



**PERSON OF THE YEAR**  
TIMOTHY  
CARDINAL DOLAN  
ARCHBISHOP OF NEW YORK

# T&M Protection Resources

## Evolved for a Changing World

**Services include:**

- Executive Protection
- Security Consulting Services
- Sport & Entertainment Security
- Technology Risk
- Intelligence
- Investigations
- Litigation Support
- Sexual Misconduct Consulting & Investigations



230 Park Avenue, Suite 440, New York, NY 10169  
212.422.0000 www.tmprotection.com



**AN INDUSTRY LEADER**

[msasecurity.net](http://msasecurity.net)

## HIGH CONSEQUENCE THREAT PROTECTION



For over 30 years, MSA Security® has led the industry in providing best-in-class explosive detection, protective, investigative and intelligence services to address an evolving threat spectrum – protecting people, property and assets, and delivering greater peace of mind.

9 Murray Street, New York, NY | (212) 509-1336

**Look for the RED or BLUE DHS SAFETY Act Seal to receive the highest level of protection possible.**





Paul Cannon  
Electromechanical  
Specialist



Brian Casler  
Electromechanical  
Specialist



Vito Del Vecovo  
Electromechanical  
Specialist



Toby Heath  
Electromechanical  
Specialist



Mike McGorty Jr  
Integrated Solutions  
Specialist

Visit our booth at ASIS. Meet our team and look at a sampling of ASSA ABLOY Electromechanical solutions.

In today's complex world, connections are more critical than ever.

Visit ASSA ABLOY to learn how you can connect to more of what matters most at [assaabloydss.com](http://assaabloydss.com).



# Connect to More

Opportunities | People | Partnerships | Applications



The global leader in door opening solutions

**ASSA ABLOY**

The ASIS NYC Chapter thanks the following companies, organizations and institutions for their support to the chapter through advertising in this issue of *Security Director*.

Advanced Electronic Solutions	60
Aeroturn	24
Alliance Systems Integrators	12
AlliedUniversal	30
ASSA ABLOY	2
ASIS International	34
ASIS Long Island Chapter	58
Brownyard	58
Detex	28
Doyle Security Services	Back Cover
Doyle Security Services	46
Executive Protection Institute	16
Global Elite Group	16
Johnson Controls	8
Kratos	22
MSA	1
Mulligan	4
Opex	Inside Back
Riverdale Mills	60
Safeguards International	14
Securitas	26
Sentinel Consulting	6
T&M Protection Resources	Inside Front
Yama	70



Chapter Leadership	5
From the Editor's Desk	7
Chapter Leadership Message	9
Person of the Year	10
Eugene Casey Award	13
Keynote Speaker	15
Award of Merit: Mulligan Security	17
Conference Program	35
Directory of Exhibitors	38
Exhibitors List & Booth Numbers	45

## Articles

Javits Embraces High-Tech Hospitality	18
Protecting Houses of Worship	27
Managing Security Projects	32
Beyond Bollards	47
Surviving Mother Nature	49
Physical Access Control Systems	52
Certification Profile: Caress Kennedy	55
Small Unmanned Aerial Systems	56
Evaluating the Total Resilience Lifecycle	59
Advancing Security in NYC and Beyond	62
Disruptive Technology	64
Workplace Harassment	66
Is Your Mailroom Your Open Door?	68
Trade Show Committees	70
Women in Security	71

CONTENTS



**WE KNOW THE NEW YORK  
METRO AREA LIKE NO OTHER  
PRIVATE SECURITY FIRM.**



- **High-Rise Security and Access Control**
- **Fire/Life Safety**
- **Executive Protection**
- **Consulting and Investigative Services**



**MULLIGAN**  
SECURITY

Two Penn Plaza New York NY 10121 212-563-0500 www.MulliganSecurity.com



**ASIS International  
New York City Chapter  
Leadership**

**Elected Officers**

**Chairman**

Lynn Brown  
Secure Access & Digital Systems  
516-623-7500  
info@secureaccessds.com

**Chapter Vice Chairman**

Don Francisco, CPP  
Advanced Electronic Solutions, Inc.  
347-386-2146  
dfrancisco@nyaes.com

**Treasurer**

Steve Sacchetti  
Allied Universal Security Services  
212-328-0209  
stephen.sacchetti@aus.com

**Secretary**

Brian Reich, CPP  
TD Bank, N.A.

**Sergeant at Arms**

Manny Gomez, CPP  
MG Security Services  
917-270-1196  
mgomez@mgsecurityservcies.com

**Advisory Board**

George W. Anderson  
Port Authority of NY/NJ  
212-435-4002  
ganderson@panynj.gov

Lynn Brown  
Secure Access & Digital Systems  
516-623-7500  
info@secureaccessds.com

Raymond L. Dean, CPP  
Access System Integration  
917-592-9091  
raymond.dn@gmail.com

Lawrence Loesch, CPP, Esq.  
Security Consultant  
646-831-4868  
lfoesch1@yahoo.com

Craig Schwab, MBA, CPP  
BlackRock, Inc.  
646-231-1466  
craig.schwab@blackrock.com

**Women in Security Liaison**

Denise Niles  
Advanced Electronic Solutions, Inc.  
718-461-2600  
dniles@nyaes.com

**Young Professionals Liaison**

Izabela Regula  
Allied Universal Security Services  
212-271-0659  
izabela.pelszynska@aus.com

