulnerability assessment expertise, he is a School Crisis Assistance Team vol-

unteer through the National Organization for Victims Assistance (NOVA). He is certified in Vulnerability Assessment Methodology through Sandia National Laboratories and the ALPHA vulnerability assessment methodology. He serves on ASIS International's School Safety & Security Council, the Campus Safety Conference advisory board, and the advisory council for the Partner Alliance for Safer Schools (PASS).

He authored "School Security: How to Build and Strengthen a School Safety Program," where readers are introduced to loss prevention and safety practices, including how to implement specific measures, how to raise security awareness and how to prepare for emergencies. The book also discusses how to positively influence student behavior, lead staff training programs, and write security policies. Timm participated in Best Practices for School Building Safety at the Federal Commission on School Safety in 2018, held by the Department of Homeland Security. He earned a degree in speech communications and a certificate in business administration from the University of Illinois at Urbana-Champaign.

Timm says that to be successful in the security industry, there are two critical aspects. "Number one – Be collaborative. This industry has more than enough individuals who have adopted an isolationist approach based on the misconception that they know more than everyone else. Pursue a better course by joining associations, teams and panels. Let's make things safer together. Number two – Get credentialed. Obtaining industry credentials requires continuous learning. Challenge yourself and encourage others to do the same," he says.

Throughout his career, Timm is most proud of publishing his book in 2015. "A lot of time and effort went into that initiative. I'm thankful for the assistance I've received, especially from my family, during both editions," he says. The 2nd edition is set to publish soon.



Mission 500

ASSOCIATIONS

Mission 500 is a nonprofit organization that works closely with the security industry to serve the needs of children and communities in crisis in the U.S. The organization advocates for children and families in crisis, inspires and acts as a catalyst in the security industry for excellence in corporate social responsibility, and mobilizes volunteers and resources to make a difference for children and families living in poverty in the U.S.

Mission 500 partners with numerous associations including Title 1 schools, Habitat for Humanity, The Refugee, the New York Fire Department Burn Center Foundation and many more. Since its 501(c)(3) status in 2016, Mission 500, along with security industry leaders and volunteers, has helped produce more than 340,000 meals, assemble care packs filled with essential hygiene items for 3,700 families and distribute more than 11,500 book bags with school supplies to students attending Title One schools. Recently, Mission 500 also collaborated with Feeding America, U.S. hunger relief organization, to provide meals to families in need during the COVID-19 pandemic.

In addition, Mission 500 hosts various awards, such as the Corporate Social Responsibility Award, designed to honor companies in the security industry who make important contributions to those in need; the Humanitarian Award, designed to honor individuals in the security industry and their respective contributions toward social causes; and the Innovative Partner Award.

"Every organization, school, child and family

we have been able to help makes a difference. We can honestly say that each hand we have given seems like the first time – that feeling resonates with each and every trip, event, run, walk we have done," says Ken Gould, Chairman of the Board. "Volunteers are the lifeline to Mission 500, and we greatly depend on them to help bring new ideas and donations all year long. We appreciate the countless hours they put in and their dedication."

During the COVID-19 pandemic, Mission 500 members have taken to creating events on a virtual platform. "Families and children in need cannot take a back seat during the current pandemic, so we are doing things differently this year to help maintain the work of Mission 500. Our focus is still strong, and this new virtual reality is something we will leverage to the fullest extent," says Gould.

In June, for instance, the organization launched the M500 Club, an initiative designed to help Mission 500 continue with its charitable work during the pandemic by directly engaging individuals with virtual events. M500 Club features virtual 5k run/walks, cycling (spinning) events, talent shows, karaoke sing-offs, buzz and shaving challenges, basketball shooting contests and more.

Despite the challenges charities around the world are experiencing due to the widespread cancellation of events, Mission 500 is pushing the envelope wherever possible. With golf having been earmarked as a safe recreational event during the pandemic, Mission 500 is staging the M500 Golf Challenge in New Jersey on September 21st. Sponsors and players are invited to support the event. And with ISC West now a virtual event, the annual Mission 500 5K/2K has also gone virtual. Information on both events is available at www.Mission500.org

SECURITY | 2020 SOLUTIONS BY SECTOR

SAVE THE DATE

MARCH 2020  26 Education: Colleges and Universities	APRIL 2020  21 Building a GSOC	MAY 2020  19 Critical Infrastructure: Gas, Oil, Water	JUNE 2020  25 Education: K12	JULY 2020  28 Healthcare/Hospitals/ Medical Centers	AUGUST 2020  13 Retail
AUGUST 2020  20 Hospitality/Hotels	SEPTEMBER 2020  24 Insider Threat	OCTOBER 2020  13 Security and Workplace Diversity	OCTOBER 2020  29 Education: K12	NOVEMBER 2020  19 The Security 500	DECEMBER 2020  15 Healthcare/Hospitals/ Medical Centers

SOLUTIONS By Sector

webinars brought to you by



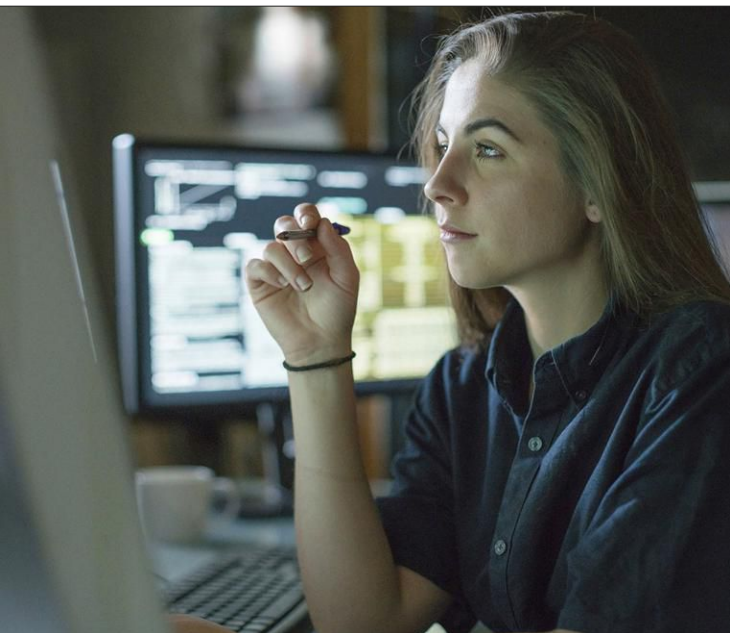
EARN 1 HOUR
of continuing education for most webinars!



Both live and on demand attendees may be eligible to receive Continuing Professional Education credit or CPEs toward ASIS re-certification. BNP Media is authorized by the IACET to offer 0.1 CEU each for these programs.

Register now for FREE at SecurityMagazine.com/webinars
FOR ANY WEBINAR IN THIS SERIES!

Security Careers in Investigations



Security professionals who are considering the potential direction for their private sector career often overlook certain functional areas. While considered part of a security leader's portfolio, many of these less obvious choices offer a broad diversity of challenges. One of these areas found in almost every industry sector is investigations.

The investigations career space is growing globally due to a wide variety of reasons. Proliferation of individual bad behavior, growing fraud schemes, intelligence targeting, insider threats, corruption, distractions due to major disruptive events and crises and general lack of ethics in leadership all contribute to the expansion in investigative openings.

There are many opportunities within various corporate departments that have accountability

for a wide variety of investigative areas separate from traditional corporate security departments. Often organizations have multiple investigative tracks handled separately by different functions within the same company.

In addition to opportunities within conventional organizations, there are numerous opportunities externally with law firms, large and small investigative service providers, companies that support investigative activities together with technical analysis and large-member accounting services firms with investigative practices.

