SUBJECT MATTER EXPERT REFERENCE GUIDE

Guide Overview

For more than six decades, ASIS Annual Seminar and Exhibits (ASIS 2017) has been the premier event for security professionals worldwide, providing industry-leading education, countless business connections and the latest products and services. This year, ASIS is providing this reference guide to serve as a resource for media representatives looking for sources on-site, as well as a reference for future story opportunities. We encourage you to reach out directly to the experts included in this guide, and use the quotes provided – with attribution to the designated individual – in articles associated with ASIS 2017.

Applied Research Associates, Inc.

Active Shooter

Security System Engineering/Design

Critical Infrastructure Protection

Anti-terrorism

Joseph Smith, PSP
Director & Senior Vice President
jsmith@ara.com
601-638-5401

Marketing/PR Contact
jsmith@ara.com

What is the biggest challenge facing the industry today? We risk becoming an after thought for most people. Security must be integrated even more into our lives and businesses. To accomplish this security must be seamless to our users.

What do you see as the greatest opportunity for innovation? The advent of truly ubiquitous computing and access to the internet will create security challenges but also open up unlimited potential. Securely providing what appears to be full and open access to the internet is an area where innovation is required and demanded.

What do you think will have the biggest impact on the industry in the next 3-5 years? If we allow terrorism to become the new normal and our expectations of freedom and security are diminished, we shall have lost the battle. We must not become complacent or numb to the horrors we face.

Professional Bio

Joseph Smith, PSP is a security and blast protection consultant with over 35 years of experience in security engineering and explosion effects from conventional, nuclear and improvised (terrorist) explosions. He holds civil engineering degrees from the U.S. Air Force Academy and Columbia University. Mr. Smith serves as a Director and Senior V.P. of Applied Research Associates, a 1,200 person engineering & sciences consulting firm where he leads the company's Security Engineering & Applied Sciences business. He has developed and tested hardening technologies to protect against nuclear weapons while serving at the Air Force Weapons Laboratory. He has led teams for security assessments of many national monuments, icons and critical infrastructure. Mr. Smith is a frequent speaker and has spoken at numerous ASIS International Annual Seminars.

Arbor Insight

Booth #420

Crime/Loss Prevention

Enterprise Security Risk Management

Workplace Violence Investigations

Scott LaVictor
CEO
scott.lavictor@arborinsight.com
734-992-7267

Marketing/PR Contact
hello@arborinsight.com

What do you see as the greatest opportunity for innovation? The combination of mobile technology and Artificial Intelligence, specifically Machine Learning, has the opportunity to vastly increase both the quality and value of incident reporting from security professionals and the general workforce alike.

Professional Bio

Scott LaVictor is CEO at Arbor Insight, home of Neighborhood Watch for Corporations™ and Intelligent Digital Elicitation,™ a technology that uses Artificial Intelligence to uncover better information from human-computer interactions. Scott is a veteran of the U.S. Intelligence Community and recently managed Corporate Investigations for a Fortune 150 manufacturer.

ASSA ABLOY Americas

Booth #3203

Cybersecurity/ Information Security

Critical Infrastructure Protection

Active Shooter

Security System Engineering/Design

Peter Boriskin
Vice President of Product Management
Peter.Boriskin@assaabloy.com
503-621-2675

Marketing/PR Contact
Erik Hidle
Senior Account Executive
erik@brand-definition.com

Professional Bio

Peter Boriskin is the vice president of commercial product management for ASSA ABLOY Americas. He has 20 years of experience working with security technology, particularly the enterprise security marketplace. In his previous roles, Boriskin was the product management leader for UTC Fire & Security's Lenel business and the vice president of product management for Tyco International's Access Control and Video Systems division. Extensively trained in network security, threat assessment, and incident management, he was part of the founding team for the Open Security Exchange. Boriskin is an active member of ASIS International.

What is the biggest challenge facing the industry today? Based on recent events in the industry, the biggest challenge would be the move from "physical security" and "logical security" as two separate disciplines to looking at them both as "security," or as the management of security assets from an IP perspective. In the past few months the industry has seen instances where digital locks received firmware updates that bricked units, as well as cameras that were compromised by malware attacks. The security of security is an issue that is front and center right now. Years ago we talked about the convergence of physical and IP security. Now we see organizations, from a manufacturer standpoint, jumping in to that concept of securing digital security components with both feet. Because the stakes are so high, we must proactively manage this convergence. We need to recognize that there is no longer a difference between logical and physical security and just talk about security.

What do you see as the greatest opportunity for innovation? I think one of the biggest opportunities right now is to tailor our security products and solutions to help our customers do what they do for a living better, faster and more securely. I think we have a good handle on providing security. We have a good handle on providing solutions that support all the connected components. Now we should focus on how we help our customers go beyond just safety and security to an approach that considers how to protect people, property and assets in such a way that makes them more effective and more efficient. How can security solutions help them improve their workflow? Cabinet locks in a hospital are a great example of this. Operationally, if the doctors and nursing staff can have medicines, even controlled medicines, located securely in a patient's room then we are making their jobs easier and giving them more time to focus on patient care. By seeking out other opportunities to improve operational efficiency, we can provide greater value to our customers.

What do you think will have the biggest impact on the industry in the next 3-5 years? Mobile technologies will have a huge impact. With the proliferation of mobile devices, and with network providers offering unlimited data at reasonable costs, it is lowering the barrier to entry for mobile technologies in security. I think it's going to be the standard fare to have continuously connected data in your pocket along with all the technologies in that little black rectangle. I think that is going to be a big change in our industry. Once we hit a tipping point of people using that device for cashless payments and access control, we are really going to see it accelerate.

Martin Huddart
President, Access and Egress Hardware Group and Vice President, Electronic Access Control Technologies
martin.huddart@assaabloy.com
503-621-2675
Booth #3203

What is the biggest challenge facing the industry today? One of the biggest challenges facing the industry today is for end users to pick amongst a dizzying array of new technologies available to them to secure their facilities. With the rapid pace at which new technology is being introduced, it can be difficult to know that you are selecting the best technologies for your organization and that you are using them in the most effective way. In addition, you want to ensure that any new technologies are able to integrate with existing systems and are future proofed to anticipated needs down the road.

What do you see as the greatest opportunity for innovation? I see making security solutions easier to deploy and manage as one of the next greatest opportunities for innovation. I may not have said this a few years ago, but now that there are so many options for securing all types of doors, it is our responsibility as manufacturers to ensure that these advancements are easily deployed and maintained. We can collectively make the selection, integration, installation, commissioning and maintenance of security technology much simpler for the access control system manufacturer, the integrator, and the end user.

What do you think will have the biggest impact on the industry in the next 3-5 years? Looking further out, I believe that there are two trends that will impact the industry over the next 3-5 years. Mobile is first, then further out it will be Artificial Intelligence (AI). Mobile has and will continue to impact every aspect of our lives, including the way we manage access. Eventually the phone (or whatever wearable it morphs into) will be your key. AI will fundamentally change many industries. Currently, there are many companies trying to make our homes smarter by creating algorithms for 'robots' to make smarter decisions on behalf of humans for security, HVAC and lighting to name the big three. As our homes become 'smarter', the same will happen in the Industrial IoT space for schools, hospitals and government buildings. We live in interesting times in the security industry.

Athos Group

Enterprise Security Risk Management

Soft Target Protection

Workplace Violence

Jeffrey Sweetin
Executive Vice President, Operations
jsweetin@athosgroup.com
720-234-1003

What is the biggest challenge facing the industry today? Over-dependence on a single solution. Whether it's technology, barriers, or guards, organizations that select one countermeasure and build their program around it, are under-securing their assets. Effective security integrates multiple solutions.

What do you see as the greatest opportunity for innovation?Use of technology to increase the efficiency of security personnel. Technology is often seen as an alternate to security personnel. There are great opportunities in the industry for technology to augment and leverage human security assets.

What do you think will have the biggest impact on the industry in the next 3-5 years? Increased acceptance by corporations of the need for multi-faceted internal security programs. Security will continue to move to the forefront in critical areas: budget, construction, etc.

Professional Bio

Jeff serves as Executive VP for the Athos Group, a corporate security outsourcing and consulting firm. At Athos, Jeff provides solutions for corporate clients from a wide variety of sectors. Before Athos, he served as Security Director for Encana, an international energy producer. Before Encana, Jeff was the Regional Security Director for Anadarko Petroleum Corporation. In 2012, Jeff retired after 27 years as a DEA Special Agent and Executive holding positions including Director of Training and Special Agent in Charge of DEA's Denver Division. In 1986, Jeff began his law enforcement career as a police officer in Arlington, Virginia, where he served 4 years. Jeff, a recognized speaker, holds a bachelor's degree from Towson University and a Master's in Education from the University of Virginia.

Avigilon Corporation

Booth #4056

Security System Engineering/Design

Critical Infrastructure Protection

Cybersecurity/ Information Security

Dr. Mahesh Saptharishi
Chief Technology Officer
Mahesh.Saptharishi@avigilon.com
604-629-5182

Marketing/PR Contact
Amy Day
Manager, Global Communications
amy.day@avigilon.com
604-785-5637

What is the biggest challenge facing the industry today? The biggest challenge facing the industry today is that the volume of video data captured far exceeds the capacity of human attention. However, through the power of AI, we are developing technologies and products that dramatically increase the effectiveness of security systems by focusing human attention on what matters most.

Professional Bio

Dr. Mahesh Saptharishi has over 17 years of experience developing intelligent video analytics technology as well as software and camera hardware specifically for the security industry. As Chief Technology Officer, Dr. Saptharishi is responsible for driving innovation in Avigilon's product and intellectual property portfolios, identifying strategic technology capabilities, and exploring new business opportunities. He previously served as Senior Vice President, Analytics and Data Science at Avigilon and has been with the company since its acquisition of VideoIQ Inc. in January 2014 where he was President, Chief Technology Officer and Co-founder. Dr. Saptharishi also co-founded and led the core analytics team at Broad Reach Technologies, Inc., where he was Vice President of Research & Development. He received his Doctorate in Machine Learning from Carnegie Mellon University and has also authored multiple peerreviewed scientific publications, articles and patents.