Jairo Borja, MBA  
Berkeley College  
212-986-4343  
jib@berkeleycollege.edu

**Law Enforcement Liaison**

Joseph D'Amico  
MSA Security  
212-509-1336 x 294  
jdamico@msasecurity.net

Lt. Michael T. O'Sullivan  
New York State Police, Troop NYC  
917-492-7157  
michael.osullivan@troopers.ny.gov

**Legislative Council Rep.**

Lawrence Loesch, CPP, Esq.  
Security Consultant  
646-831-4868  
lfoesch1@yahoo.com

**Committee Chairs/Co-Chairs**

**CPP Continuing Education**

Michael Hymanson, CPP  
US Security Associates  
914-557-4277  
mhymanson@ussecurityassociates.com

**Membership**

Maria DiCarlo Cofell  
First Republic Bank  
212-506-7787  
mcofell@firstrepublic.com

**Program Committee**

George W. Anderson, Chair  
Port Authority of NY/NJ  
212-435-4002  
ganderson@panynj.gov

Maria DiCarlo Cofell  
First Republic Bank  
212-506-7787  
mcofell@firstrepublic.com

Cynthia Webster, CFE  
Reynard Group LLC  
212-399-5651  
cwebster@reynardgroup.com

Izabela Regula  
Allied Universal Security Services  
212-271-0659  
izabela.pelszynska@aus.com

**Speaker Committee**

Terence B. Hoey, CPP, PCI, PSP  
US DHS, FEMA, Region II  
646-372-0838  
terence.hoey@fema.dhs.gov

Kenneth McGuire  
MSA Security  
212-509-1336 x 224  
kmcguire@msasecurity.net

**Trade Show Committee**

Raymond L. Dean, CPP, Chair  
Access System Integration  
917-592-9091  
raymond.dn@gmail.com

Craig Schwab, MBA, CPP, Co-Chair  
BlackRock, Inc.  
646-231-1466  
craig.schwab@blackrock.com

**Chapter Information Officer**

Rich Patti, CISSP  
Comtek Solutions  
856-424-1223 (Office)  
rich@comtek-s.com

**Vice President**

**ASIS Region 5D**  
Donald J. Nailor, PSP  
Siemens Industry, Inc.  
860-883-4776  
donald.nailor@siemens.com

**Vice President**

**ASIS Region 5D**  
Mario J. Doyle, CPP  
Doyle Security Services  
646-831-4868  
mdoyle@asisli.org

**Annual Golf Outing**

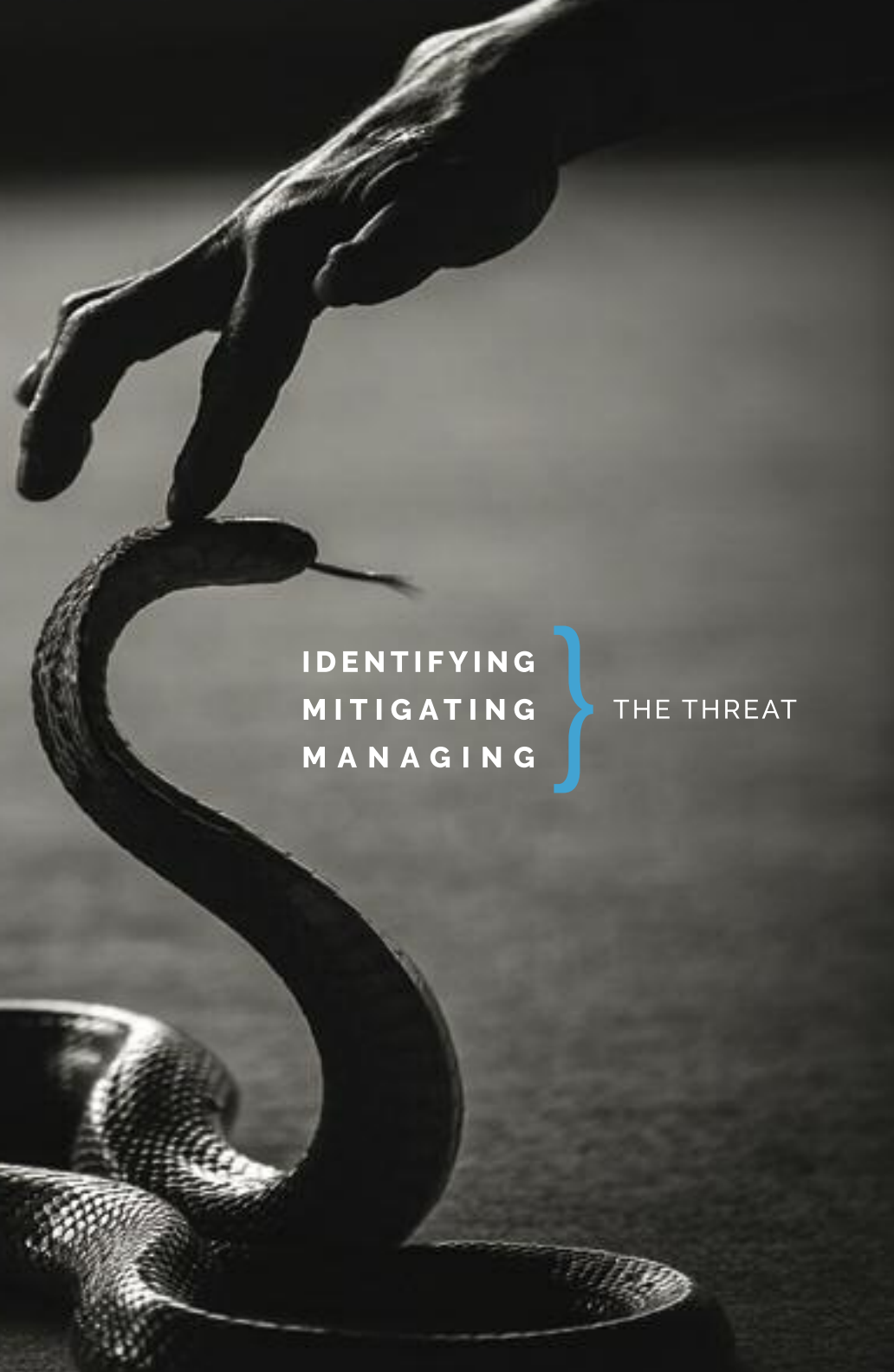
Lynn Brown, Chair  
Secure Access & Digital Systems  
516-623-7500  
chairman@asisnyc.org