Below is a high-level list of investigative activities to consider when planning your career:

- Anti-Money Laundering (AML)
- Corruption — Conflicts of Interest, Bribery, Illegal Gratuities, Economic Extortion
- Counterfeit Products, Components and Raw Materials - Product Integrity
- Credit Card Fraud
- Due Diligence — Mergers and Acquisitions
- Due Diligence — Vendors, Suppliers, Partners and Customers
- Employee Misconduct — Compliance, Liability and Ethics
- Financial Statement Fraud (Net Worth/Net Income Overstatements/Understatements)
- Fraudulent Disbursements — Billing, Expense, Payroll, Check Tampering, Register Tampering
- Fraudulent Disbursements — Insurance Fraud
- Government Security/Intelligence Matters with Private Sector Organizations
- Individual/Personnel Employment Backgrounds
- Intellectual Property — Trademarks,

Copyright, Confidential and Trade Secrets

- Legal Department Support, Inquiries, Internal/ External Actions, etc.
- Management of Investigative Programs
- Property Theft, Diversion and Misappropriation — Supply Chain, Distribution False Sales and Shipping
- Retail Loss Prevention
- Technical Forensics — Technologies, Cyber and Data Information Systems
- Theft of Cash — Skimming, Larceny, Write-Offs, etc.

Each of these areas has experience and education requirements. They also require a deep understanding of governing laws, regulations and other unique challenges. In today's environment it is also possible to have cross-border implications.

Salaries vary widely, but it is not uncommon to see compensation equivalent to that of CSOs, even at the individual contributor level. These are

typically roles that conduct the higher-end, complex and sophisticated investigations.

Technology such as artificial intelligence coupled with expansion in data collection may reduce staff for many basic compliance and transactional investigative teams. However, the volume of investigations resulting from individual criminal activity, organized crime, terrorist organizations, state actors, unethical companies and internal opportunists continues to grow. Often, much of these fall upon victims within the private sector to address, creating a wealth of investigative career opportunities within organizations. **SECURITY**

About the Columnist



Jerry J. Brennan is CEO of the Security Management Resources Group of Companies (www.smrgroup.com), the leading global executive search practice focused exclusively on corporate and information security positions.

Presenting...

Nothing New!

But in the security world, its no surprise that often the best solutions aren't new at all. When the situation happens where all your preparations and training are put to the test, the best and most reliable solution is often "boots on the ground".

You trust your trained security force and you can trust Par-Kut International to provide security booths and guard shelters to help you keep your boots on the ground, where they are needed, when they are needed.

Par-Kut buildings are not the most high tech solution out there, but when you need something that "just works" (and will continue to do so for a long time) think Par-Kut. We've got you covered.



BULLET RESISTANT • ARCHITECTURAL • SECURITY BOOTHS • GATE HOUSES

800.394.6599

PARKUT.COM

The Unifying Power of Security



When Benjamin Franklin emerged onto the steps of Philadelphia's Independence Hall at the close of the 1787 Continental Convention, he was asked whether the Founding Fathers had decided on a monarchy or a republic. "A republic, if you can keep it," he reportedly said.

Only once has the ability to keep that republic been in serious doubt – in the years up to and during the Civil War. Could it be in doubt again today? If so, security can be a model for preserving the republic.

How did we get here? Long, unstable fault lines in the bedrock that undergirds U.S. society have become active, sending seismic waves that have shaken the social contract. Citizens can't agree on basic facts. People question whether COVID-19 is real amid shifting medical advice and conflicting data on case and death rates. The footing keeps getting less stable. Economic freefall. Surging unemployment. White supremacists, fascists and anarchists boldly emerging from the shadows. Loss of faith in law enforcement by swaths of the populace after black citizens perished in police custody. Rampant misinformation

campaigns by anonymous groups and nations. The result is a bitterly split populace that has retreated to their respective echo chambers.

Each step toward human rights, or even civil discourse, spawns a group like the Boogaloo Boys or Antifa. Political correctness routinely stifles free speech on campuses and elsewhere. Franklin's challenge is being tested like never before.

America's fault lines hearken back to its founding. The U.S. was weaned on the twin but competing principles of rugged individualism and collectivism. Individualism is 17th century trappers, 19th century pioneers and cowboys, as well as the current era's technology and internet titans. It is an entire social and economic system that exalts private property and "moderate selfishness," as Alexis de Tocqueville phrased it in his mid-nineteenth century classic *Democracy in America*.

Collectivism, or communitarianism, is the 17th century Mayflower Compact, 19th century utopian communities, and today's internet of open networking and Wikipedia – a competing system that puts the group above the individual, which de Tocqueville called the "soft tyranny" of bureaucracies.

Today's flashpoint in this tension is whether a face mask is a symbol of oppression by an overreaching nanny state or an expression of responsibility for other's welfare. Fortunately, security professionals represent an example of finding common ground.

We need to characterize the current crisis not as a culture war or a battle between the economy and flattening the curve, but as a call to service to help our neighbors. We are in a war against Coronavirus – not simply as Americans, but as human beings – and we need our citizens to

embrace public service.

Nowhere can you find people more archetypically individualistic than in private security. They trend Republican, libertarian, law-and-order oriented, anti-regulation and intensely patriotic. They sound like individualists in the extreme, but you will find no group of people more dedicated to public service or aiding their fellow human being.

Consider the case of a corporate security colleague who moved from the “People’s Republic of New Jersey,” as he puts it, to Texas. On his way there, he navigated a westward jughandle so he could avoid the freedom-suppressing state of Maryland. As extreme as this sounds, this man would put his life on the line to save or help anyone. Countless security professionals come from the ranks of the military or law enforcement, where coming to the aid of a brother or sister – or any victim – is burned into their psyche. Most would say that there is no higher calling than public service. In fact, many of these “rugged individualists”

were the first to enlist to go to Vietnam, Iraq and Afghanistan. There is nothing more collectivist than that.

Addressing officers who were potentially on the verge of a coup, General George Washington uttered words that serve well today and offer hope that we can rise to Benjamin Franklin’s challenge to the American citizenry: “You will, by the dignity of your conduct, afford occasion for posterity to say, when speaking of the glorious example you have exhibited to mankind, ‘Had this day been wanting, the world had never seen the last stage of perfection to which human nature is capable of attaining.’” Let the dignity of our conduct set the example. **SECURITY**



About the Columnist

Michael Gips is a Principal at Global Insights in Professional Security, LLC. He was previously an executive at ASIS International.

LIFE IS DIFFERENT TODAY



How will your workplace respond?

As you strive to keep employees and visitors safe in this new normal, we are bringing together the latest technology to help you reopen your workplace with confidence.

Explore solutions for your organization at
adtcommercial.com or call **855-ADT-COMM**

ADT Commercial

© 2020 ADT Commercial LLC. All rights reserved. The product/service names listed in this document are marks and/or registered marks of their respective owners and used under license. Unauthorized use strictly prohibited. License information available at www.adt.com/commercial/licenses. 08/20

Communal Efforts are the Way to Better House of Worship Security

By Robert Graves,
Contributing Writer

Faith-based institutions need to be welcoming and inclusive with their duty of care to provide a safe space for worship, even with constraints on safety and security budgets.

There is no hate more pernicious or more persistent than the vilification of people based on their ethnicity or faith, particularly when that hatred is used to justify violence. According to the most recent data

from the Federal Bureau of Investigation (FBI), approximately one in five bias crimes target persons because of their religion. Although houses of worship represent a relatively low percentage of active threat attacks (approximately four percent of events between 2000–2018, according to the FBI), any invasion of sacred spaces will be among the highest impact events any of us ever experiences.