BrightPlanet

Cybersecurity/ Information Security

Enterprise Security Risk Management

Anti-terrorism

Tyson Johnson
VP - Strategy & Business Development
tjohnson@brightplanet.com
905-510-0750

What is the biggest challenge facing the industry today? Internally, the ability of security risk management executives to develop the business cases needed to fund and implement successful programs.

Professional Bio

Tyson currently develops strategy and solutions for clients at the crossroads of open and internal data. Developing unique ways to leverage all-source information and leading edge technologies to manage risk.

What do you see as the greatest opportunity for innovation? Innovation through the development of new solutions to changing threats across digital, physical, cyber, etc. Understanding how it all fits together and how to implement new solutions across a number of stakeholders. The security professional must innovate to remain current and successful.

What do you think will have the biggest impact on the industry in the next 3-5 years? The growth in cyber risk - the unavoidable reality that most all risk issues will touch the online world. The advancements in cyber security integration and its ability to keep pace with the bad actors.budget, construction, etc.

City of Newport News

Critical Infrastructure Protection

Soft Target Protection

Workplace Violence

Yan Byalik, CPP
Security Administrator
ybyalik@nnva.gov
757-926-7476

What is the biggest challenge facing the industry today? The issue with security is that we are in the prevention business. When something happens, everyone says it's because we failed to prevent it. Our failures are very public but proving that we were successful, that is far more illusive. How do we convince people that we deterred something, that we stopped something? So the challenge today is, really, staying relevant in a dynamic and more virtualized world; Its convincing our stakeholders that each day that nothing bad happened is in its own way a success.

Professional Bio

Yan has over 16 years of experience in campus, theme park, and municipal security including over a decade in security management. A graduate of Virginia Tech, he has authored and co-authored a number of articles and book reviews in security and serves as the ASIS Region 5A ARVP.

Emergency University

Crisis Management

Odelia Braun, M.D., J.D.
Chief Medical Director
tfarina@emergencyuniversity.com
866-233-4357

Marketing/PR Contact
T. Farina
Marketing/PR
tfarina@emergencyuniversity.com
415-999-5766

What do you think will have the biggest impact on the industry in the next 3-5 years? Incorporating the general workforce into Corporate Security's Emergency Response Plans. By recognizing that untrained personnel are typically the first to witness an emergency situation, it is essential that we provide them the ability to efficiently alert trained security/ responders to the scene of the incident via emerging technologies. Thus the response and save rate will greatly improve and victims will not continue to die needlessly in medical emergencies or disasters.

Professional Bio

Dr. Odelia Braun has always been an emergency response innovator/educator. Since becoming a Board-certified emergency physician, she has been actively involved in clinical research and developing cutting-edge programs, which enhanced emergency response systems and improved survival rates long before they became accepted in the mainstream. In addition to her medical degree, she became an attorney, which has lent a very practical perspective of the corporate world. Dr. Braun founded Emergency University with the vision that corporate entities could drastically improve safety and thus survival with anemergency response system model that is customizable, yet standardized and in line with proven public sector systems! Emergency University works extensively with government and global corporate clients.

ESCO Communications

Security System Engineering/Design

Critical Infrastructure Protection

Enterprise Security Risk Management

Jay "Chuck" McCormick, PSP
Technical Solutions Engineer
chuck.mccormick@escocommunications.com
317-557-0753

Marketing/PR Contact
T. Farina
Marketing/PR
tfarina@emergencyuniversity.com
415-999-5766

What is the biggest challenge facing the industry today? Moving from being commodity driven to a knowledge driven industry. Application of the commodity is where ROI and longevity

Professional Bio

Thirty plus years' experience and expertise in every phase of solution engineered physical security systems. Identifies through comprehensive site physical security assessment documentation to develop, implements and maintains security processes that reduce risk and limit exposure to liability. Performs discovery interviews, quantitative lighting assessments, product selection, single/ multi-site design, field operation inspection, and commissioning. Driven by passion for security, integrity, education and holistic problem solving.

What is the biggest challenge facing the industry today? Hosted services for verified alarm response.

What do you think will have the biggest impact on the industry in the next 3-5 years? Continued convergence and understanding of network topology

Federal Protective Service

Booth #5201

Active Shooter

Crisis Management

Critical Infrastructure Protection

Anti-terrorism

Richard Swengros
Deputy Director, Operations
richard.w.swengros@hq.dhs.gov
202-732-8000

What is the biggest challenge facing the industry today? One of our biggest challenges, a challenge not uncommon to the security industry, will be to implement security measures necessary to mitigate the risk presented by an increasingly complex and danger threat environment against a shrinking fiscal appetite applied to security. The evolving threat alone requires leaders across the security enterprise to be innovative in the approach and leverage all pillars of security to find the balance necessary to protect critical assets. The progress we have seen in the collaboration between intelligence and law enforcement communities should be extended to the security community to ensure all protection assets are striving to the same security objective across the Homeland.

Professional Bio

Mr. Swengros retired as an Army Military Police Colonel after almost 35 years of service and currently serves as the Deputy Director for Operations, Federal Protective Service (FPS). He is responsible for managing FPS protection operations in support of protecting federal employees and facilities and those who visit the facilities and seek services from the federal government. This effort includes application and integration of law enforcement capabilities, protective intelligence capabilities, and security capabilities of the work force, which includes over 1300 LE personnel and 13,500 armed contract security guards to achieve the protection mission.

GreyCastle Security

Active Shooter

Crisis Management

Critical Infrastructure Protection

Anti-terrorism

Reg Harnish, CISSP, CISA, CISM, ITIL
Chief Executive Officer
dmaloney@greycastlesecurity.com
518-274-7233

Marketing/PR Contact
Dean Maloney
Associate Marketing Analyst
dmaloney@greycastlesecurity.com
518-274-7233

What is the biggest challenge facing the industry today? The biggest challenge facing the industry today is still us, the people. Until we all have a degree of awareness, or at least comfortability, with cyber security, we will still have our credit cards confiscated and identities stolen.

What is the biggest challenge facing the industry today? The greatest opportunity for innovation is still us the people. The only way to solve a problem is with ideas. You cannot kill a problem with bullets. The only way you can solve ideas is with better ideas. Creating a culture around cyber security is the only way we will overcome this challenge.

Professional Bio

Reg Harnish is the CEO of GreyCastle Security, a leading cyber security risk assessment, advisory and mitigation firm headquartered in Troy, New York. As CEO of GreyCastle, Reg is responsible for defining and executing the company's vision. Under his leadership, the company has experienced six consecutive years of triple-digit growth and countless industry accolades. Today, GreyCastle Security is working with organizations in nearly every state in the U.S. Reg is a nationally-recognized speaker and has presented at countless industry events. He was recently recognized as the 2017 cyber security Consultant of the Year by the cyber security Excellence Awards and he has been featured in Time, Forbes, CBS Nightly News, The Washington Post, Dark Reading and others. Reg is a member of the Forbes Technology Council and a fellow of the National cyber security Institute in Washington, DC.

What do you think will have the biggest impact on the industry in the next 3-5 years? The greatest impact on the industry will be the complete erosion of privacy. Our information should be shared democratically like it was in simpler times when everyone knew everything about you. Your favorite color. Your favorite food. What made you laugh. Your kids' names. Where is the harm in that? Once information flows freely, governments will be forced to follow suit with transparency.

Hetherington Group

Cybersecurity/ Information Security

Soft Target Protection

Investigations

Cynthia Hetherington, CFE
President
ch@hetheringtongroup.com
973-706-7525

Marketing/PR Contact
Robert Baggett
Strategist
rb@robertbaggett.com
919-623-4996

What is the biggest challenge facing the industry today? Cyber-warfare, online reputation and asset management needs to be addressed in a nimble and decisive manner. Security experts need to adapt limber approaches to asymmetrical attacks.

What do you see as the greatest opportunity for innovation? Co-developing solutions in the cyber security market need to be approached with a collaborative and entrepreneurial spirit.

What do you think will have the biggest impact on the industry in the next 3-5 years? Cyber-warfare attacks will spur on the industry to accept existing solutions and help create new products

Professional Bio

Cynthia Hetherington has provided numerous corporate security officials, military intelligence units, and federal, state and local agencies with training on online intelligence practices. Recipient of the 2012 'Speaker of the Year Award' by the Association of Certified Fraud Examiners (www.ACFE.org). Her company, the Hetherington Group, is a national consulting, publishing and training firm specializing in intelligence, security and investigations.

Hitachi Systems Security

Cybersecurity/ Information Security

Enterprise Security Risk Management

Tim McCreight, CPP, CISSP, CISA
Director - Strategic Alliances
tim.mccreight@hitachi-systems-security.com
403-971-2500

Marketing/PR Contact
Robert Bond
Director of Marketing
robert.bond@hitachi-systems-security.com
450-430-8166

What is the biggest challenge facing the industry today? Our greatest challenge is remaining relevant in an ever changing landscape. I believe our investment in Enterprise Security Risk Management, or ESRM, is our best hope for the future of our profession.

Professional Bio

Tim acquired over 30 years in the security industry with leadership experience in both the physical and information security realms. He held executive positions at a number of organizations, notably as the Chief Information Security Officer (CISO) for the Government of Alberta and as Director, Enterprise Information Security for Suncor Energy Services Inc. Tim has presented as a keynote speaker at conferences across North America on such diverse topics as enterprise security risk management, converged security, and implementing enterprise information security programs. Tim was awarded his Master of Science in Security and Risk Management (with Merit) from the University of Leicester and attained his CISSP, CPP, and CISA security designations. Tim is a regular columnist for Canadian Security Magazine, and was interviewed in 2011 for his work as CISO with the Government of Alberta. Tim is also a member of the Board of Directors for ASIS International.