**Security Director Magazine**





Cynthia Webster, CFE, Editor  
The Reynard Group LLC  
212-399-5651  
cwebster@reynardgroup.com

Don Blauweiss, Art Director  
Don Blauweiss Advertising & Design  
don@blauweissadvertising.com  
914-779-6846

Diane Dudzinski, Advertising  
Don Blauweiss Advertising & Design  
diane@blauweissadvertising.com  
914-779-6846



IDENTIFYING  
MITIGATING  
MANAGING } THE THREAT

-  Assessment & Planning
-  Engineering & Design
-  Managed Services
-  Security Training

# CREATING SECURE ENVIRONMENTS

## From The Editor's Desk



Welcome to the 2018 edition of Security Director Magazine and the 28th ASIS NYC Security Conference and Trade Show operated in conjunction with ASIS International. I hope that you have an opportunity to take advantage of all that the Show offers.

The theme for 2018 is "Advancing Security in New York City and Beyond" and Security Director Magazine contains recommendations and ideas from new contributors as well as familiar bylines. Maybe you are the manager of a security project or leading an investigation into sexual harassment. Maybe your company wants to add drones to its emergency management plan or maybe your mailroom is not secure. Whatever your concerns, you will find products and services highlighted on the pages in the magazine in addition to articles from your colleagues that tackle difficult subjects and provide food for thought. Speaking of drones, you won't want to miss the panel discussion moderated by Don Francisco, CPP, Vice-Chairman of the NYC Chapter. He has convened a panel of experts who will discuss the pros and cons of using drones for emergency management and how these unmanned aerial systems are here to stay.

You can also read about Timothy Cardinal Dolan's illustrious career. We are honoring His Eminence, Timothy Cardinal Dolan, Archbishop of New York, as our Person of the Year. He is known for his warmth, his sense of humor and his kindness to members of law enforcement and their families and you won't want to miss his remarks at the Person of the Year luncheon on May 17th.

Terence B. "(Terry)" Hoey, CPP, PCI, PSP, is the recipient of this year's Eugene J. Casey CPP Award and you can read about him in the magazine. The Eugene J. Casey CPP Award is given for distinguished service to the NYC Chapter and Terry, a true patriot, always finds time to serve the chapter.

We are also honoring Bill and Kevin Mulligan, the father-son team behind Mulligan Security Corp., with the first ever Award of Merit. Their decades-long support of the Mulligan Match at the annual golf outing has made it possible for the Chapter to support many worthwhile charities.

For those who are new to this industry or are reading this magazine for the first time, ASIS, originally known as the American Society of Industrial Security, encompasses the ever-expanding world of security to include everyone who has a role in the protection of assets. Volunteers are essential to the NYC Chapter and I hope that you will consider

participating in our many events throughout the year. Please reach out to the leadership of the NYC Chapter; their contact information is in the magazine and they will welcome your input. No one ever has time to volunteer so just do it!

ASIS is made up of the best security and law enforcement professionals in the world and it is a privilege to be a member and to serve as the editor of this magazine. One young man will never have the opportunity to be a member of ASIS. Cpl. Alejandro ("Alex") Romero, USMC, was killed in a freak parachute mishap on January 22, 2018. Cpl. Romero, 22, was a member of Bravo Company, Third Reconnaissance Battalion, and was by all accounts, an exemplary Marine. He joins the ranks of all of our dedicated men and women who serve and have served on the front line.

I hope that you enjoy the 28th Trade Show and look forward to hearing from you by email at [editor@asisnyc.org](mailto:editor@asisnyc.org). According to Socrates, "The secret of change is to focus all of your energy, not on fighting the old, but on building the new." The 2019 Security Conference and Trade Show will be here before you know it. See you next year!

*Cynthia (Cindy) Webster, CFE*  
Editor  
[editor@asisnyc.org](mailto:editor@asisnyc.org).

# Safer. SMARTER. Secure Protection.

Tyco is now Johnson Controls, the world leader in security, fire protection, HVAC, building controls and energy storage. With industry-leading integration services we help you improve how you manage security and provide protection, safeguarding against theft, violence and threats.



To learn more, visit [TycoIS.com](http://TycoIS.com) or contact one of our representatives.