Last year, after a 22-year career as a Special Agent of the FBI and a brief stint in the private sector, I changed careers to devote my energies full-time to the safety and well-being of the Jewish community, joining Secure Community Network, the official safety and security organization of the Jewish community in the U.S. and Canada. Through its partnership with The Jewish Federation of Greater Washington, I have the opportunity to enhance communal security efforts for the security efforts of the Jewish community in the metropolitan D.C. area, addressing the threats and challenges posed by rising anti-semitism. That work has reinforced my belief that it is communal efforts that provide the best path to better house of worship security.

It is impossible to know with any certainty when and where the next attack on a house of worship will be. As security professionals, we know such an attack will likely come again

at some point and that preparedness is key. The best strategy to protect families, communities and institutions is to build within each of these a culture of safety, security and resilience. To this end, I work daily to help synagogues, community centers, day schools and other Jewish organizations in my community to be safer, more secure and better prepared to face threats. I provide advice, education and training, all grounded in the simple truth that it is up to every one of us – individuals, community leaders, parents, teachers, role models – to do all we can to make our community safer.

Faith-based institutions face unique challenges in balancing traditions of being welcoming and inclusive with their duty of care to provide a safe space for worship. Those challenges are exacerbated by constraints on safety and security budgets in a non-profit environment. Security professionals sometimes forget about the budget cycle – even nonprofits have annual budget submission requirements. Formal risk assessments are key to giving institutional leaders a clear picture of what is needed to close any security gaps, understanding their risk appetite, keeping their expectations realistic and allowing them to make well-informed risk management decisions.

In working with faith-based organizations and communities, I apply three fundamental principles of security readiness – maintain situational awareness, harden the facility and prepare to respond to incidents. As with all endeavors, a comprehensive security strategy and plan begins with and succeeds through attention to the fundamentals. It is through the efforts of the members, staff and clergy, working with security professionals, that these principles can be effectively implemented to enhance congregational and institutional safety and security.

Situational Awareness

Safety begins with being alert to the world around us, wherever we may be. The more engaged we are with our environment, the better we can recognize hazards and threats. The more our neighbors know us as people and as a com-

munity, the better positioned they are to notice and warn us of danger, and to stand with us against threats. This holds true for houses of worship and their members, staff and clergy as well.

Most institutions look first to security camera systems to meet their situational awareness needs. Few, however, can afford sufficient numbers of high-resolution digital cameras to cover all external and internal areas they need to monitor. Fewer still can afford dedicated staff to monitor those cameras effectively. With limited resources, security cameras should be prioritized to afford staff a quick, safe means of putting eyes on critical places when needed, and for forensic purposes post-incident. Camera placement should be risk-driven, with priority first to regular access points on the perimeter of the property and the buildings themselves. Second priority should be given to other high-risk or high-concern areas, such as playgrounds, which should be identified through a formal threat, vulnerability and risk assessment. Camera systems should be accessible remotely, so that they can be checked from anywhere on or off the property. Areas covered by cameras should also be covered by an intrusion detection system or other sensors to alert staff of a potential threat and to cue them to check the camera feed. While newer camera systems include advanced analytics for threat or hazard detection and alerts embedded in the system, these are typically very expensive and the artificial intelligence algorithms driving them are still evolving. Until the price point for these systems drops and the effectiveness of the analytics rises, houses of worship are better served by proven and robust, albeit less sophisticated, technologies.

Congregations often overlook the most valuable resource available to them for maintaining situational awareness – their own membership. An engaged membership is the single best situational awareness tool any church, mosque, or synagogue can have to detect potential hazards or threats. Regular attendees should engage strangers the same way they greet members they see each week, in accordance with their traditions, with the aim

of facilitating their worship experience. If they sense something is amiss, they should know to trust their instincts and who to alert for assistance. The congregation's cadre of greeters and ushers, whether they are board members or volunteers, should be trained to recognize potential hazards or threats and to respond appropriately. Such training should include identification of behaviors indicating a potential attack, de-escalation techniques for addressing disruptive persons, recognizing and off-setting implicit bias, basic first aid, and most importantly, knowledge of the institution's emergency response plans and procedures. The aim of that training should not be to make security officers of the greeters and ushers, but to provide them tools to enhance the safety of the congregants and visitors and to enhance the effectiveness of professional safety and security staff.

A third element of situational awareness is developing strong working relationships with local police and other first responders. Sir Robert Peele, founder of the London Metropolitan Police, is famously quoted to have said, "The police are the public and the public are the police." The police are the component of our society that is engaged with threats and hazards beyond the visual range of the house of worship. An active, collaborative relationship between the house of worship and its local police is essential for the police to effectively communicate any alerts and for the congregation to effectively take action on those warnings. Recent and on-going developments add new complexity to community relations with police, and faith-based organizations are uniquely positioned to contribute to community discussions on policing. That contribution should begin with a frank, in-house discussion about what role the police should play in the institution's security strategy and plan. Whether it is critical incident response, deliv-

ering crime prevention and safety education to the congregants and staff, providing visible armed presence during services and events, or some other role, the institution should invest the time to meet with and get to know the local law enforcement that exists to serve them as members of the community. They should meet the officers who

patrol their area, as well as their leadership, and afford the police an opportunity to get to know the congregation and the facility. Congregational leadership should use these meetings to share the institution's needs, concerns and expectations with local public safety officials. As a key constituency of the larger community, when faith-based organizations engage in these conversations with public safety agencies, they can lead and shape that conversa-

tion and can serve as a bridge between law enforcement and the community.

"Just as people check before allowing strangers into their homes, so too should they control entry to their houses of worship."

Facility Hardening

Congregations should work to make themselves tougher targets for potential perpetrators of criminal or terroristic acts. This presents perhaps the most overt challenge to a faith-based organization as it seeks to balance safety and security with openness. There is a tendency, both by congregants and security professionals, to think of facility hardening in terms of measures that risk turning houses of worship into fortresses. There are straight-forward measures which can be implemented, that are both effective and relatively unthreatening to visitors. The simple things everyone already does – or should be doing – to protect their families and homes from criminals offer a blueprint for how to protect community facilities.

Just as people check before allowing strangers into their homes, so too should they control entry to their houses of worship. Every facility should have an affirmative system of access control that

allows it to lock its doors and to identify visitors before admitting them. An electronically controlled lock on entry gates and doors, tied into the security camera system, is a modest expense that can afford the congregation and staff good control of access to the facility, especially during low occupancy times. It should be augmented by greeters and ushers during services and events, as needed, to accommodate crowds. Houses of worship can welcome the stranger without allowing the wolf into the fold.

An extension of access control is the ability to secure facility doors from the inside. It is no surprise that most religious facilities are designed to be locked from the outside (if at all) when they are secured after services or an event. The attack on a synagogue in Halle, Germany, on Yom Kippur in October 2019, demonstrated the importance of being able to lock doors from the inside. That congregation had secured its newly installed security door at the beginning of services, preventing an armed assailant from entering and attacking those inside. Every facility should be able to lock its doors from the inside, especially in an emergency. Ideally, the locking system should be tied to a panic-alarm, which can be used to alert both those inside the facility and 9-1-1 dispatch of a non-fire emergency at the site.

For enterprise security professionals, it may seem obvious, but the importance of routine facility maintenance cannot be overstated and bears repeating. Keeping doors, windows, fences and gates in good repair is a fundamental measure to ensuring a secure facility. Too often, routine checks and maintenance are deferred, either as an oversight or as a cost-saving measure, until there is an incident. Exterior doors and windows should be checked regularly to ensure they readily latch and are secure from unauthorized entry. Fire doors should be checked to ensure panic bars function as designed. Foliage and undergrowth should be trimmed to ensure good lines of sight for camera systems, to minimize places for bad actors to conceal themselves and to reduce fire

hazards. Most police departments have crime prevention officers who can help to identify problem areas and remediations in this area. Having them do a crime prevention survey can be an effective way to build the kinds of relationships described earlier.