HTX Labs
Booth #2649

Enterprise Security Risk Management

Critical Infrastructure Protection

Security Technologist/ Futurist and Analytical Philosopher

Grant A. Fisher
Founder, President
Grant@HTXLabs.com
832-731-7965

Marketing/PR Contact
Megan Kenney
Strategist
Megan@HTXLabs.com
281-413-2449

Professional Bio

Grant Fisher is a serial entrepreneur and Philosopher with over 15 years experience in the Private Security Sector. He is currently the Founder and President of HTX Labs where he oversees the strategy and development of Intellectual Property related to Experience Transfer™, critical response conditioning and advanced cognitive resilience. His role within the Virtual Reality community is the most recent step in a long line of introducing frontier technology to industry. He previously founded Gnosys, an Augmented Reality smart process application, International Shield Inc, a disruptive Counter Intelligence consultancy and previously LED Basic/ Arbor Moonlight, who first introduced LED technology to general lighting and security applications. Additionally he has spent time with Tyco's Advanced Integration: PetroChem Team, as well as Roberts Law Group/ Chemical Security Group and holds a BA in Philosophy from the University of Houston.

What is the biggest challenge facing the industry today? Irrelevancy. While it is nearly impossible to forecast a future where the demand for security is diminished, the Private Security Industry has seen its domain continually reduced as technologies leveraged for life safety and security are more readily cared for by departments and individuals that understand the technology… more than its intended purpose. While technology still offers the greatest potential for a more efficient and effective security landscape, security professionals must be the ones to proactively drive the implementation of innovative technology solutions that go beyond security.

What do you see as the greatest opportunity for innovation? The Human Interface. The landscape of security technologies has burst - the myriad of solutions and products has created a culture that endorses product agnosticism, and that has come at the expense of specialization and true expertise. While the spirit of innovation should remain strong in the pursuit of better, faster and more secure solutions, the way Security Professionals are asked to use, operate, configure and rely upon these technologies has not changed. Frontier Technologies like IoT, Machine Learning, Augmented and Virtual Reality offer a tremendous promise of how the interface between the Human Element and the technology is poised to evolve.

What do you think will have the biggest impact on the industry in the next 3-5 years? An Evolving and Unfamiliar Threat Environment. Since 2001, threat has been assessed through a lens that allows for the extreme to weigh heavy in the allocation of resources and efforts to alleviate these associated risks. While legacy threats such as simple theft, corporate espionage or cyber incursions still amount to far greater actualized risks, the industry has been subjugated to the sensationalist tendencies of our time. Having personally lost my house in the historic flooding Houston endured during Hurricane Harvey, and bearing witness to the most powerful Atlantic Storm in Irma….the new reality will force Security Professionals to be responsive to an ever changing world. Business Continuity, Corporate Adaptability and Comprehensive Risk Mitigation will take center stage in the new Roles, Responsibilities and Expectations of Security Professionals.

IFPO en Español
Booth #4194

Investigations

Enterprise Security Risk Management

Training

Kevin Palacios PSP, PCI, CPP, CPOI
Director
kpalacios@ifpo.es
22923600

Marketing/PR Contact
Kevin Palacios
Director - Ecuador Security
kp_ecuador@yahoo.com
+593999702907

Professional Bio

IFPO Instructor, ASIS ARVP, responsible for the development of Spanish language material and IFPO network in South America, Spain and other Spanish speaking countries

What is the biggest challenge facing the industry today? To develop competent security professionals that would be one step ahead of all modern threats - most security professionals are unconscious of their incompetency until it's too late.

What do you see as the greatest opportunity for innovation? To put ASIS/ANSI/ISO standards to use in "real" life.

What do you think will have the biggest impact on the industry in the next 3-5 years? Enterprise Security Risk Management standards.

IronYun
Booth #4168

Security System Engineering/Design

Crime/Loss Prevention

Critical Infrastructure Protection

Enterprise Security Risk Management

Soft Target Protection

Investigations

Workplace Violence

Anti-terrorism

Paul Sun
President
paulsun@ironyun.com
203-273-8472

Marketing/PR Contact
(Same as above)

What is the biggest challenge facing the industry today? The security industry is receiving and processing a huge amount of data today (estimating 8.3 billion hours of data per week in North America alone), and this amount is only increasing with the increase in security threats worldwide, including terrorist attacks and social unrest. However, the tools to efficiently analyze such data in real time still require a lot of manual monitoring and intervention. Human resources are both limited and costly, which results in delayed detection in time-sensitive issues. The biggest challenge is thus the development of an automatized system to alleviate the manual bottlenecks.

Professional Bio
Paul Sun is a seasoned technology executive and serial entrepreneur with multiple successes in venture capital funded companies. Paul was the founder of three successful venture capital funded high technology start up companies. Mr. Sun was the President & CEO of Avidia Systems, Inc, a highly successful telecom startup. Mr. Sun was also the Chairman & CTO of DSL.net, Inc., a company he founded and built into a NASDAQ publicly listed company. Paul was also the President & CEO of Motia, Inc. In 2009, he was recruited by the Taiwan government's leading R&D center ITRI to help build the newly formed Cloud Computing Center. In 2015, Mr. Sun founded IronYun.

What do you see as the greatest opportunity for innovation? Deep learning. Deep learning technology, like what Google uses in their search engine, has pervaded and improved several aspects in our daily life: smart devices, automated vehicles, smart homes, etc. It is time to implement this technology in the security industry to maximize our efficiency.

What do you think will have the biggest impact on the industry in the next 3-5 years? The Internet of Things (IoT) in combination with deep learning and cloud computing. Globalization in every industry is accelerating with the IoT because of its convenience, easy access, low cost, and security. With this technology, every system in the security industry will have to be upgraded or changed as old systems are eliminated. Automatization and globalization will also cause a shift in job opportunities and structures of the workplace: for example, no longer will a security officer be required to physically be in the building to monitor the office entrance - he can monitor from home across the city, or choose to only receive real-time alert message on his smart phone when problems occur on site. The technicians must be trained in IoT and related technologies, and the number of traditional security employees can be decreased in favor of computer scientists. In short, a shift towards automatization and remote access in real time will occur.

Johnson Controls
Booth # 4119

Crisis Management

Critical Infrastructure Protection

Cybersecurity/ Information Security

Jason Ouellette
Product General Manager, Global, Access Control
jouellette@Tycoint.com
1-978-577-4175

Marketing/PR Contact
Andrea Gural
Principal, Eclipse Media Group for Johnson Controls
agural@eclipsemediagroup.net
207-233-7507

What is the biggest challenge facing the industry today? The legacy solutions in the field which have enjoyed 15 to 20 lifespan and the now growing demand for cyber secure solutions which include this older infrastructure that can have vulnerabilities or limitations in being able to adopt the newer requirements as physical security and IT standards continue to further converge.

What do you see as the greatest opportunity for innovation? Concerns about safeguarding personal information are top-of-mind and that isn't likely to change anytime soon. Securing personal data within access control systems means integrating with companies whose job it is to secure information

Professional Bio
Product General Manager for Tyco Security Products' Software House, Kantech and CEM Systems, Elpas and Innometriks brands, is responsible for the product management, engineering and program management of access control solutions including software, firmware and hardware products. In this role, Jason handles the management for the access control product lifecycle management end to end — from concept inception to product retirement. Jason is based in Westford, Mass., joined JCI in 1999, and has previously served as a customer support specialist, software engineer, engineering manager and the director of R&D, in the American Dynamics Intellex products and Software House Access Control products as well as Director of Product Management for the Access Control business. Jason also served in the U.S. Air Force from 1989 to 1996 as a medical laboratory specialist and later as a computer implementation specialist and held positions at CDSI, and SAIC before coming to JCI.

as well as exploring emerging technological options that ultimately remove the need for companies to store someone's personal data and keep the data with the individual. The industry can expect to see double-digit growth in mobile credential use this year and it presents opportunities going forward,especially as standards are put into place. We are a smartphone and device-based society, thus there is room for innovation and expansion as we look to integrate mobile credential options into our access control offerings.

What do you think will have the biggest impact on the industry in the next 3-5 years? The growing emphasis on leveraging big data and the growth of IoT has security customers asking about ways to move their current data from on-site solutions to cloud-based ones. Although we are currently seeing the emphasis placed more on edge device solutions than cloud-based ones, I believe in three to five years the cloud will become the focus. We are already seeing providers such as Workday and Salesforce with successful cloud-based platforms and that is building trust in the concept down the road for mission critical products such as access control.

Kiernan Group Holdings, Inc.

Active Shooter

Soft Target Protection

Workplace Violence

Dr. Kathleen Kiernan
CEO and Founder
kiernan@kiernan.co
571-290-0260

Marketing/PR Contact
Susan Forman
DGI Comm
sforman@dgicomm.com
212-825-3210

Professional Bio

Kathleen L. Kiernan, Ed.D., is the CEO and Founder of Kiernan Group Holdings, Inc. (KGH), a global consulting firm that innovated the Preparedness Without Paranoia™ concept. KGH brings together experts in intelligence, law enforcement and security to serve government and private sector clients. Dr. Kiernan is a 29-year veteran of Federal Law Enforcement with a long track record in the law enforcement and national security communities, including the Assistant Director for the Office of Strategic Information and Intelligence at the U.S. Bureau of Alcohol, Tobacco and Firearms. Complementing that real-world experience is a doctorate in Education from Northern Illinois University in DeKalb, Ill., as well as master's degrees from the Joint Military Intelligence College in Washington, D.C., and from George Mason University in Northern Virginia.