## **James R. Kitchen**

Manager, National Accounts/Corporate Sales  
[jim.kitchen@jci.com](mailto:jim.kitchen@jci.com)



## A MESSAGE FROM YOUR **CHAPTER LEADERSHIP**



**Lynn Brown**



**Don Francisco**

Welcome to the 28th Annual Security Conference, Educational Seminars and Trade Show presented by the NYC Chapter of ASIS and ASIS International.

The NYC Chapter of ASIS is excited and proud to welcome His Eminence, Timothy Cardinal Dolan, the Archbishop of New York, as the Person of the Year.

Twenty-eight years ago, our trade show plus educational seminars, started with six vendors on the mezzanine level of the Penta Hotel and has grown into one of five global ASIS educational trade shows. It is the largest regional trade show of its kind and it is where thousands of security and law enforcement professionals can view the latest technology and services as well as attend a full roster of educational programs and networking events, including the Spring Fling 2018 where like-minded security professionals enjoyed a relaxing evening of fun, food and drinks at the Hard Rock Café.

This has been an exciting year for the Chapter. Our CPP Review class, offered in October and November 2017, was well-attended and a success. We supported several charities including Samaritan Purse, the Make-A-Wish-Foundation, and the Ricky Martin Foundation, a not-for-profit organization that provided relief to the residents of Puerto Rico after that island was devastated by Hurricane Maria. Our monthly lunch meetings have showcased dynamic guest speakers who share their knowledge and expertise and in February 2018, we had a breakfast meeting at the New York City headquarters of Facebook that included a behind-the-scenes tour of the facility, led by Nick Lovrien, Facebook's Global CSO.

The Board has supported the efforts of our Women in Security (WIS) and our Young Professionals (YP) to continue to grow the membership of this great Chapter.

Our scholarship program promotes and supports higher education as

well as recognizes and rewards the outstanding achievement and professionalism of those in our industry. In addition, our Chapter is proud to sponsor a Mentoring Program.

The NYC Chapter of ASIS is blessed with the best security and law enforcement professionals in the industry and I am honored to call them colleagues and friends. Our Chapter would not be great without the ongoing support of numerous volunteers and companies that understand the need to leverage our resources and shared knowledge for the betterment of the security industry.

Don and I look forward to seeing you at our annual charity golf outing on June 11, 2018 at The Village Club of Sands Point. All proceeds will be donated to the St. Jude Children's Research Hospital, so please plan to join us for a fun-filled day on a beautiful golf course.

*Lynn Brown, Chapter Chairman*

*Don Francisco, CPP, Vice Chairman*

*His Eminence*  
**Timothy**  
**Cardinal Dolan**  
 Archbishop of New York



Timothy Dolan was named Archbishop of New York by Pope Benedict XVI on February 23, 2009.

He had served as Archbishop of Milwaukee, appointed there by Pope Saint John Paul II on June 25, 2002.

Born February 6, 1950, Cardinal Dolan was the first of five children born to Shirley and Robert Dolan. His education began at Holy Infant Parish School in Ballwin, Missouri, and continued through the high school and college seminaries in Saint Louis. He then completed his priestly formation at the Pontifical North American College in Rome, where he earned a License in Sacred Theology at the Pontifical University of St. Thomas Aquinas.

Ordained to the priesthood for the Archdiocese of Saint Louis on June 19, 1976, he served as associate pastor at Immacolata Parish in Richmond

Heights, Mo., until 1979 when he began studies for a doctorate in American Church History at The Catholic University of America.

On his return to Saint Louis, Cardinal Dolan again served in parish ministry from 1983-87, and then was appointed to a five-year term as secretary to the Apostolic Nunciature in Washington, D.C. When he returned to St. Louis in 1992, he was appointed vice-rector and professor of Church History at Kenrick-Glennon Seminary, as well as an adjunct professor of theology at Saint Louis University.

In 1994, he was appointed rector of the Pontifical North American College in Rome, where he remained until June 2001. While in Rome, he also served as a visiting professor of Church History both at the Pontifical Gregorian University and the Pontifical University of St. Thomas Aquinas.



On June 19, 2001 — the 25th anniversary of his ordination to the priesthood — then Monsignor Dolan was named the Auxiliary Bishop of St. Louis by Pope Saint John Paul II, choosing for his Episcopal motto the profession of faith of St. Peter: *Ad Quem Ibimus*, "To Whom Shall We Go?" (Jn 6:68).

Cardinal Dolan served as chairman of Catholic Relief Services, and is a member of the Board of Trustees of The Catholic University of America. He is also a member of the Pontifical Council for Promoting New Evangelization, the Pontifical Council for Social Communications; and, at the Vatican, the Congregation for Eastern Churches,

and the Congregation for the Evangelization of Peoples.

Cardinal Dolan was elected to a three year term as president of the United States Conference of Catholic Bishops, in November, 2010. He now serves as chair of the Bishops' Committee on Pro-Life activities.

On January 6, 2012, His Holiness Pope Benedict XVI announced that Timothy Dolan was to be appointed to the College of Cardinals.

Following the resignation of Pope Benedict XVI, Cardinal Dolan participated in the Conclave that elected Pope Francis in March, 2013.

# Alliance Systems Integrators



CCTV Security Systems Command Center



Data Infrastructure



Critical Infrastructure



IP Video Systems



Enterprise Access Control Systems

Alliance Systems Integrators, Inc. has been in the security business since 1992. We've designed and installed cctv security systems, perimeter detection and access control systems utilizing the latest and most innovative technologies. Alliance believes in quality and pride in every facet of our work.