The presence of security or facility staff can also serve as a deterrent for criminals or other villains. Routine daily checks of the facility's exterior and grounds, whether by staff members or congregational volunteers, demonstrates that the facility is not easy prey and will likely deter all but the most committed bad actors. The addition of uniformed safety officers, armed security guards, or law enforcement during special events or services adds another very visible layer to that deterrence.

Incident Response

Preparedness to respond to incidents begins with giving advanced thought and planning to hazards and threats that might be encountered. As part of that planning, there should be a commitment to action. We all know the slogan, "See something, Say something." Institutional safety, security and emergency response plans should be based on the principle, "see something, do something." If something seems wrong or out of place, members, staff and clergy should be empowered and encouraged to investigate (if it feels safe to do so). If it does not feel safe, they should be ready to take action by notifying the appropriate person or authority, bearing in mind that the police would rather be called for something that turns out to be nothing, than not be called for something that turns into a tragedy. For each type of emergency in those plans, the decision points for alerting institutional leadership and for alerting public safety agencies should be identified. The policies, protocols and procedures should be well explained to the membership and consistently applied to all, members and guests alike.

The core of incident response is individual and institutional preparedness to act in an emergency. Just as many people are trained to know what to

do if someone is choking or having a heart attack, they should also train to know how to respond to a variety of emergency situations. Members of the congregation and staff should be offered, and encouraged to attend, training to enhance their personal, emergency response skills. While the likelihood of encountering an active threat in a house of worship is low, the skills gained through such training are invaluable if active threats are encountered anywhere and translate to preparedness to respond to other types of emergencies. First aid training, including Stop the Bleed training, could be critical in the event of an attack on a house of worship. It is also a valuable life-skill and is more likely to be used in cases of routine accidents. The emergency plans and procedures should be made available to all members and staff, and trained and drilled regularly. Honing these skills can imbue the congregants and institutions with resilience and self-confidence that dissuades opportunistic predators.

Finally, institutions must report suspicious activities, bias incidents and crime to appropriate authorities for follow-up action. While this is obviously the case for acts involving violence or threats of violence, it is equally true for acts of simple vandalism, trespass, or other petty crime. People who have attacked houses of worship and their members did not wake up on the day of their attack with a new idea to create mayhem or death. They were on a pathway to violence that began some time before. As whatever grievance they held took shape, their ideation assigned blame to persons of a particular faith or ethnicity and rationalized violence against them. They planned and prepared for their attack, along the way telegraphing their intent to those closest to them and in many cases to their intended targets through surveillance, harassment, trespass,

or vandalism. In isolation, such acts may appear minor or unimportant to the institution. The police, however, will likely be able to place incidents in context and assess any threat they may signal. Law enforcement are better positioned to make a determination if under law an incident is

a hate crime, a bias incident or something else. These professionals typically come equipped with specialized skills for identifying, de-escalating and managing hazards and threats that the membership should not be expected to possess or exercise on their own.

A Final Thought

Hate against people and institutions because of their faith is a scourge that has plagued civilization for millennia. As I work daily with the Jewish community of the metropolitan D.C. area in the face of rising anti-semitism, I am evermore certain that the most effective approach to securing houses of worship and their members starts with the basics – maintain situational awareness, harden the facility and prepare to respond to incidents. Nobody can predict or prevent every attack, but by working in collaboration with and supported by security professionals, who understand the breadth and depth of the threats that are out there, houses of worship and their members can be prepared, secure and resilient. **SECURITY**

“Institutional safety, security and emergency response plans should be based on the principle, “see something, do something.”

About the Author



Robert Graves is the Regional Security Advisor - National Capital Region for Secure Community Network. Through its partnership with the Jewish Federation of Greater Washington, Graves provides security advice, assistance, training and information sharing for the safety of the D.C. area Jewish Community. Graves retired from the FBI in 2017 after a 22-year career, focusing on National Security investigations.

DID YOU KNOW?

YOUR FREE DIGITAL SUBSCRIPTION NEEDS TO BE RENEWED EACH YEAR

CLICK HERE TO RENEW NOW!



SECURITY



SecurityMagazine.com

It's Coming: National Cybersecurity Awareness Month



As echoed frequently within the ranks of the military: “Proper Planning and Practice Prevents Piss Poor Performance.” While this truism is most often utilized to whip our nation’s first line of defense into fighting shape, it’s a credo that our cybersecurity community would do well to heed — especially given the fact that the space cybersecurity occupies in the minds of the general populace, while growing, is yet nascent at best.

Flashback to 2004 and the genesis of National Cybersecurity Awareness Month (NCSAM), an initiative created to raise awareness in the U.S. around the importance of cybersecurity. Founded by the National Cyber Security Division within the Department of Homeland Security and the nonprofit National Cyber Security Alliance, NCSAM has taken place each October, since its mid-aughts inception, in efforts to ensure all Americans have knowledge of the resources and tools they need to be safer and more secure online.

So, why am I referencing the NCSAM when it’s still a full month out? Well, it goes back to that famous military mantra, championing pre-

paredness. The last place one wants to receive low marks, especially in today’s increasingly digital and hyperconnected environment, is in cybersecurity. It’s imperative that our community works collectively to develop and advance clear, concise and actionable messaging that not only raises awareness around cybersecurity but promotes manageable tactics and best practices for its adoption. After all, as my Latin professor was quick to remind — “*praemonitus, praemunitus*” — “forewarned is forearmed.”

To that end, this year’s NCSAM is dividing up each week in October into different focal themes. Week 1 of which is: “If You Connect It, Protect It.” Here, the effort is to emphasize that all personal devices connected to the internet are potentially vulnerable to attacks. As the popularity of BYOD and the IoT continue to grow, it’s imperative that organizations have a comprehensive, secure program in place that maximizes both user productivity and satisfaction while cutting costs and facilitating business continuity securely.

Week 2 is a logical extension of Week 1, focused on “Securing Devices at Home and Work.” As millions of us have grown accustomed to and continue working from home, this delineation between work and home has become increasingly porous. Suffice it to say, devices — no matter the environment in which they are situated — must be secure without any performance trade-offs. Enter robust solutions like continuous authentication and unified endpoint security that leverage artificial intelligence, machine learning and automation to provide next-generation cyber

threat prevention across all devices — anytime, anywhere.

And because we're still in the midst of a global pandemic, Week 3 wisely adopts a narrower focus: "Securing Internet-Connected Devices in Healthcare." With cybercriminals targeting health files, insurance data and medical devices, it's critical that the healthcare industry adopts AI-driven technology to help their IT staff secure sensitive information, protect against vulnerabilities and prevent future attacks. This is even more important given the rise of telemedicine, healthcare IoT and the use of contact-tracing apps in efforts to mitigate the current pandemic. Historically, these challenges have posed more of a privacy concern in the minds of many people, which only serves to highlight the importance of an integral, symbiotic relationship between privacy and security. Perfecting healthcare cybersecurity will ultimately allay the privacy concerns of patients while improving overall patient care.

Lastly, NCSAM 2020 wraps up with Week 4 focused on "The Future of Connected Devices." That future is one that must be fortified with a Zero Trust, Zero Touch security model — one where no user, system, or device is automatically trusted within a network. This advanced level of precaution results in an all-around seamless and more secure environment and is something I touched upon, in-depth, in a recent column.