What is the biggest challenge facing the industry today? The biggest challenge facing security professionals today is the need to simultaneously protect both hard and soft targets in an open society. The convergence of different threat vectors and actors—enabled by access to technology, fueled by hatred and ideology—adds complexity to the planning, response and recovery cycles should attacks occur. The new threat vectors range from attacks on our national security and terrorism, to criminal organizations using tools of violence, to the lone wolf with no association to any organization but with a specific agenda. This convergence has facilitated a more hybrid kind of threat whose attacks take everyday commercial products—like vehicles, for example—and misappropriate their intended use into weapons of violence. These hybrid attacks, now, almost seem ordinary. Unmanned Aircraft Systems (UAS) present a particularly unique and unusual challenge. UAS technology, which was originally purposed for commercial and industrial work, can be improvised by those with bad intentions to attack both soft and hard targets. We previously only protected assets in two dimensions: through physical barriers such as fences and gates, barbed wire and badges for access. Now we must think of security in three dimensions. For instance, the UAS is generally a flying computer that can crack the third dimension, flying over a facility, stealing intellectual property, while compromising that organization's ability to safely and securely conduct business. Adopting that hard target mentality and mitigation protocols is key for the future of our nation's security. Being prepared does not have to be an intimidating or overwhelming task for organizations or their workforce. One can be prepared without being paranoid. This preparedness transcends where we work, where we live, where we play and where we worship. Security sense is really common sense.

What do you see as the greatest opportunity for innovation? The greatest opportunity for innovation is a completely prepared human being. The Return on Investment (ROI) is invaluable. There is always a presumption in the private sector that most threat issues will be taken care of by first responders. In fact, our citizenry is uniquely positioned to recognize anomalies in everyday patterns of behaviors and operating procedures. Early awareness of threat indicators is the key for organizations and security professionals to react efficiently to these active threats. The prepared human being remains the first line of defense and, when trained properly, will have the discretion to use technical capabilities to mitigate universal threats. The responsibility of security should be an organic work skill. Because a threat to one is a threat to all, a seamless relationship between public and private sector preparedness needs to evolve. Both entities must understand the nature of evolving threats and have the tools, training and information to respond appropriately and with confidence and capability to any active threat. And much the way most organizations prepare for a fire drill without experiencing a fire, the mindset to drill for a potential threat before an event occurs is essential to evaluating the response and recovery of any organization.

What do you think will have the biggest impact on the industry in the next 3-5 years? The biggest impact on the industry in the next three to five years will be hybrid threats. The new active threat may no longer carry a gun, but will be misappropriating commercial products into non-traditional weapons of violence, while blending in cyber capabilities with new and varying delivery systems. Much like the 9/11 attackers who used planes as weapons, the new threat will be directed at both hard and soft targets using vehicles, UAS and other commercial products as weapons. Our goal should be to minimize this potential impact on the industry by educating and training organizations and their workforces as well as general citizenry (from the kitchen table to the boardroom table) on threat and risk assessment methods; providing organizations with skills in emergency preparedness planning; and facilitating the adoption of common-sense security practices, such as increasing situational awareness and developing effective mitigation protocols.

KPMG, LLP

Enterprise Security Risk Management

Cybersecurity/ Information Security

Critical Infrastructure Protection

Deborah Watson, CISSP, GCIH, GMOB, GICSP
Director
dlwatson@kpmg.com
832-509-9126

Marketing/PR Contact
Ann Marie Gorden
Manager, KPMG Corporate Communications
agorden@kpmg.com
201-505-6288

What is the biggest challenge facing the industry today? The constant balancing act of innovation and information security remains to be the industry's greatest challenge today. We have always been challenged to enable employees to be innovative; now we have to balance that with meeting compliance requirements and mitigating evolving email security and malware risks. And with innovation at the core of many companies today, budgets and resources are less focused on security. Smart companies are striking a balance by seizing the opportunity to build cyber security into their products and innovate around security.

Professional Bio

Deborah Watson is an information technology specialist, focused on Corporate Information Security Strategy, Compliance, Infrastructure Security and Data Protection at KPMG. She has more than 18 years of experience in the information technology and security fields. While Ms. Watson's most recent expertise includes security strategy, security privacy, risk management, messaging security and compliance, she also has extensive experience in infrastructure security design, encryption, key management, endpoint hardening, antivirus architectures, system architecture and design, business continuity, patch and vulnerability management, and project management capabilities. Ms. Watson holds a Master's degree in Information Technology Management from Harvard University.

Land O'Lakes, Inc.

Investigations, Workplace Violence

Critical Infrastructure Protection

Crisis Management

Don Taussig, CPP
Director of Global Security Services
ditaussig@landolakes.com
651-236-0204

Professional Bio

Don Taussig, CPP, is the Director of Global Security Services at Land O'Lakes, Inc., where he is accountable for enterprise-wide security, crisis management and corporate travel programs. In the past Don served in several roles, in both public and private sectors, of ever increasing responsibility. His experience includes more than 30 years of executive leadership and consulting in the areas of corporate security, law enforcement, investigations and international operations. He retired from the U.S. Army's Military Police Corps in 1996 and from the U.S. Civil Service in 2011. One highlight of Don's career was his appointment as a Director of Security in the Executive Office of the President. Don's other notable roles included serving as a Special Agent in Charge for Executive Protection for the NATO Commander, as a Chief Security Officer for U.S. Bureau of Reclamation (USBR) within the U.S. Department of the Interior, as Security Officer with U.S. Department of State and as a member of the National Disaster Response Team while with Department of Homeland Security.

Micro Focus

Active Shooter

Cybersecurity/ Information Security

Enterprise Security Risk Management

Ron LaPedis, CISSP, ISSAP, ISSMP
Global Enablement Specialist
ron.lapedis@microfocus.com
650-797-4063

Marketing/PR Contact
Randy McDonald
NA Field Marketing
Randy.McDonald@microfocus.com
1-650-797-4063

What is the biggest challenge facing the industry today? Insiders and outsiders-becoming-insiders are the greatest threats to cyber security. Through targeted attacks, criminals are seeking to trick privileged insiders to either install malware or give up their credentials.

Professional Bio

Ron LaPedis, a global enablement specialist at Micro Focus, has more than 25 years of information security & IT disaster recovery experience. He has lead or participated in the design of dozens of business continuity plans and secure networks for financial and healthcare institutions around the world. In addition to his business skills, he has extensive training and experience in emergency response using the Incident Command System (ICS) and is a first responder with the San Mateo County Sheriff's volunteer communications unit.

What do you see as the greatest opportunity for innovation? Machine learning or artificial intelligence are the big buzzwords. Whatever you call it, the ability for a machine to distill thousands of points of information and act on the threats contained within is important to close the doors that cyber criminals are using to gain entrance into the organization.

What do you think will have the biggest impact on the industry in the next 3-5 years? The linkage of cyber security, physical security, and business continuity programs.

Microsoft

Security System Engineering/Design

Jim Black, CPP, PSP, CSC
Security Design Team Manager
kpalacios@ifpo.es
714-906-9067

What is the biggest challenge facing the industry today? Security Theatre! That is, reactive security giving a general appearance of protection, with insufficient concern for appropriateness or effectiveness.

What do you see as the greatest opportunity for innovation? Artificial Intelligence has the potential to bridge the limits of human attention and perception to identify physical security risks earlier and more consistently than ever before.

What do you think will have the biggest impact on the industry in the next 3-5 years? Artificial Intelligence and the cloud will change the way security professionals work in a variety of ways. The industry is just now scratching the surface of leveraging the fantastic possibilities.

Professional Bio

Jim Black is the Security Design Team Manager for Microsoft where he is responsible for the physical security design program for the company's critical infrastructure facilities around the world. Mr. Black is credentialed as a Certified Protection Professional and Physical Security Professional through ASIS International, and a Certified Security Consultant through the International Association of Professional Security Consultants. Over the past two decades, Jim has been privileged to be trusted by a diverse group of the nation's leading companies in assessing risks, planning protective measures, and engineering physical security solutions for facilities within 13 of the nation's 16 Critical Infrastructure Sectors as defined by DHS. He is a member of the ASIS Security Architecture and Engineering Council.

Microsoft Global Security

Security System Engineering/Design

Workplace Violence

Investigations

Brian K. Tuskan
Sr. Director of Security
btuskan@microsoft.com
425-705-5107

What is the biggest challenge facing the industry today? Finding the right solution and provider to deliver.

What do you see as the greatest opportunity for innovation? The cloud.

What do you think will have the biggest impact on the industry in the next 3-5 years? Artificial Intelligence and Machine Learning.

Professional Bio

Brian Tuskan has more than 16 years of corporate security experience as the Senior Director of Security at the Microsoft Corporation. He has led Microsoft Global Security teams in physical security operations, investigations, background screening, security communications, retail security, event security, intelligence and business development. Tuskan is currently spearheading the technology development of Microsoft's Global Security's Virtual Security Operations Center (VSOC), which will be the security operations center of the future, leveraging intelligent cloud, intelligent edge, AI, robotics and 3D mixed-reality to manage global life-safety security operations for the business. Through the combination of advanced technology, security response will become smarter, more coordinated and proactive, Tuskan says. Prior to joining Microsoft, Tuskan spent more than 12 years in law enforcement with the City of Redmond Police in Washington and the Honolulu Police Department. During his distinguished law enforcement career, he worked as a patrol officer, ATV specialized unit, SWAT tactical team member, criminal intelligence and analysis, undercover narcotics detective, major crimes detective and officer-incharge. Outside of Microsoft, Tuskan founded Cop to Corporate, a blog that helps law enforcement professionals plan their transition to the private sector. He has also provided mentorship and coaching for military veterans looking to transition to the private section, and he has presented on this topic at the FBI National Academy Associates and Homeland Security Investigations. Additionally, Tuskan sits on the Microsoft Worldwide Public Safety and Justice Advisory Council, is an Advisory Board Member of Secure Strategy Group, and served on the ASIS Leadership & Management Practices Council. He has a Criminal Justice degree from Wayland Baptist University, is a graduate of the University of Washington Foster School of Business Executive Development Program, and received an Executive Leadership Certificate from Georgetown University.