We have implemented advanced security solutions for businesses, utilities and major organizations in the Northeastern

part of the U.S. We provide clientele with expert installations of security and communication systems.



Licensed by NYS Dept. of State

855-616-SAFE

[www.AllianceSystemsIntegrators.com](http://www.AllianceSystemsIntegrators.com)

## Terence B. Hoey



Terence B. Hoey ("Terry"), is employed by the U.S. Department of Homeland Security (DHS), Federal Emergency Management Agency (FEMA), Region 2 (R2), Office of the Regional Administrator (ORA), as the Law Enforcement Liaison (LEL) and intelligence representative. He is assigned to the Federal Bureau of Investigation (FBI), New York Field Office, Counterterrorism Division, Joint Terrorism Task Force (JTTF) and the Crisis Management Squad (A-17).

He is a key advisor to the Regional Administrator on all issue related to law enforcement liaison activities, intelligence, information-sharing and critical infrastructure protection. He is also regarded as a subject matter expert in the application of the Prevention, Protection and Response Mission areas. His area of responsibility spans New York, New Jersey, Puerto Rico and the U.S. Virgin Islands.

Prior to joining FEMA, R2 he was a senior leader, federal law enforcement officer (FLEO) and program manager with DHS, Federal Protective Service (FPS), R2 where he was responsible, at the regional level, for the law enforcement and physical security management programs throughout New York, New Jersey, Puerto Rico and the U.S. Virgin Islands.

Terence holds all three coveted board certifications from ASIS International: Certified Protection Professional (CPP); Professional Certified Investigator (PCI); and Physical Security Professional (PSP). He is regarded as an expert in all areas of security management, protection, investigations and cyber/physical security. In June of 2016, Terence was recognized as the first DHS employee to receive all three ASIS board certifications, referred to as the "Triple Crown." At that time, he was one of six in

the entire federal government with all three ASIS board certifications and one of approximately 135 worldwide.

He is an active member of several professional and not for profit organizations, including: ASIS International, Chief Security Officer (CSO) Center; ASIS NYC Chapter; National Law Enforcement Associates (NLEA); International Association of Chiefs of Police (IACP) and appointed to the Private Sector Liaison Committee (PSLC); and The General Society of Mechanics and Tradesman of the City of New York; and the Ancient Order of Hibernians (AOH).

In addition, he is an Ambassador and Servant Leader for the Navy SEAL Foundation (NSF), a member of the Camp Fire Club of America (CFCA) and a trained Boy Scouts of America Leader. He is an accomplished Stolen Valor researcher and investigator and Veterans advocate and his work has attracted national media attention.

Terry is a retired U.S. Navy Master Chief Petty Officer (MCPO) who spent 32 years on active and reserve duty from 1979 through 2011. He is an Honor Graduate of the U.S. Navy Senior Enlisted Academy (SEA) Class 94, Brown Group. Major tours and commands included: USS Valdez (FF-1096); USS Edson (DD-946); Instructor at Surface Warfare Officers School Command (SWOSCOLCOM), graduating Engineering Officer of the Watch (EOOW) Course, Class #1; USS Hepburn (FF-1055) where he served as an EOOW and the Oil King; Naval Reserve (NR) Naval Special Warfare (NSW) Unit TWO and deployed to NSW Unit TWO in Machrihanish, Scotland for Operation DESERT STORM; NR Mobile Inshore Undersea Warfare (MIUW) Unit 203; NR EOD Technical Division;

Continued on page 72

# WHY DID THE UNIVERSITY OF NEVADA LAS VEGAS CHOOSE SAFEGUARDS INTERNATIONAL FOR CRISIS PLANNING AND SECURITY?



**THEY WANTED TO PLAY IT SAFE.**

## SO DID THE GUGGENHEIM MUSEUM, NEW YORK PUBLIC LIBRARY, SILVERSTEIN PROPERTIES, MT. SINAI HOSPITAL AND CORPORATIONS AND ACADEMIC FACILITIES ALL OVER THE USA.

*"Safeguards International did an outstanding job designing a security system for our 40,000-seat stadium and perimeter. So when we needed a video surveillance system for our 300-acre campus, we trusted Safeguards International to design and oversee it."*

Jose A. Elique, Chief of Police  
Director, UNLV Department of Police Services

Safeguards International is a full service electronic security, life safety systems and design company.

For over 20 years SI has designed comprehensive systems which address the specific, immediate and long-term asset protection, loss prevention and risk management needs of commercial, industrial, institutional, cultural and residential properties.

### Safeguards International's expertise includes these critical areas of security:

- Consulting and Project Management
- System Design and Specifications

- Risk and Vulnerability Analysis
- Business Continuity Planning
- Merger and Acquisition Due Diligence
- Compliance to NYFD Local Law 26
- Workplace Violence Intervention Strategies
- Emergency Planning
- Disaster Recovery
- IT Security and Network Security

You'll feel more secure when your security is with the company America trusts.



**Allan Schwartz, CPP, CHS-IV** is founder and President/CEO of Safeguards International. He brings a significant and rare technological background to the security field.

As a rocket scientist he developed numerous innovations in America's defense and space programs. He is Board Certified in Homeland Security level IV. He is also an ASIS International Board Certified Protection Professional.



**SAFEGUARDS INTERNATIONAL, INC.**  
**Crisis planning and security. Play it safe.**  
914.771.9739 ■ [www.safeguardsintl.com](http://www.safeguardsintl.com)

## Scott Morrison

Managing Director

Head of Global Crisis Management/  
Command Centers and North America Security  
JPMorgan Chase & Co.