Consider this brief missive, then, as your start-ing signal — a blueprint for preparing strong, resonant messaging next month in the advancement of our collective awareness of ever-evolving cybersecurity knowledge, skills and abilities. **SECURITY**

About the Columnist



John McClurg is Sr. Vice President and CISO at BlackBerry. He previously was CSO at Dell; VP of Global Security at Honeywell International; and a twice-dec-
orated member of the FBI.

**CONTINUING
EDUCATION
CENTER**
ENGINEERING + MECHANICAL SYSTEMS

SECURITY

**SECURITY IN
KNOWING**

Through the CE Center and *Security*,
earn CEUs for free and expand your industry expertise at:
ce.securitymagazine.com
SECURITY

CYBER SECURITY

CYBER ATTACK

You've Been Hacked – Now What?

By Brian Wrozek,
Contributing Writer

If you're reading this article because of the headline, you're in trouble my friend.

Cybersecurity threats come in many varieties – criminals, nation states, malicious insiders, ransomware, phishing, malware...the list goes on and on. But just because there are a lot of moving parts to cyber-

security, it doesn't mean you can't be prepared to respond to a data breach or other security incidents. If you've done your job correctly, you will never ask "now what?" when such an incident occurs, because you'll already have an incident response (IR) plan in place that prescribes exactly what you need to do.

Cybersecurity IR is different from physical security IR, though. With physical security, the top priority is human safety, and then "catch the bad guy" is the second priority. So, you gather all your video and other pieces of evidence to help law enforcement find the perpetrator. Cybersecurity is different. Your top priority is mitigating the damage that's been done, which may include getting the business back up and running. And, since the attacker is usually beyond your jurisdiction, it's rarely a productive use of time to hunt them down, unless it's an insider. The good news is, it's possible to put together a comprehensive and tested plan to effectively respond to cyberattacks. And, you don't have to be a technical person to do

this – you can be the facilitator of a cross-functional team that includes technical people (employees or consultants), as well as other relevant executives.

So, the question everyone needs to ask themselves is not “now what?” – it’s “how do I plan for this?” So, let’s take a look at how to create an effective cybersecurity IR plan.

First Things First - Build a Plan Based on Best Practices

The first step to building an effective cybersecurity IR plan is to adopt an industry-standard IR framework, such as NIST 800-61. This sets the foundation for your plan and dramatically reduces the dreaded “trial and error” that inevitably comes with “do-it-yourself” approaches. NIST 800-61 breaks down IR into four phases:

- **Preparation** - Having an IR playbook in place is key so you’re ready for action should an incident occur. The playbook should define procedures, as well as the cross-functional team required for effective IR. It’s really the same thing as having a physical security IR plan – if someone breaks into the office, there should be a prescribed set of steps to take.
- **Detection and analysis** - Detecting an attack is the first step in any IR plan. Analyzing where the attack came from (internal or external source) and what systems it touched are important for remediation efforts.
- **Containment, eradication and recovery** - Preventing the attacker from moving anywhere else on the network or exfiltrating data (containment) and then ultimately removing them from the network is critical. Once the attacker is removed, recovery can begin – patching vulnerabilities exploited by the attacker, following steps to meet regulatory compliance, etc.
- **Post-incident follow-up** - Reviewing how well the organization executed on its IR plan and applying those “lessons learned” so response can continuously improve is key as well.

Obviously, the preparation phase is the foundation on which to execute the other phases. Given

it’s importance, let’s take a deeper look at this critical stage.

Building the Plan

First of all, if your expertise lies more in physical security than cybersecurity, fear not. There is always help to be had, either among internal technical personnel, or the plethora of outside cybersecurity consultants roaming the world today (ranging from solo practitioners to global consulting firms). These outsourced professionals can be put on an IR retainer, where they can help with everything from the preparation phase, straight through to post-incident follow-up.

At a high level, there are a lot of non-technical aspects to a cybersecurity IR plan that are similar to a physical security plan. For example, you need to choose someone to lead IR, assemble a cross-functional team, do periodic practice runs so people will know exactly what to do if something actually does happen, etc. The cross-functional team typically involves representatives from areas of the company that are responsible for different areas of activity required by the response. So, this would include:

- CISO, CIO or both – Ransomware and breaches have become board-level issues, so there should be executive representatives on the team that can report directly to the CEO and the board.
- Technical leads - These are people responsible for different parts of the company computing infrastructure – security, network, infrastructure, etc. They gather computer logs and evidence to support the investigation (it is common to utilize third-party experts in the forensics efforts).
- Legal - Cyber incidents often have liability issues attached to them. Legal counsel should be part of the IR team to evaluate how a particular incident might open the company to legal exposure, and provide counsel on how to mitigate that exposure.
- HR – Insiders are a major source of cyber risk, and if an employee causes a cyber incident, HR needs to be on the ground floor, so a legal and effective strategy can be developed to address

the employee issue. Likewise, a cyber incident might be the result of a lack of employee training around cyber-safe behavior, so HR should also be directly involved in designing training programs that reduce the likelihood of this happening in the future.

- Corporate communications professionals -

Cybersecurity incidents create all sorts of internal and external communications challenges. If the company has to disclose the breach to comply with regulations, it could wind up being reported in the media. Likewise, if employees' personal information has been compromised, they will need to be instructed

on measures they should take to protect themselves. And, if it's something catastrophic, like a ransomware attack, employees will need to understand how to continue performing their work while the situation is addressed.

- Finance - Responding to a breach may require hiring outside experts or acquiring new technology very quickly. Having corporate finance on the cross-functional team can streamline the process of getting the right skills and equipment, as quickly as possible.

- Risk management leaders - If there is a Chief Risk Officer, a Chief Compliance Officer, or something similar, that person should also be involved in the IR team.

Once the team is established, it is important to define the role of each member as well as communications protocols. This sets the framework for IR. From there, the team should work together to develop response plans for the different types of likely incidents: data breaches, ransomware attacks, denial of service attacks, insider data theft and more.



YOUR NAVIGATOR TO LEADERSHIP IN SECURITY

Expert Consulting Services



For more information:

(202) 670 6364

mike@gipsinsights.com

gipsinsights.com/corporatesecurity

Testing the Plan

Creating a plan is an important first step; testing that plan is equally important. Failure to effectively execute on a plan is often just as bad as having no plan at all. According to the Optiv “State of the CISO” report, 36 percent of CISOs said they do not practice their IR plans at least once per year. Another 19 percent said they practice once per year.

Given the complexity of responding to a cyber incident, this level of practice is insufficient. And, when it’s time to execute on the plan, companies may even find that members of the original IR team are no longer with the company, or their contact information has changed, or new lines of business have started that are not accounted for in the plan. Given the pace of change in business, IR plans should be practiced and updated at least twice each year.

Testing often takes the form of tabletop exercises, where members of the cross-functional IR team spend half a day or more playing “war games” based on a variety of different scenarios. These exercises help team members internalize their responsibilities during a cybersecurity incident, and what steps they need to take based on different scenarios.

Additionally, it is an excellent idea to practice computer forensics processes because they help determine how the attack occurred, what type of attack it was, what damage the attackers did, and whether or not attackers are still on the company network.

A good way to practice forensics is to randomly choose a system and have the appropriate person conduct forensics on it. Capturing disk images and searching log files can take hours, so practicing will ensure forensics are conducted as efficiently as possible if an actual attack occurs.

“Creating a plan is an important first step; testing that plan is equally important.”

Every Incident Creates New Questions

Some measures during IR are prescribed. For example, if your company is regulated and required to report a breach within 72 hours, that is pretty straightforward. But in cases where things are not that clear, many business and technical questions can arise.