MSA Security

Anti-terrorism

Investigations

High consequence security

Bill Flynn
Strategic Advisor
910-233-0045

Marketing/PR Contact
Brendan Terry
brendan.terry@icrinc.com
203-6828-212

Professional Bio

William F. Flynn is a Strategic Advisor with MSA Security, President of GARDA Risk Management LLC and a Senior Fellow at GWU Center for Cyber & Homeland Security. He previously served as Deputy Assistant Secretary at the Department of Homeland Security

What is the biggest challenge facing the industry today? The insider threat has become the Achilles heel for critical infrastructure protection. While data breeches and theft of information have received much of the attention, the impacts also include fraud, sabotage, espionage and workplace violence. Furthermore, there has been a shift in the domestic threat landscape from centrally planned and coordinated attacks, to lone wolves and isolated groups who are inspired by groups such as ISIL to take action within their communities.

What do you see as the greatest opportunity for innovation? The private sector should partner with government and focus their corporate social responsibilities on disenfranchised, at-risk communities that are being targeted by terrorist recruiters.

What do you think will have the biggest impact on the industry in the next 3-5 years? In the next 3-5 years we will witness a terrorist diaspora whereby thousands of individuals who travelled to Syria and Iraq will be returning to the West with the skills and tradecraft they acquired fighting alongside ISIS.

NC4 Inc.

Booth # 501

Critical Infrastructure Protection

Enterprise Security Risk Management

Traveler Tracking and Corporate Duty of Care

Eric Hankins
Sr. Director, Travel Risk Solutions
eric.hankins@nc4.com
240-604-1115

Marketing/PR Contact
Kathy Condellire
Marketing Manager
kathy.condellire@nc4.com
314-686-4111

Professional Bio

Eric Hankins, NC4's Senior Director for Travel Risk Solutions, has nearly twenty years' experience in the design and development of tools to apply global risk analysis and real-time intelligence to corporate security and duty of care missions, from the enterprise policy level down to the experience of the individual traveler. He currently drives NC4's efforts to conceive and develop solutions to meet the needs of its customers in the corporate security, risk management, business continuity, supply chain management, and corporate travel markets. Throughout his career, Hankins has worked closely with thought leaders in international corporate security and business travel management, gaining a deep understanding of industry's need for timely, targeted intelligence and the technologies to collect and deliver it. Prior to his current position, Hankins was COO and the principal architect of traveler tracking solutions at TranSecur, Inc., the oldest continually operating global security intelligence provider in the United States.

What is the biggest challenge facing the industry today? Making sense of the vast and ever-growing quantities of granular open source information on social media networks presents an often overwhelming challenge to resource-constrained risk management operations, making it very difficult to get reliable and relevant information about emerging threats in time to assess and mitigate risk proactively.

What do you see as the greatest opportunity for innovation? There is a tremendous opportunity for innovation in developing automated systems that can tirelessly and iteratively scan these enormous troves of information, sifting through mountains of raw data and synthesizing it into relevant and actionable intelligence. Using current techniques and technology, the work is time consuming, expensive, and prone to error – but the payoff can be immeasurable when everything falls into place. Developing automation, especially systems that can be trained and learn from experience, will speed up the process, lower costs, and increase success rates.

What do you think will have the biggest impact on the industry in the next 3-5 years? The continuing improvement and decreasing cost of computer hardware and the advances in the science of machine learning will allow us to approach, incrementally, a fuller realization of the raw power of globally crowd-sourced situational awareness.

Newcastle Consulting, LLC

Active Shooter

Security System Engineering/Design

Crisis Management

Critical Infrastructure Protection

Cybersecurity/ Information Security

Enterprise Security Risk Management

Soft Target Protection

Workplace Violence

Investigations

J. Kelly Stewart, MBA, 2 MAs, CHS-IV, CMAS, CFC
Managing Director & CEO
jkstewart@nccllc.net
202-374-8236

Marketing/PR Contact
J. Kelly Stewart
202-374-8236
development@nccllc.net

What is the biggest challenge facing the industry today? Biggest challenge facing the security industry today is the elevated concerns and unwarranted acts of terrorism propagated by increases in cyber security threats and wanton acts of violence.

What do you see as the greatest opportunity for innovation? Collaboration will push the need for technology to fuel increases and efficiencies in the data surge. Equally significant is the push for efficiency gains through technology. These innovations will create value and revenue thus increasing quality of life and potentially leveling the playing field rather than having the opposite affect of creating too vast a gap between the haves and the have-nots.

What do you think will have the biggest impact on the industry in the next 3-5 years? Artificial Intelligence and Pocket Supercomputers.

Professional Bio

Managing Director, CEO and Founder of Newcastle Consulting, LLC leading an Enterprise Security Risk and Information Management Consultancy that has cultivated more than 25 years of providing proactive, predictive, and responsive advice and access to information critical in building a companies' resilience to operational risk. Our aim is achieving excellence by exceeding expectations through careful analysis in approaches to risk management, security design, and resiliency. Concentration is spent on training individuals on an integrated approach to security governance, risk, and compliance as well as offering an in-depth examination of all aspects of planning and implementation of a risk assessment program. We focus on a systematic, prevention-based methodology that was applied, learned and honed through a distinguished tenure with the United States Secret Service, the National Nuclear Security Administration and various Fortune 500 and 1000 companies.

Orbital ATK

Security System Engineering/Design

Enterprise Security Risk Management

Workplace Violence

Gregory Jarpey, PSP
Security Operations Manager
gregory.jarpey@orbitalatk.com
763-744-5239

What is the biggest challenge facing the industry today? The insider threat is the greatest challenge to any organization. Employees stealing or leaving the company with proprietary information can irreparably harm any company.

What do you see as the greatest opportunity for innovation? Getting the physical security operations center to work with the information systems operations center by making them become one.

What do you think will have the biggest impact on the industry in the next 3-5 years? Cyber security and physical security learning to properly work together for the betterment and increase of company security postures around the world.

Professional Bio

Gregory Jarpey works for Orbital ATK as the Security Operations Manager for Corporate Security. He has more than 20 years of security experience working in the retail, utility, aerospace and defense sectors of industry. Greg has his Bachelor's degree in Business Management and received his PSP (Physical Security Professional) certification from ASIS in 2004. Greg is a member of the ASIS Physical Security Council and contributor to the ASIS Protection of Assets manuals released in 2012. He hosted a local ASIS chapter meeting in 2010 by conducting a round table about SOC's. Greg published his first book "The Security Operations Center Guidebook: A Practical Guide for a Successful SOC" in June 2017.

R.L. Oatman & Associates, Inc.

Executive Protection

Robert L. Oatman, CPP
President
rloatman@rloatman.com
410-494-1126

What is the biggest challenge facing the industry today? The future of many professionals in our industry will be defined by technology. Tools such as specialized aps for smartphones, access control, video surveillance, tracking devices and drones. This same technology will also help those who wish harm against our efforts.

What do you see as the greatest opportunity for innovation? Real-time Intelligence. Security depends on informed planning, which requires intelligence and other information. The ability to plan wisely, avoid detected threats and react effectively to sudden changes in conditions is a game changer. Being able to optimize these decisions should be based on comprehensive and up to date intelligence. At home - workplace - travel having the information advantage, creates a greater situational awareness.

What do you think will have the biggest impact on the industry in the next 3-5 years? To be ready for the future, security professionals will have to stay informed about developing and foreseeable technologies, both favorable and unfavorable to our efforts. We need to be prepared for those technologies that have not been invented or deployed.

Professional Bio

Mr. Oatman CPP has been providing Executive Protection, risk assessments and training around the world since 1989. He retired as a Major - Chief of Detectives - Baltimore County P.D. MD in 1989. Mr. Oatman holds a B.S. degree from the University of Baltimore and is a graduate of the F.B.I. National Academy. He has authored 4 books on E.P. He developed the first 2 day ASIS EP program in 1998, and serves as Chairman of the ASIS E.P. council - Chairman Ijet Intelligence Security Advisory Board.

R3 Continuum

Crisis Management

Workplace Violence

Active Shooter

Anti-terrorism

Bruce T. Blythe
Chairman/Crisis Management Consultant
bruce.blythe@r3continuum.com
404-841-3402

Marketing/PR Contact
Jamie Gassmann
jamie.gassmann@r3continuum.com
952-641-0636

What is the biggest challenge facing the industry today? The world is not becoming a safer place. The rate of change, including security concerns, presents a vital need for security professionals. Beyond the focus on preventing critical incidents, there is a responsibility for organizations to prepare for crisis incidents and be ready 24/7 to effectively respond when unexpected events threaten the core assets of an organization.

What do you see as the greatest opportunity for innovation? Getting the physical security operations center to work with the information systems operations center by making them become one.

What do you think will have the biggest impact on the industry in the next 3-5 years? Cyber security and physical security learning to properly work together for the betterment and increase of company security postures around the world.

Professional Bio

Bruce T. Blythe is an internationally acclaimed crisis management specialist who provides crisis preparedness, crisis response, and strategic crisis leadership services worldwide. His organization (R3 Continuum) responds to crises 1500 times on average per month. He's a clinical psychologist and author of Blindsided: A Manager's Guide to Crisis Leadership (2014). Mr. Blythe is a former U.S. Marine Corps Military Police Officer and consultant to the FBI on workplace violence and terrorism. He speaks annually at 50 conferences worldwide with specialties in crisis preparedness, workplace violence, human side of crisis, and strategic crisis leadership.