Scott Morrison is currently the Head of Global Crisis Management and Command Centers at JPMorgan Chase & Co. where he is responsible for the Crisis Management process and the Command Centers in New York, London, and Singapore that provide 24/7/365 over-watch of more than 240,000 employees operating globally in over 60 countries. He also serves as the Regional Security Manager for North America and is responsible for protecting 195,000 employees across 6000+ corporate and Chase retail sites. In addition, his remit includes 16,000+ ATMs, frequent high profile corporate events, and more than 25 high value facilities.

Previously, Scott served as the Executive Strategic Initiatives Advisor to the three-star Commander. He concurrently served as the Director of the Commander's Action Group (CAG) at the NATO Special Operations Headquarters (NSHQ) in Belgium where he focused on strategic political-military issues and was responsible for maintaining connectivity with key stakeholders, conducting analysis and assessments, and developing strategic initiatives. Prior to that assignment, he served as the NSHQ Liaison to the U.S. European Command (USEUCOM), the Special Operations Command Europe (SOCEUR), and the Special Operations Command Africa (SOCAFRICA) in Stuttgart, Germany. Before joining the NSHQ, he worked as a consultant for Booz Allen Hamilton in McLean, Virginia, focusing on Special Operations, Irregular

Warfare (IW), and partner Special Operations Forces (SOF), during which time he conducted an extensive study of NATO SOF.

Mr. Morrison served twenty years in the United States Army where he began his career as a rifleman

in C Company, 1st Battalion, 75th Infantry (Ranger) and completed his service on the Army Staff in the Pentagon focusing on Special Operations issues. He led an Airborne Infantry Rifle Platoon in the 82nd Airborne Division during the first Gulf War and subsequently entered Army Special Forces where his primary focus was in-extremis operations. During his tenure in Special Operations he deployed on a wide variety of missions in the Balkans, Southwest Asia, and Africa. Mr. Morrison also spent a year in Iraq as the senior advisor to the Commander of the 3rd Brigade of the 2nd Iraqi Infantry Division.

Mr. Morrison has lived and served abroad for over 17 years and has extensive experience working alongside Allies and other international partners in multinational environments. He holds a MA in Defence Studies from King's College, University of London; a MA in Military Science in Unconventional Warfare from American Military University; and a BS in Engineering with a concentration in Military Studies from the United States Military Academy at West Point. Mr. Morrison is also a graduate of the United Kingdom's Joint Services Command and Staff College.



**Go beyond old-school bodyguards. Become a pro in protection.**

Train with some of the most experienced, most honorable pros in the business. Learn about EPI. [www.personalprotection.com](http://www.personalprotection.com)



**EPI EXECUTIVE PROTECTION INSTITUTE**  
WE PUT THE PRO IN PROTECTION

## Mulligan Security Corp.

The New York Chapter of ASIS International could not function without the support of companies and individuals. To that order, the Board of Directors created The Award of Merit in 2017 and is proud to announce that the first winner of the award is Mulligan Security Corp. ("Mulligan"). For more than 20 years, Mulligan has gone above and beyond the call of duty with unstinting support for the many activities of the New York City Chapter including our educational seminars, lunches and their annual sponsorship of the hole-in-one prize at the annual charity golf tournament plus the Mulligan Match.

What began as a throw-away comment among friends has grown into a substantial commitment from Mulligan and each year, their dollar-for-dollar match allows the NYC Chapter to support such worthwhile charities as Vet Dogs of America and the Lexie Bean Foundation. In the words of Lynn Brown, the Chairman of the NYC Chapter of ASIS and Chairman of the Annual Golf Outing, "None of my requests have ever been denied. Bill and Kevin Mulligan are gracious, special people and our industry is lucky to have them."

Mulligan Security Corp. was founded in 1992 by William (Bill) P. Mulligan, a true visionary, and his son, Kevin Mulligan, the guiding hand behind the vision. Bill and Kevin studied the NYC security industry and determined how to vastly improve the quality of security services available to prime high-rise commercial office buildings, major corporate facilities, and client company headquarters.

The answer was simple: the combination of a better-trained and more professional team provides a superior product to clients.

Bill's 23 years as a detective with the New York City Police Department and as a Federal Agent were filled with intense, hands on, real-world experiences. Bill developed instincts from thousands of hours on the street investigating an assortment of criminal cases that allowed him to sense the unseen and anticipate the unknown.



Alongside his father, Kevin developed the business side of Mulligan Security from the ground up. While attending St. Johns University Kevin worked on the weekends as a Mulligan security officer in order to better understand the true nature of the business.

From the beginning Kevin and his father understood the importance of establishing a well-trained and highly-professional security staff. Always looking for ways to better protect their clients, the Mulligans determined that improved training and supervision on fire safety for building personnel, security officers, and tenants was necessary. As a result, they developed a Fire Safety Director program within their corporation. Since that time Mulligan has implemented 24/7 coverage of Fire Safety Directors at their sites. They have also expanded their executive protection, consulting, and investigative services practices. Mulligan Security's primary goal is always to be the best, not the biggest, and they have truly been a best friend to the NYC Chapter of ASIS. We wish them every success as they continue to provide the highest level of security and personal service.