For example, if you’re hit with ransomware, do you call the police? If an intruder is still on the network, do you take emergency action and shut down your internet connection to stop data from leaving the company? Or, if it’s an insider attack, should you let the attacker continue so you can catch him in the act?

Questions like these will invariably come up – and in many cases, you may face questions you haven’t considered before. But, if you have a rehearsed plan in place and your IR team is executing properly, you will have more time and resources to dedicate to finding the best answer, rather than being distracted by endless firefights because you were not prepared for the incident. Put another way, you won’t have to devote any resources to figuring out “now what?” Instead, you can focus on the most important issues leading to the company’s recovery to normal. **SECURITY**

About the Author



Brian Wrozek is a seasoned cybersecurity executive with more than 20 years of experience in IT and information security and management.

As CISO at Optiv Security, Wrozek oversees all corporate security functions including cyber operations, incident response, vulnerability management and security governance activities.

Get to Know the Standards Advancing Cybersecurity

Cybersecurity Lab

EAT•N
Powering Business Worldwide

Eaton has the first research and testing facility approved to participate in UL's Cybersecurity client lab validation program in Pittsburgh, Penn. *Image courtesy of Eaton*

By Max Wandera,
Contributing Writer

There are currently a multitude of different standards and regulations to address the urgent need to secure our connected world, yet it's time to create a unified global conformance assessment.

A world with amped up connectivity and electrical demand needs confidence that connected systems are constructed with trusted products. The exponential growth of the Industrial Internet of Things (IIoT) is creating a crucial need for robust cybersecurity practices and

well-defined standards that provide customers with confidence that their connected devices will operate securely throughout their entire lifecycle.

By 2025, 41.6 billion connected devices will be generating 79.4 zettabytes (ZB) of data that will need to be securely maintained and processed. Analysts forecast that this increase in connected devices and the data they generate will continue to grow exponentially. The resulting increase in critical data and computing is expected to require four times more electricity over the next decade.

These factors make cybersecurity a must-have for product development, much like safety and quality. Manufacturers need to develop connected products with security in mind by ensuring we have the right talent, are leveraging the right technologies and embedding cybersecurity best practices throughout our product development lifecycle.

Understanding Device-Level Cybersecurity Certifications

For power management that is digitalized and connected, UL created its 2900 Standard for Software Cybersecurity for Network-Connectable Products (UL 2900). These guidelines were the first of their kind and include processes to test devices for security vulnerabilities, software weaknesses and malware. This standard confirms that the device manufacturer meets the guidelines for:

- Risk management processes.

- Evaluation and testing for the presence of vulnerabilities, software weaknesses and malware.
- Requirements for security risk controls in the architecture and product design.

UL also provides a Cybersecurity Client Lab Validation program for manufacturers, which certifies testing laboratories with the global capability to test products with intelligence or embedded logic to key aspects of its 2900 standard. By purchasing products tested in these specialized labs, customers can rest easier, knowing their devices are compliant with the industry's highest cybersecurity requirements before they are installed in critical systems.

Similarly, the International Electrotechnical Commission (IEC) adopted the 62443 series of standards, which provides a framework to address the cybersecurity of Industrial Control Systems. These standards provide requirements for all of the principal roles across the system lifecycle – from product design and development through integration, installation, operation and support as described in the image. In 2018, the IEC added 62443-4-2 to improve the security of products.

Eaton was the first company in its industry to achieve dual certifications for rigorous IEC 62443 and UL 2900 product certifications. Our uninterruptible power supply (UPS) connectivity devices meet both IEC 62443-4-1, 62443-4-2 and UL 2900-1 cybersecurity standards. We also possess the first lab approved to participate in UL's Cybersecurity client lab validation program – providing the capability to test Eaton products with intelligence or embedded logic to key aspects of the UL 2900 Standards.

Beyond these device-level standards, cybersecurity is essential in the overall development of a product lifecycle. Product cybersecurity certifications are needed to support trusted connectivity. It is just as important to validate that secure product development principles are applied by manufacturers. This can be confirmed by manufacturers that follow an accredited Secure Development Lifecycle (SDL), which ensures cybersecurity has been embedded throughout the entire product development process.

Why is Secure Development Lifecycle (SDL) Important?

A “Defense-in-Depth” mechanism that is effective today may not be effective tomorrow because the vulnerabilities keep evolving. This is why administrators of industrial control system networks must be ever-alert to changes in the cybersecurity landscape and work to prevent any potential vulnerabilities.

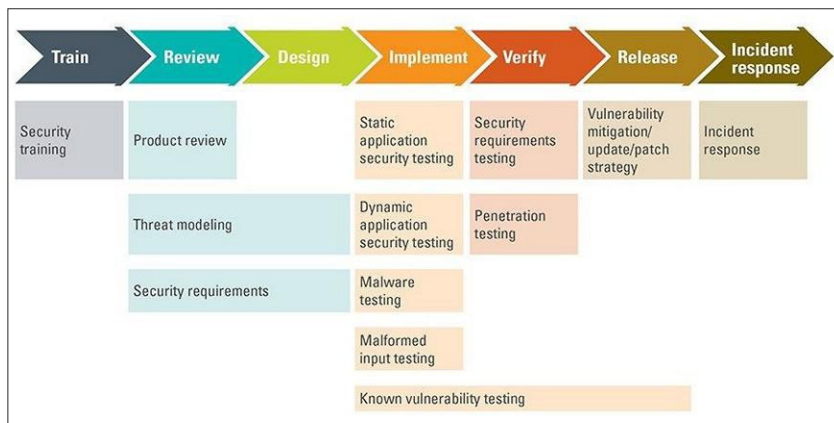
SDL was created in response to an increase in virus and malware outbreaks at the turn of the twenty-first century. This approach to product development places cybersecurity front and center from inception to deployment and lifecycle maintenance. SDL can help manufacturers stay ahead of cybercriminals by managing cybersecurity risks throughout the entire lifecycle of a product or solution.

For manufacturers, adopting a SDL approach that has been validated by a third-party is critical to creating trusted environments. It's the third-party certification that gives customers confidence in the processes and technologies they're applying, much like safety certifications and standards in the National Electric Code.

Although SDL is not an inherent code or standard, it does dictate how cybersecurity should be integrated into processes for product procurement, design, implementation and testing teams.

IEC 62443-4-1 lays out guidelines for secure product lifecycle development in the electrical industry. The IEC guideline specifies process requirements for the secure development of products used in industrial automation and control systems. It defines a secure development lifecycle for developing and maintaining secure products. These guidelines can be applied to new or existing processes for developing, maintaining and retiring hardware, software or firmware for new or existing products.

Third-party validation for SDL processes is important because it provides customers with confidence and helps reduce risk by confirming that the technologies and processes they're applying comply with proven industry guidelines. At Eaton, we take SDL very seriously to proactively



The IEC 62443 series of standards provides a framework to address the cybersecurity of Industrial Control Systems. *Image courtesy of Eaton*

manage cybersecurity risks in products through a framework involving threat modeling, requirements analysis, implementation, verification and ongoing maintenance.

The Importance of Unifying Global Cybersecurity Standards for Connected Devices

Moving forward, advancing cybersecurity in our increasingly connected world will require industries and standards organizations to identify a unified global criterion for assessing products. To help create a more cyber-secure future through global standardization we have partnered with UL, the International Electrotechnical Commission (IEC) and other industry partners to drive for development of a global cybersecurity conformance assessment for power management products.