Dr. George Vergolias
Medical Directort
George.vergolias@r3continuum.com
919-523-8817

What is the biggest challenge facing the industry today? Technological advances have allowed us to gain access to enormous amounts of data, quickly, and often in real time. The challenge is figuring out how to filter that data to the right person with the right expertise who can analyze it and make sound threat mitigation decisions.

Professional Bio

Dr. George Vergolias is a forensic psychologist and threat management expert, with 20 years of clinical experience. He currently serves as Medical Director of R3 Continuum, leading their Threat of Violence and Workplace Violence programs. Dr. Vergolias has directly assessed or managed over 500 cases related to elevated risk for violence, self-harm, sexual assault, stalking, and communicated threats.

What do you see as the greatest opportunity for innovation? We know more now about behavioral threat indicators than ever in our past, and every few years continue to accelerate that knowledge base. The marriage of that knowledge with technological advancements in data mining and analysis has great potential for innovation.

What do you think will have the biggest impact on the industry in the next 3-5 years? A challenge and also opportunity in the next 3-5 years will be the ability for disparate areas of the security industry (physical site security, cyber/IT, behavioral assessment, etc.) to collaborate in ways to provide a full array of security and threat mitigation solutions.

Radian Compliance, LLC

Cybersecurity/ Information Security

Legal and Regulatory Compliance

Lisa DuBrock, CPA
Managing Partner
ldubrock@radiancompliance.com
847-997-2032

What is the biggest challenge facing the industry today? Customer Satisfaction. Customer needs, technology, regulations and standards are changing so fast that keeping the customer informed and satisfied is becoming more difficult.

Professional Bio

Lisa is a Managing Partner for Radian Compliance, LLC where she specializes in design and implementation for her clients of Management System Standards surrounding: Security – Information, Physical and Private as well as Business Continuity frameworks. She also provides her clients with internal audit in the areas of ISO 9001 Quality Management and ISO 20000 Service Management Systems. Lisa sits on the ASIS – Standards and Guidelines Commission developing American National Standards. She has been instrumental in developing standards supporting Private Security Companies, Business Continuity and Organizational Resilience. She additionally sat on the ANAB Committee of Experts to draft the Accreditation rule supporting ANSI/ASIS PSC.1 – Private Security Companies Management System Standard. She is an active member of the ISO/US-TAG committee developing ISO standards supporting Business Continuity, Private Security Companies, Societal Security, and Fraud and Countermeasures.

Retail Loss Prevention Council

Booth # Council Booth

Crime/Loss Prevention

Soft Target Protection

Workplace Violence

Alan Greggo, CPP
Chairperson- Retail Loss Prevention Council
agregg@microsoft.com
513-236-2642

What is the biggest challenge facing the industry today? The biggest challenge facing the retail loss prevention industry is the threat to life when violence breaks out, such as a shooter in a retail venue. Every business should be planning and practicing to address this threat.

Professional Bio

Alan Greggo currently serves the retail business at Microsoft in Global Security Asset Protection. He is a Certified Protection Professional and Certified Fraud Examiner. He has 37 years of Retail Loss Prevention leadership experience. Greggo Co-Authored the book "Retail Security and Loss Prevention Solutions" with Millie Kresevich, CRC Press, 2010.

What do you see as the greatest opportunity for innovation? I see our greatest opportunity for innovation as our ability to diversify ASIS Membership both culturally and generationally. We can learn so much from the international community, and younger generations bringing their social media and IT knowledge to ASIS.

What do you think will have the biggest impact on the industry in the next 3-5 years? I think the biggest impact on our industry would be to add a requirement to every certification ASIS offers specifying that a candidate have a basic knowledge of IT terminology and best practices for creating strong partnerships with their corporate IT leaders.

Robotic Assistance Devices

Booth # 1155

Critical Infrastructure Protection

Enterprise Security Risk Management

Investigations

Steve Reinharz
Founder and President
steve.reinharz@roboticassistancedevices.com
949-636-7060

Marketing/PR Contact
Jessica Stout
Account Manager
jessica@compassintegrated.com
952-641-0636

What do you see as the greatest opportunity for innovation? Artificial intelligence and robots are increasingly valuable to end users and guarding providers for various use cases, including security and operations, and are poised to be the greatest opportunity for innovation. Robots have a significant place in the utility market, where thermal imaging can be deployed to detect failing power lines, thereby automating otherwise dangerous jobs. Operational efficiencies can be significantly realized as more and more of these robots are introduced in the workplace to augment human abilities, reduce liability and provide remote monitoring. With so many opportunities on the horizon in the robotics realms - such as human detection analysis using machine vision - the possibilities in this space are really endless. Robotics is the next frontier in securing the public, private and enterprise sectors.

Professional Bio

Steve Reinharz is the Founder and CEO of Robotic Assistance Devices (RAD), where he oversees the development, sales and marketing, and strategic vision for the company. Reinharz has more than 20 years of experience in various facets of the high-tech industry - as the founder of security integration firm Security Zone, Inc., and a strategic leader at global enterprises. Reinharz has extensive knowledge of a diverse portfolio of technologies, developing practical, effective solutions for end-user customers. As CEO of RAD, Reinharz leverages his extensive knowledge and interest in robotics and artificial intelligence to design and develop robotic solutions that increase business efficiency and deliver cost savings. Reinharz is a native of Toronto, Ontario, Canada, and attended the University of Western Ontario, where he earned dual bachelor of science degrees in political science and commercial studies. Follow him on Twitter: @SteveReinharz.

Rozin Security Consulting LLC

Anti-terrorism

Soft Target Protection

Behavior Threat Detection

Michael Rozin
President
michael@rozinsecurity.com
952-240-9395

Marketing/PR Contact
Kathryn Rozin
CEO
612-578-5058
kathryn@rozinsecurity.com

What is the biggest challenge facing the industry today? The biggest challenge facing the security industry today is the advancement of technology which creates highly sophisticated threat actors and at times less sophisticated security operators.

What do you see as the greatest opportunity for innovation? One of the greatest opportunity for innovation is development of security methods to systematically and effectively address the human factor through recognition of malicious intent before harmful acts are carried out.

What do you think will have the biggest impact on the industry in the next 3-5 years? The changing threat landscape will have the biggest impact on the industry in the next 3-5 years, it will force security industry to adopt new and more effective methods.

Professional Bio

Mr. Rozin is the President of Rozin Security Consulting LLC an international security risk management, training and proactive security services firm. Michael is recognized as the creator of the Suspicion Indicators Recognition & Assessment (SIRA®) System—an advanced threat detection and prevention program. Mr. Rozin worked as a security manager focused on counter-terrorism at Mall of America. Michael developed and managed a behavior threat detection unit and variety of additional innovative proactive security programs. Michael's work at MOA is recognized at Department of Homeland Security as a leading approach to securing open to public facilities. Mr. Rozin served in a special operations unit in the Israel Defense Forces. After military service, he joined the Israel Airport Authority as a security agent for Ben-Gurion International Airport. Michael is a graduate of the Institute for Counter-Terrorism in Hertzliya, Israel and completed the Advanced Security and Anti-Terrorism Training at Israeli Security Academy.

SafePlans

Active Shooter

Crisis Management

Soft Target Protection

Anti-terrorism

Workplace Violence

Bomb threat management

Brad Spicer
CEO
brad@safeplans.com
573-636-5377

Marketing/PR Contact
Director of Business Development
ron@safeplans.com
866-210-7233, ext. 207

Professional Bio

Brad Spicer is an Army veteran with 20 years law enforcement experience; including in SWAT and dignitary protection. He developed ERIP, an all-hazards preparedness software that is designated by Homeland Security as a qualified anti-terrorism technology and, Intruderology, a leading active shooter defense training system. SafePlans has provided preparedness solutions for thousands of organizations including states, financial institutions, major school systems and fortune 500 companies.

What is the biggest challenge facing the industry today? Threats, such as vehicle based attacks on large crowds, continue to evolve at a pace that typically exceeds security funding. While security is a truly specialized skill, organizations must look to decentralize security operations and integrate all employees into the security framework and culture.

What do you see as the greatest opportunity for innovation? The need to crowd source and expand security operations to include all employees and even the public is a tremendous opportunity. For instance, with our site mapping technology a teacher or employee can photograph key information about their classroom or place of work and this information can be securely shared with local public safety. Understanding how their door locks and the direction it opens can help the employee respond more effectively, and having access to this data improves public safety response time.

What do you think will have the biggest impact on the industry in the next 3-5 years? Programs like See Something-Say Something, Run-Hide-Fight and Stop the Bleed will continue to improve the publics ability to assist law enforcement and security professionals in making our places of work, worship and education even safer.

Savage Security

Security System Engineering/Design

Critical Infrastructure Protection

Cybersecurity/ Information Security

Enterprise Security Risk Management

Investigations

Kyle Bubp, GCIH, GCUX, RHCSA, MCITP:EA, MCITP:SA
Principal Consultant
kyle@savagesec.com
865-399-1520

Professional Bio

For over a decade, Kyle Bubp has been elevating the state of security for enterprises, service providers, government organizations and the industry at large. Throughout his career, Kyle has worked on several privileged and classified U.S. government projects for multiple 3-letter agencies. He has developed secure architectures for fingerprint processing, protected research for the scientific and academic communities, and locked down environments for defense logistics. He's put his skills to the test at a massive scale for an international hosting company, led the security practice at a Atlanta-based VAR, and has since co-founded Savage Security, a cyber security research and consulting firm. Kyle has been published in ISSA Journal, provides news media with insights into security, and speaks at security conferences around the United States as he continues his goal of educating others about security.

What is the biggest challenge facing the industry today? Ignorance. Many organizations don't have a good handle on what threats exist, how to mitigate them, and how to discern what is a real, durable solution versus marketing hype from a vendor.