**GLOBAL ELITE GROUP**

**THE LEADER IN PROTECTIVE SERVICES**

- Building Security & Access Control
- Event & Venue Security Services
- Canine & Screening Equipment Services
- Fire Guard Watch Services

Everyday Global Elite Group protects the people, property and assets of clients through its highly-specialized security service divisions focused on physical security, emergency management, consulting and aviation security.

A customized approach to all your on-going security needs from physical applications for corporate facilities and properties, to emergency response and after incident services. Event security for functions and venues of all sizes, public or private.

Global Elite Group has fully-staffed offices around the world including South America, Asia, Europe and the Middle East.

*Be Global. Go Global.*

[inquiries@globaleliteinc.com](mailto:inquiries@globaleliteinc.com) • 516.414.0487  
[www.globaleliteinc.com](http://www.globaleliteinc.com)




 US OSPAs 2016 & 2017 Winner of Outstanding Contract Security Company.



# JAVITS EMBRACES HIGH-TECH HOSPITALITY

By Holly Gilbert Stowell

**W**ith 3 million visitors crossing its threshold annually, the Jacob K. Javits Convention Center is a New York City landmark. It's hard to miss the six-block long complex, which stretches from West 34th Street to West 40th Street in midtown Manhattan and features more than 840,000 square feet of exhibition space and 28,000 square feet of meeting rooms. Javits hosts an array of events annually, including the New York International Auto Show, the National Retail Federation's annual convention, and New York Comic Con.

The Javits Center has undergone changes in recent years, including a \$463 million renovation from 2009 to 2014. In addition to improvements to the mechanical and sustainability systems, the upgrade included adding 6,000 new glass panels to the outside. Before the new patterned panels

were installed, Javits had a mirror-like façade, making the facility among the top bird-killers in New York City. Birds would frequently fly into the glass walls, not recognizing that the building was there.

Now Javits is considered one of New York's bird-friendliest facilities; besides upgrading the panels, Javits installed a green roof space spanning nearly 7 acres, which is home to 26 bird species. This rooftop also lowers the facility's annual energy consumption by 26 percent by lowering heat-gain and water runoff.

But hospitality at Javits is not just for the birds. Providing excellent customer service while maintaining security is a top priority for the center. Security personnel are front and center when customers approach the immediate outside vicinity or enter the building.

"We're engaging the client, making eye contact with the people coming in—we want to be the first person you see when you come in the door," says Kenneth Dixon, director of security and safety solutions at Javits. "Our focus is a balance



Courtesy Javits Center

between hospitality and security, and finding that right balance is a key to our success."

## CHALLENGES

Being a busy convention center means constantly dealing with theft, lost property, and other larceny issues, Dixon explains.

The type of theft that occurs varies, including exhibitors who steal from other exhibitors, attendees who steal from exhibitors, and employee theft.

The threat of terrorism also looms large over Javits, where anywhere from 60,000 to 70,000 attendees gather daily. In the spirit of being proactive, security decided to move heavy cement planters to a strategic location in front of the building "to give us a little more protection against vehicular attacks like the ones in London, Berlin, and Stockholm," he says.

Unattended packages are also a cause for concern, Dixon says, citing the 2013 Boston Marathon bombings and other terror attacks caused by improvised explosive devices left behind.

To further address these security concerns, and to align with the new look and feel from the recent renovation at Javits, Dixon explains that there have been several changes to security procedures, technologies, and staffing at Javits.

"It was the first quarter of 2015 when we started implementing some new policies, and really started to monitor what happened at night, as well as address the legacy larceny complaints that we've had," Dixon says.

With a new and improved

security operations center, an increase in the security workforce, and a hospitality-centered approach, Dixon is confident Javits is now an even safer place for its customers, vendors, and staff. Here's a look at some of the ways in which the Javits Center has accomplished that mission.

## TECHNOLOGY

Upgrading the center's security technology was a foundational step in beefing up security at Javits, and the center upgraded everything from cameras to its state-of-the-art command center. Dixon notes that Javits went from 150 legacy cameras to 860 4K-resolution IP cameras from Axis and Arecont Vision in the last year and a half.

### Cameras.

As of press time, the center anticipates having approximately 1,000 cameras at the end of this summer. They are situated throughout the facility, Dixon says, including in the exhibit space, at ingress and egress points, and on the loading docks.

Not only has Javits increased the number and quality of its cameras, but security decided to strategically place them at a visual level where they serve

as a deterrent. In the past, cameras were placed above people's heads and were



Courtesy Javits Center

painted the same color as the walls and columns to create a more visually appealing look. Now, however, the cameras are placed lower and unpainted, so they may be clearly seen by everyone who comes to the center.

"The people who are looking for the cameras really see them, and know that they are being filmed," says Dixon. "The chances of getting away with something here at the Javits Center are far less than what they used to be."

Javits is also currently testing a video management system from Genetec to manage the wealth of footage collected by the cameras. In addition, the cameras have facial recognition technology capability, so that video can be exported to law enforcement for identification if the need arises.

### Command center.

The command center at Javits is the heart and soul of the safety and security program, Dixon says, and is used for monitoring, dispatch, video review, and alarm monitoring.

Last spring, Javits put in an 18-monitor video wall from Orion that can be customized to view the cameras chosen by the operator. "That allows us to show 30, 40, 50, 60 cameras at a time—or just one at a time—on 18 monitors," Dixon explains. "We can quickly change camera layouts on the video wall for whatever's going on at any given time."