Think of it this way: the security of a network or system is only as strong as its weakest link. As more manufacturers and industries build and deploy IIoT devices, the security and safety of systems providing essential operations become more important and more difficult to manage. These complexities are due, in part, to a lack of a global, universally accepted cybersecurity standard and conformance assessment scheme designed to validate connected products.

The economic challenges to safeguarding IIoT ecosystems spawn from the complex manufactur-

ing supply chain and the difficulty of assigning clear liabilities to manufacturers and system integrators for any vulnerabilities introduced. Most products and systems assemblies consist of components from different suppliers. Where should the element of trust begin and end if there is no global conformity assessment scheme to ensure that products and systems are designed to be compliant with the global standards defined by the industry?

There are currently a multitude of different standards and regulations created by various organizations, countries and regional alliances across the globe. All of these standards and regulations address the urgent need to secure our connected world; however, they also create the potential for confusion and possibility of weak links in critical infrastructure ecosystems. A unified global conformance assessment would address these challenges and more. The time to drive this singular certification is now. We are working with leaders across the industry to do just that. **SECURITY**

About the Author



Max Wandera, as director of the Cybersecurity Center of Excellence at Eaton, provides leadership and oversight for the research, design, development and implementation of security technologies

for products, systems and software applications. In his position, he is also responsible for Eaton's Secure Product Development Lifecycle Policy and compliance. Wandera holds Global Information Assurance Certification (GIAC) Security Leadership and Certified Information Systems Security Professional (CISSP) accreditations. His expertise enables him to act as the voice of Eaton on product cybersecurity matters and lead cross-functional collaboration with corporate officers, industry leaders and government entities, including the Cybersecurity and Infrastructure Security Agency (CISA) to shape the future of cybersecurity and trusted connectivity.

Derailing Ransomware 2.0 Requires a Little Trickery

Ransomware attacks are on the rise – and they are getting more and more sophisticated and destructive. That is bad news for executives struggling to maintain a high level of cybersecurity even as their organizations continue to cope with the massive impact of a pandemic.



somware that can spread across a corporate network and infect systems by encrypting data so it cannot be accessed. Even worse, it also steals the data it finds, and then exfiltrates the data to servers controlled by hackers who then threaten to release it if a ransom is not paid. Maze regularly targets

The good news? Technology is available to help companies better defend against ransomware, a type of malware that threatens to publish a victim organization's data or continually block access to systems unless it pays a ransom via cryptocurrency.

Recent ransomware developments show just how dangerous these attacks have become. Here is a brief sampling:

- **Zeppelin:** The newest member of the VegaLocker family of ransomware, first seen in November 2019, is an example of increasingly common ransomware-as-a-service (RaaS), where cybercriminals develop ransomware and sell it to others or rent it and take a portion of any ransom collected. Zeppelin is thought to rely on water-holing attacks, in which Web sites likely to be visited by targeted victims are embedded with malware.
- **Sodinokibi:** Another example of RaaS, and also known as REvil, it was discovered in April 2019 and exploits known security vulnerabilities and phishing campaigns. The ransomware encrypts a user's files and can gain administrative access by exploiting vulnerabilities.
- **Maze:** A sophisticated strain of Windows ran-

managed service providers, so by infecting one company it can possibly infect many more.

- **RobbinHood:** A ransomware family that targets organizations using a vulnerable kernel driver to prepare systems for encryption. In 2019, the ransomware creators successfully attacked and received ransom payouts from a number of U.S. cities. RobbinHood ransom demands can range from three bitcoins for a single computer to 13 bitcoins for a complete network, which amounts to tens of thousands of dollars.

There are many more. The point is, ransomware is far more insidious today than in the past, and in some cases, it is designed to attack specific types of businesses to maximize returns for the cybercriminals who write the malware.

The new, more advanced attack techniques used by cybercriminals enable them to disable security software tools and deploy ransomware on highly specific targets. These attacks also go beyond indiscriminately encrypting any data they come across. Instead, they target data that is critical to the business. Such attacks require criminals to conduct lateral movement activities such as stealing credentials, discovering network assets, prob-

ing for open ports, querying Active Directory for critical objects and escalating privileges.

Traditional security tools such as endpoint detection and response (EDR) systems and endpoint protection platforms (EPP) are important in fighting against ransomware. Advanced EDRs examine process flows and chains to see if something looks unusual. These types of observations can be helpful after an attack. As teams investigate an incident, EDR can provide the process flows it mapped during the attack.

EPP provides capabilities such as automated patch management, maintaining devices remotely and protecting endpoints from attacks.

Such tools do not stop all types of attacks, however. They are not designed to detect all ransomware methods, especially lateral movement. In order to successfully defend against the newest and most sophisticated ransomware attacks, organizations need to have a layered approach that supplements EDR, EPP and other legacy tools with additional capabilities.

Here is what cybersecurity teams need to do to build a comprehensive and effective defense against the latest ransomware:

- Protect data so attackers cannot find it or access it. Cybersecurity teams have long made it a top priority to deploy multiple layers of data protection. But with ransomware attacks becoming more sophisticated and destructive, protecting data has become even more critical. A key part of this is protecting the endpoints that generate and house so much of a company's data resources and having early detection and effective alerting of attacks. Detecting attacks early can lead to substantial cost savings.
- Leverage endpoint protection functions to effectively prevent attacker lateral movement by anticipating attack methods and efficiently derailing these efforts. For example, by providing Active Directory query redirections and deceptive credentials and shares, organizations can feed attackers false information and quickly redirect them away from production assets.

- Protect the endpoint so attackers cannot see real files, folders, removable storage, network shares, or cloud storage, only decoys. If the ransomware cannot find production data, it cannot have any negative affect on it. Companies can create an environment where every endpoint becomes a decoy that is designed to disrupt an attacker's ability to break out and further infiltrate a network. This can be done without requiring agents on the endpoint or causing disruption to the endpoints or network operations. In this way, an organization can gain early alerting of lateral movement activities while misdirecting the attack into the decoy environment to collect forensics evidence, which can speed up adversary intelligence development and attack analysis. The decoy environment can even feed the ransomware unlimited data to keep it from moving on to other production targets.

There is no getting around the fact that ransomware attacks continue to rise in number and gain in sophistication. That means organizations need to understand the importance of creating multiple layers of protection.

While there is no single solution to defending against all ransomware attacks, a strategy that combines traditional tools with newer solutions featuring deception-based detection within the network can help companies bolster their defenses to a much greater extent.

Such advanced technology can quickly find multiple types of lateral movement and has the ability to hide assets and redirect ransomware to deceptive file shares. Working in unison, cyber deception and EDR/EPP tools create a comprehensive cyber defense that enables companies to outsmart the smartest ransomware. **SECURITY**

About the Author



Carolyn Crandall holds the roles of Chief Deception Officer and CMO at Attivo Networks. She is a high-impact technology executive with more than 30 years of experience.

Product Spotlight

on Surveillance for Airports/Seaports

PTZ Domes for Challenging Lighting Conditions

➤ Spectra Enhanced series of PTZ domes are ideal for airport applications with challenging lighting and broad surveillance areas with long perimeters to monitor. Spectra



Enhanced 7 combines PTZ technology in one camera. It offers 4K resolution with 18x optical zoom, enabling a much wider field of view for better detection, classification and identification. Built with a frameless direct drive motor system with fast and automated tracking, it eliminates the risk of PTZ cameras pointing out the wrong direction and missing valuable threat information. Airports can now get on target quickly and accurately for fast response time. Powered by deep learning algorithms, analytics are quickly set up and improve detection accuracy with lower false positives. It increases the camera's ability to easily categorize objects within the scene, tracking and counting of people and vehicles. Airport personnel can focus on situations needing immediate attention and analyze information to improve operation efficiencies.