What do you see as the greatest opportunity for innovation? We continue to hear about "the basics" every time someone gets breached. If someone could build a tool that would automatically apply "the basics" to systems, and implement compensating controls where necessary, I think that would go a long way. Unfortunately, I don't think this is something that can be completely automated. It's going to take a shift in the security industry to transfer ownership of security back to the system/data owners, with current security staff becoming advisors and architects. So, the greatest opportunity here is a shift in the entire security dynamic. We need to first understand the business before we can start recommending any risk mitigation. From that point, it's important to implement solutions that are provably effective. If you can't measure the efficacy of the control you've put in place... it's probably not doing much.

What do you think will have the biggest impact on the industry in the next 3-5 years? Criminals have figured out that they can make massive amount of money for minimal effort. For example, the authors of WannaCry just recently emptied a Bitcoin wallet worth $143,000 USD. Now that it's pretty obvious there are a massive amount of machines out there that can be exploited via old vulnerabilities and simple misconfigurations (Mirai botnet for example), I think many more attackers will be writing malware for a multitude of devices (think IoT, SCADA, medical devices, not just Windows workstations anymore). IoT is growing at a scale that's going to be difficult to retroactively secure, and we need to implore manufacturers to start building security into these devices.

Securitech Group, Inc.
Booth # 1155

Active Shooter

Crime/Loss Prevention

Critical Infrastructure Protection

Mark Berger
President
mberger@securitech.com
917-304-6118

Marketing/PR Contact
Maranda Thompson
mthompson@securitech.com
718-392-9000

What is the biggest challenge facing the industry today? Providing security while creating an environment that does not foster fear.

What do you see as the greatest opportunity for innovation? Creating invisible, but effective physical security solutions.

What do you think will have the biggest impact on the industry in the next 3-5 years? Upcoming economic downturn.

Professional Bio

Mark Berger is the President and Chief Product Officer of Securitech Group, Inc., an innovative lock manufacturer in NY. Securitech employs over 50 people, and is proud of its roots and identity as the go-to manufacturer for code-compliant locking solutions, especially within NYC. HPD, NYC Transit and the NYS Office of Mental Health are just a few of the city and state agencies which specify Securitech solutions, many of which were tailored to their specific needs. He holds several patents and is passionately involved in designing locking products which meet today's emerging needs while respecting life safety codes. In recent years he has designed the custom lockset for the new Sandy Hook school as well as the apartment building entrance and exit locks for the New York City Housing Authority's Layered Access Control program.

Setracon Enterprise Security Risk Managment Solutions

Enterprise Security Risk Management

Critical Infrastructure Protection

Crisis Management

Active Shooter

Jeffrey A. Slotnick, CPP, PSP
President
jeff.slotnick@setracon.com
253-255-1260

What is the biggest challenge facing the industry today? Internet of Things, Cyber Security, ESRM as a Strategy, and eliminating silos within Enterprises.

What do you see as the greatest opportunity for innovation? Data Analytics and Causal Analytics to Enterprise Security as a valuable contributor.

What do you think will have the biggest impact on the industry in the next 3-5 years? ESRM as a guiding strategy and the alignment of the CSO with the CISO/CIO.

Professional Bio

Mr. Jeffrey A. Slotnick, CPP, PSP is an internationally known Enterprise Security Risk Consultant with more than 28 years of experience, peer recognized as a "Thought Leader" and a "Critical Architect in homeland security." As an ISO credentialed Lead Auditor Jeff is responsible for the some of the latest advancements in All Hazards Disaster Resilience, Organizational Resilience Management, ISO/ANSI Standards Development, Resiliency Information Management Processes, and Enterprise Security Risk Management. Jeff is focused on the professional development and training of security, law enforcement, and military personnel, the provision of exceptional security services, protective services, and all facets of Enterprise Security Risk Management including risk, vulnerability, and threat assessments, Emergency Response Planning, Business Continuity Planning, and Physical Security System Master Planning, Design and Integration. Mr. Slotnick has extensive experience in the Public Works and Utilities field with specific expertise in Water, Waste Water, Dams, Transportation Infrastructure, Light and Heavy Rail, Supply Chain, Religious Institutions, Schools, Data Centers, and Medical Facilities. Jeff is a Senior Regional Vice President for ASIS International, Faculty Advisor for the University of Phoenix Bachelor of Science in Cyber Security and Security Management Degree Program, a member of the Risk Management Society and a 15 year Reserve Law Enforcement Officer for the City of Centralia, Washington.

Sielox LLC.
Booth # 1533

Crisis Management

Security System Engineering/Design

Active Shooter

Karen Evans, ASIS member
CEO
karen.evans@sielox.com
856-861-4570

Marketing/PR Contact
Mark Evans
EVP
info@sielox.com
856-861-4570

Professional Bio
With 30 years of experience, Ms. Evans is a seasoned veteran in the security industry leading sales teams regionally, nationally and internationally, developing strong business channel partners and spearheading the operations of the Sielox business. Karen presents at many conferences and in 2013 was awarded The Women's Security Council (WSC) second annual Woman of the Year Award

What do you see as the greatest opportunity for innovation? Integration of wireless locks to enhance lockdown capabilities for any facility. The reduced hardware and installation costs are key drivers to control every door with immediate lockdown capabilities.

STANLEY Healthcare
Booth # 3133

Workplace Violence

Steve Elder
Director of Communications
steve.elder@sbdinc.com
613-287-1428

Professional Bio
Steve Elder has held several roles in marketing and communications with STANLEY Healthcare over a 15+ year period. In that time, he has had the opportunity to learn from many healthcare professionals about the challenges of providing a safe environment for acute care patients, and residents in a long term care setting. He writes frequently on safety and security for healthcare, with a particular emphasis on how to integrate technology into the care environment.

What is the biggest challenge facing the industry today? Hospitals must get to grips with the rise in violence against staff. Security for patients (like infants) receives a lot of attention, and many hospitals having specialized electronic technology in place to provide individual security. But the stats show that staff members are even more at risk: 76% of nurses report verbal or physical violence in the last year, while in hot spots like the ED, such incidents happen weekly. There are techniques to reduce the likelihood of this happening and security technology to reduce the harm. Violence shouldn't be considered as "part of the job" and hospital workers deserve a safe workplace.

STANLEY Security
Booth # 3133

Active Shooter

Crime/Loss Prevention

Enterprise Security Risk Management

Personal safety, alarm verification, data analytics

Brad McMullen
Vice President Product Solutions & Marketing
brad.mcmullen@sbdinc.com
317-572-1937

Marketing/PR Contact
Lynda Murphy
President - Murphyknott PR
lynda@murphyknott.com
312-867-9177

Professional Bio
Product & Marketing Vice President leading the development of new, industry-changing solutions for end-user businesses looking to improve their security, business operations and ROI. Technology forward approach leveraging big data, virtual reality, and other tools to provide innovative solutions for customers.

What is the biggest challenge facing the industry today? Cyber Security Threats. Anything connected to the network could be an access point for hackers. We need to ensure all security solutions address the concern of Cyber Threat.

What do you see as the greatest opportunity for innovation? Autonomous drones and robots to provide real time data gathering and response.

What do you think will have the biggest impact on the industry in the next 3-5 years? Big Data, Machine Learning and Artificial Intelligence. The ability to gather, analyze and formulate decisions quickly based on data will drive enormous productivity and security insights for companies who choose to utilize these solutions.

Stratfor

Booth # 4583

Active Shooter

Soft Target Protection

Anti-terrorism

Scott Stewart
VP, Tactical Analysis
steve.elder@sbdinc.com
512-744-4300

Marketing/PR Contact
Joshua Cook
Director of Public Relations
joshua.cook@stratfor.com
512-744-4309

What is the biggest challenge facing the industry today? Information overload. Every day security professionals are being inundated with information - what I call electronic waterboarding - but they lack the tools to help turn this information into actionable intelligence by providing proper context.

Professional Bio
Scott Stewart supervises Stratfor's analysis of terrorism and security issues. Before joining Stratfor, he was a special agent with the U.S. State Department for 10 years and was involved in hundreds of terrorism investigations. Mr. Stewart was the lead State Department investigator assigned to the 1993 World Trade Center bombing and the follow-up New York City bomb plot. He also led a team of American agents assisting the Argentine investigation of the 1992 bombing of the Israeli Embassy in Buenos Aires and was involved in investigations following a series of attacks and attempted attacks by the Iraqi intelligence service during the first Gulf War.

What do you see as the greatest opportunity for innovation? Related to the problem of information overload, I believe that there is great opportunity to provide an innovative system for providing actionable intelligence to security professionals.

What do you think will have the biggest impact on the industry in the next 3-5 years? Continuing shifts in technology and the embrace of new technologies by criminals and terrorists.

Fred Burton
VP, Intelligence and Chief Security Officer
fred.burton@stratfor.com
512-744-4300

What is the biggest challenge facing the industry today? Perception, everyone is a security expert

What do you see as the greatest opportunity for innovation? Everyone is chasing the secret potion or magic wand to identify the next Edward Snowden in the workplace, including me.

Professional Bio
Fred Burton is Vice President of Intelligence and Counterterrorism at Stratfor, a leading geopolitical intelligence firm, and one of the world's foremost experts on security, terrorists and terrorist organizations. He is a former police officer, State Department special agent and New York times best-selling author.

Switch

Booth # 3133

Cybersecurity/ Information Security

Joseph McDonald, CPP, PSP
CSO
joe@switch.com
702-444-4106

What do you think will have the biggest impact on the industry in the next 3-5 years? The understanding that cyber is only another environment to be secured. Not a magical space where people use a different language. A different tool box will be needed, but the principles are the same.

Professional Bio
Joe is the Chief Security Officer for Switch Communications where he is responsible for personnel, physical, infrastructure and information security. He has an extensive and well-rounded background in Security, his chosen profession. For the past 25 years he purposefully worked in as many aspects of the Security Profession as he could. His career included positions as Corporate Facility Security Officer for a Defense contractor, Security and Facilities Director for a National Bank Call Center, Senior Security Consultant and Engineered Systems Sales Manager for major systems integrators designing large security and surveillance systems for gaming and industrial venues, and as a Municipal Police Officer.