Find out more at www.pelco.com/airports

Security Center for Airports

➤ Genetec Security Center for Airports enables security managers, terminal and ground handling staff, control room operators, and passenger



experience managers to work together using a single unified product. In addition to video management (Security Center Omnicast), access control (Security Center Synergis) and Automatic License Plate recognition capabilities (Security Center AutoVuTM), Security Center for Airports features a number of airport-specific capabilities including:

- Security Center Flight Business Logic: correlates flight information with other operational resources and automates surveillance and operation management based on flight and gate information so security teams are always in sync.
- Security Center Boarding Route Management: uses Security Center SynergisTM to define specific routes and streamline boarding and deplaning operations.
- Security Center Restricted Area Surveillance: relies on multiple intrusion detection technologies (radar, LiDar, fence intrusion detection, video analytics, drone detection, etc.) to detect potential threats across wide areas to strengthen tarmac, aircraft, traveler and staff security.
- Security Center Passenger Analytics: an advanced analytics solution that extracts valuable insights from sensors like security cameras. Helps measure and visualize passenger counting, queues and occupancy to predict the passenger flow and send notifications to mitigate bottlenecks.

Find out more at www.genetec.com

Intrusion Detection and Object Tracking

- Vicon's new series of high-powered thermal sensor



Shown here integrated with PTZ

cameras integrate with high-speed SN683D PTZ dome camera to detect, identify and track intruders using thermal detection and is combined with

targeted surveillance from the PTZ for full situational awareness. When a threat is detected the PTZ automatically slews to cue, providing immediate confirmation and forensic coverage. Detection alerts automatically notify personnel of potential threats. The thermal detection system decreases the number of security personnel needed to monitor critical areas in traditional detection and surveillance.

Find out more at www.vicon-security.com

Moving Cameras Made for Extreme Environments

- Bosch MIC IP cameras are rugged, constructed



from anti-corrosive metal, and can function at -40°F to +149°F. Its built-in Intelligent Video Analytics technology provides maximum situational awareness in demanding environments. With Camera Trainer, a machine learning functionality, MIC IP cameras can recognize user-defined target objects, including moving and non-moving

objects, to alert operators of unusual scene activity. The 4K UHD version provides high-resolution for mission critical applications such as city surveillance and congested highways, making them ideal for ports and airport perimeters.

Find out more at www.bosch.com

SECURITY SUMMIT 2020

Don't miss the BlackBerry Security Summit 2020
Virtual Conference on October 6-7.

With cybersecurity threats on the rise, there are new demands and considerations required to protect remote workforces in our reality of 'home as the new enterprise' – join us to learn, explore and connect.

www.blackberry.com/securitysummit

 **BlackBerry**

> Classifieds

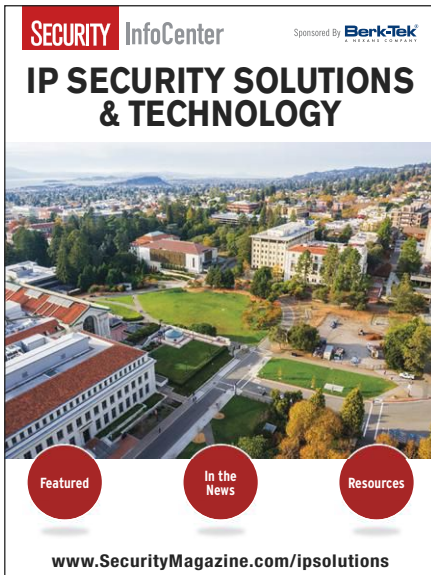
> Operations Center Equipment



COMMAND AND CONTROL

PROMO CODE
CCSPRNG20

commandandcontrolconsole.com
800-984-3135



SECURITY InfoCenter Sponsored By **Berk-Tek**

IP SECURITY SOLUTIONS & TECHNOLOGY

Featured In the News Resources

www.SecurityMagazine.com/ipsolutions

> Industry Calendar

> September 21, 2020 – September 25, 2020

GSX+ Virtual Event

www.gsx.org

> October 5, 2020 – October 7, 2020

ISC West Virtual Event

www.iscwest.com

> November 18, 2020 – November 19, 2020

ISC East, Javits Center, New York

www.isceast.com

> Ad Index

Advertiser	Page#	Website	Phone
ADT	49	adtcommercial.com	855-ADT-COMM
Aiphone	25	aiphone.com/SecMag_Sept	...
Allied Universal	13	aus.com	...
Axis Communications, Inc.	9, BC	www.axis-communications.com/sm/occupancy	...
BlackBerry	68	www.blackberry.com/securitysummit	...
Delta Scientific	21	www.deltascientific.com	661-575-1100
DKS Doorking	3	doorking.com/cloud	800-673-3299
Farpointe Data	23	www.farpointedata.com	408-731-8700
G4S	5	www.G4S.us	888-645-8645
GIPS Insights	60	gipsinsights.com/corporatesecurity	202-670-6364
Hanwha Techwin America Inc.	IFC	HanwhaSecurity.com	...
HID Global Corporation	7	hidglobal.com/mobile50	...
Learn & Earn	8	ce.securitymagazine.com	...
LIVE Earth Software Webinar	35	SecurityMagazine.com/webinars	...
Mission 500	33	mission500.org	...
Northland Control Systems Inc. Webinar	31	SecurityMagazine.com/webinars	...
Par-Kut International	47	www.parkut.com	800-394-6599
Security Magazine Bookstore	37	www.securitymag.com/books	248-244-1275
Security Magazine	55	SecurityMagazine.com/subscribe	...
Solutions by Sector	45	SecurityMagazine.com/webinars	...
Speco	19	specotech.com	...

This index is for the convenience of our readers. Every care is taken to make it accurate. Security Magazine assumes no responsibility for errors or omissions.

SECURITY (ISSN: Digital 2329-1443) Volume 57, Issue 9 - is published 12 times annually, monthly, by BNP Media II, L.L.C., 2401 W. Big Beaver Rd., Suite 700, Troy, MI 48084-3333. Telephone: (248) 362-3700, Fax: (248) 362-0317. Copyright 2020, by BNP Media II, L.L.C. All rights reserved. The contents of this publication may not be reproduced in whole or in part without the consent of the publisher. The publisher is not responsible for product claims and representations. Change of address: Send old address label along with new address to SECURITY, P.O. Box 2146, Skokie, IL 60076. Email: security@omeda.com. For subscription information or service, please contact Customer Service at: Phone: (800) 952-6643 Fax: (847) 763-9538.

> On the Web

at www.SecurityMagazine.com

> Ensuring the Safety and Security of Atlanta United

How does Scott Ashworth, Director of Security, ensure the safety of Atlanta United's fans, players and assets, while helping create a positive and unique game day experience?

> Data Protection by Design:

Eight Questions to Help Protect User Data from the Start

By implementing a data protection by design approach, both before and during product development, organizations will build more trust with customers and end users and curtail risk of future privacy-related conflicts.

> Keep Up Through Security's eNewsletter

Bi-weekly - sign up at securitymagazine.com

> Check Out Today's Cybersecurity Leader eNewsletter

Monthly - sign up at securitymagazine.com



Low-touch solutions for access management.

AXIS Visitor Access for AXIS Entry Manager

Looking for a solution that allows you to easily control who enters a building and when...without the need to buzz visitors in? With AXIS Visitor Access, you get an easy add-on application for AXIS Entry Manager, making it simple for small sites to grant visitors access using a **QR code** as a credential. All you need is an AXIS A1001 Network Door Controller and an Axis door station.

For more information, please visit:
www.axis-communications.com/visitoraccess/SM920