TAL Global Corporation

Active Shooter

Crime/Loss Prevention

Crisis Management

Critical Infrastructure Protection

Enterprise Security Risk Management

Soft Target Protection

Anti-terrorism, Workplace Violence

Investigations

Insider threats

Employee Misconduct

Oscar Villanueva, CAL PI
Chief Operating Officer
ovillanueva@talglobal.net
661-607-4755

Marketing/PR Contact
Oscar Villanueva
Chief Operating Officer
ovillanueva@talglobal.net
661-607-4755

What is the biggest challenge facing the industry today? The transfer of institutional knowledge and succession planning are critical issue in need of attention by the industry. Addressing these issues effectively should be an institutional priority.

What do you see as the greatest opportunity for innovation? I believe the area of threat assessments in connection to workplace violence provides an opportunity for useful innovation. Going from a reactive stance to a well developed predictive capabilities will be key to effective threat management going forward.

What do you think will have the biggest impact on the industry in the next 3-5 years? The generational transition of professionals, some leaving and some entering the industry. This will create opportunities for continuing innovation in policies, tactics, and technology.

Professional Bio

Mr. Villanueva is an international security expert with decades of investigative, threat and risk assessment & management, training and critical infrastructure security experience in the U.S. and around the world. Mr. Villanueva had a distinguished career as a federal security and law enforcement agent, and as an executive at the United States Postal Inspection Service (USPIS). In this capacity, Mr. Villanueva led large scale investigative, security and law enforcement operations in several large metropolitan areas in the U.S., Europe, Africa, Asia and Latin America. These operations earned Mr. Villanueva respect and appreciation in the public and private sectors. Mr. Villanueva's corporate security experience, active client engagement, and expertise in workplace violence threat assessments, insider threat investigations and retail loss prevention and logistics security, among others disciplines, have continued to be strong asset for clients domestically and internationally. Mr. Villanueva is the former Chairman of the Postal Union of the Americas, Spain, and Portugal (PUASP) Security Action Group, an organization affiliated with the United Nations and headquartered in Montevideo, Uruguay. Under his leadership, the PUASP Security Action Group developed and delivered innovative investigative, security, and infrastructure protection solutions in Latin America, Europe, and the Caribbean.

TrackTik

Booth # 733

Enterprise Security Risk Management

Critical Infrastructure Protection

Security System Engineering/Design

Mark Folmer, CPP, MSyl
VP Industry & Security
mark@tracktik.com
1-514-654-6275

Marketing/PR Contact
Levin Schmid
International Expansion Coordinator
levin@tracktik.com
1-418-271-4900

What do you see as the greatest opportunity for innovation? The private security industry, more specifically the security services industry, tends to be change resistant. Despite the potential value of the services provided, most companies have yet to adopt new technologies. As security threats become more complex, there is a growing need for innovation. Technology, more specifically process automation, workforce management and optimizing data presents a major opportunity for improvement of security programs. If properly equipped and harnessed, front line security staff, numbering in the millions, then have the ability to directly contribute to the overall security

Professional Bio

Mark started in the industry after graduating in 1996 from Concordia University in Human Resource Management and International Business. His career progressed to senior level roles being responsible for an assortment of business units across Canada. In 2009 he launched a Management Consulting business focused on Physical Security for corporate clients. In 2011, Mark accepted the role of Senior Manager, Corporate Security at Canada's largest Telecommunications company. Mark attained his CPP and volunteers with ASIS International currently serving as SRVP Region 6. He sits on the Private Security Officer Standard Technical Committee, the Private Security Company (PSC.1) standard and Security Awareness working groups. He is a member of ASIS' Security Services Council. In 2016 Mark joined software company TrackTik as its Vice president Industry & Security.

programs in place at corporations. To successfully protect assets, centralized data collection and data use can play a crucial role in making operations and businesses more robust. Security issues have risen from the ranks of operational only to the ranks of operational and strategic. By integrating modern technology into security operations, data can be collected in real time and analysed to identify operational issues and raise awareness. By doing so, accountability is more easily guaranteed, as data driven solutions can lead change management and overall security improvements.

Vidsys

Booth # 2nd Floor Cedars Room at Omni Hotel *(attached to Kay Bailey Hutchison Conference Center)*

Enterprise Security Risk Management

Physical Security Information Management

Converged Security and Information Management

James Chong
Founder and Chief Executive Officer
chongj@vidsys.com
703-883-3730

Marketing/PR Contact
Avery Ross
Public Relations Contact
avery@bluetext.com
214-502-5007

Professional Bio

James founded Vidsys in 2005 with its transformational security and information management software platform. James has over 20 years of management and technology experience, making him a world-class subject matter expert in software, IT, video surveillance, security, and complex systems. His vision for developing a highly-specialized product-driven business led to the development of several industry-leading software applications.
Prior to becoming CEO in 2015, James served as CTO and was named International Data Group's "InfoWorld Top CTO 25" for his business management leadership and innovation in the converged security technology market. James also helped create the term "PSIM" in 2006, which has evolved to become a new category within the security market, and in 2014 he introduced the evolution of PSIM to CSIM and IoT solutions. Prior to starting Vidsys, James served over ten years in executive positions with Dynamic Technology Systems, Inc. leading integrated voice, video, and data communications solutions.

What is the biggest challenge facing the industry today? The challenge many organizations face today, is that there is a massive amount of data that is being collected that is neither actionable nor intelligent. This is a huge challenge for companies to figure out how to manage all of the incoming data, and not just manage it, but to use it effectively. From cameras to access control to all kinds of RFID or GPS devices generating data, organizations need an intelligent system that can pull in all of this information to visualize and unify what is going on, and provide procedures and action plans when a particular situation is occurring.

What do you see as the greatest opportunity for innovation? Smart buildings, cities and communities are going to transform that way that we live, work, eat and travel. We are already seeing many of these innovations for smart parking, lighting, public safety and more, but the solutions will continue to expand to improve our quality of life. The use cases are truly endless. Traffic management is one area where we are starting to see big things happen. Transportation departments are integrating with hardware around the city to understand traffic flow patterns, including how many people are going in what direction at what time, and can then in real-time change the programs so that there is a smoother flow of traffic around the city. This is one example of how a city can help its citizens in a tangible way, and Vidsys is excited to be a part of projects like these that are positively impacting everyday people's lives.

What do you think will have the biggest impact on the industry in the next 3-5 years? The ever-increasing interconnectedness of everything around us will continue to expand and impact our lives in ways we can't even currently imagine. As we talk about Internet of Things, or IoT, generating massive amounts of data, some are now saying that 45 to 50 billion objects will be connected to the cloud by the year 2020. Everything from our cell phones to our cars are now providing data that will be transformational for security, real-time data and intelligence for communities, schools, buildings, and more. There will be more opportunities for social media data to be a crucial tool, and IoT device data will become more sophisticated and useful in many ways. As this occurs, managing and having situational awareness of an organization's physical assets with IT assets will be paramount.

VOTI

Booth # 817

Enterprise Security Risk Management

Critical Infrastructure Protection

Crime/Loss Prevention

Rory Olson
President and CEO
Rory.olson@votidetection.com
514-782-1566

Marketing/PR Contact
Morgan Butler
Account Executive
morgan@bizcompr.com
903-285-8662

What is the biggest challenge facing the industry today? The biggest challenge facing the security industry as a whole is that the "good guys" are not keeping up with the "bad guys." X-ray security screening technology has not been able to catch up with the rapid pace and constant changes of the threats we're facing daily. X-ray screening isn't efficiently finding the emerging threats that the dynamic travel and workplace environment face daily across the world. VOTI's 3D perspective is changing this by providing a more intelligent security screening process.

Professional Bio

Rory Olson is the Chief Executive Officer of VOTI, a leading provider of latest-generation x-ray security systems based on breakthrough 3D perspective technologies in a growing $1.8B global market. A highly accomplished entrepreneur and public company executive with more than two decades of industry experience and a track record of success, Rory has strategically delivered explosive growth for technology businesses ranging from start-ups to mature multibillion-dollar enterprises, in industries ranging from online payment processing to mobile entertainment.

Watermark Risk Management International

Crisis Management

Soft Target Protection

Anti-terrorism

Dr. Jennifer Hesterman, Retired Air Force Colonel
Vice President, Business Resiliency
jenni.hesterman@wrmi-llc.com
571-289-7225

What is the biggest challenge facing the industry today? Insider threat is possibly the biggest challenge facing the security industry; those with legitimate access to our facilities, equipment, people and data are in the position to do the greatest harm.

What do you see as the greatest opportunity for innovation? Innovation is only possible when we leverage the imagination and creativity of our employees - we should encourage and reward their out-of-the box thinking!

What do you think will have the biggest impact on the industry in the next 3-5 years? Over reliance on technology will lead to significant security failures and a trend back towards the human as the best "weapon system" to observe, detect, and mitigate threats.

Professional Bio

Dr. Jennifer Hesterman is a retired Air Force colonel who served in three Pentagon tours and commanded in the field multiple times. She holds a doctoral degree from Benedictine University, Master of Science degrees from Johns Hopkins University and Air University, and a Bachelor of Science from Penn State University. She was as a National Defense and Harvard Senior Executive Fellow. Dr. Hesterman is Vice President, Business Resiliency and Education Services for Watermark Risk Management International and a senior fellow at the Center for Cyber and Homeland Security at George Washington University. Her book "Soft Target Hardening: Protecting People from Attack" was the ASIS Security Book of the Year for 2015. She also authored "Soft Target Crisis Management" (2016) and "The Terrorist-Criminal Nexus" (2013).