One monitor is dedicated solely to door alarms. Security can also automatically lock large gates and doors with the click of a button. "We have 225 perimeter doors," Dixon says, "each of the doors has a reader in the door that lets us know whether the door is opened or closed."

If a door alarm is triggered, an audible alert, as well as video associated with the incident, automatically populates the monitor. This lets officers easily determine whether a response is warranted.

The remote open-and-close feature greatly improved convenience for guards working in the building on an overnight shift. "Years ago, we would have dispatched a security guard on the overnight

[shift]...he's maybe two or three city blocks away, and he would have to go open up the gate," Dixon notes. "Now he can just do that remotely."

Members of the safety team who patrol the show floor have smartphones to receive photographs and other media related to any dispatch calls. For example, if a child goes missing, a photo or description can be immediately disseminated.

Analytics. Frequently, crime at the Javits Center isn't reported until the victim realizes his or her property is missing, which can be hours after it occurs. Or someone leaves a package unattended, with no trace of who the person was.

The security team wanted a video analytics solution to aid in the investigative process, so it turned to BriefCam software, which compresses hours of video into just a few minutes by speeding it up. "We use BriefCam to solve cases of property that may go missing for one reason or another...and for unattended packages," Dixon says. "It's been a real game changer for us."

If someone leaves a package unattended, or stolen property is reported from a specific place, BriefCam can geofence the area where the item was left or stolen, and show the activity that occurred within a certain timeframe.

Other specific parameters can

be set; for example, if security has information about the color of clothing the suspect was wearing, it can isolate the video to show only people wearing that color. "We're able to see all the activity around the area of concern, and watch 13 or 14 hours of video in a short period of time," Dixon says. "That has helped us close significantly more cases."

At the 2016 New York Comic Con show, for example, BriefCam analytics led to several arrests when property went missing from an exhibitor's booth. Security isolated video to just around the booth and ran analytics to find the thieves.

"In the past, we didn't have the ability to run analytics like we had in this case, and the person would have been long gone," Dixon says. "The show would have been over, and we would have been chasing our tail trying to get all the information."

### Floor plans.

The floor space at Javits is versatile, and conventions can choose the layout they want at their shows. Javits also has 28,000 square feet of flexible meeting room space, meaning that the walls can be easily converted to accommodate smaller or larger groups.

The center recently moved from traditional locks and keys on its meeting room doors to card readers to provide a greater level of security, and it can

assign key cards to clients, which expire when their meeting or convention concludes.

But flexibility can come with challenges. In the event of an incident or emergency at the facility, pinpointing an exact location in the building for first responders can be difficult, because the Javits Center stretches for six city blocks, and every convention has a unique floor plan.



Courtesy Javits Center

"We've been struggling over the last year and a half to replace outdated emergency evacuation plans, because we do 175 events every year—and every single one of them is different," Dixon says.

When police or fire departments respond to an emergency or incident, they often come to the facility's main address on West 34th Street. "We have to say, 'No guys, it's actually on 39th

Street in Hall C.' Well, they don't know where Hall C is—so it ends up causing a lot of confusion and a lot of wasted time," he says.

A recently declassified geospatial tool from BAE Systems allows Javits to pinpoint a more exact location within the building. The solution works by laying customized show floor plans over the existing blueprint of the center and labeling a grid by numbers and letters.

"Now we simply say, for example, 'Go to H-33,' and first responders know, within a certain amount of space, that's exactly where the incident is," Dixon explains.

The tool also works as an evacuation map, pointing out ingress and egress routes and the adjacent streets they spill out onto. It also shows first aid office locations and where to find defibrillator machines.

"For a building that's six blocks long, it is extremely difficult to have one security evacuation plan that you can effectively articulate and communicate to everyone who is going to be involved," Dixon says.

The safety team has an app from BAE Systems on its smartphones that displays the grid for each show and evacuation routes. Javits eventually hopes to expand that app to first responders. "Right now, we are communicating with responders with a PDF, but they still find that extremely useful," he notes.

## CUSTOMER SERVICE

"It's one thing to have all these great procedures and great technology, but our most important asset is our people, and giving them the skills that they need to be successful," Dixon says. "It's the foundational aspect to everything we do."

Because providing great customer service is a key business component, bolstering the security workforce has been crucial to the improvements at the Javits Center.

### Personnel.

A personnel increase has allowed Javits to provide a more robust security force on-site during expositions and events. In the past, clients exhibiting at Javits would depend mostly on their own contract security force. Now they can work more closely

Kratos Public Safety & Security Solutions, Inc. (previously known as Henry Brothers) is an industry leader in system integration focused on communications, access control, video surveillance, and building automation. We provide a full array of services to our clients such as system design, custom installation, 24/7 technical support, and remote system monitoring.

-  Video Surveillance
-  Access Control
-  Communications
-  Maintenance & Service



**Our Government Contracts:**

**NY OGS**  
NY State Office of General Services

**GSA**  
US General Services Administration

**NCPA**  
National Cooperative Purchasing Alliance



**500 Employees in 31 Locations Nationwide**

Northeast & Transportation  
Regional Headquarters  
17-01 Pollitt Drive  
Fair Lawn, NJ 07410  
(201) 794-6500

[www.kratospss.com](http://www.kratospss.com)

with the increased staff provided by the center.

“There are 25 other companies that are approved to provide



Courtesy Javits Center

security services in the Javits Center, and we, for all intents and purposes, would be the 26th—but we’re here every day,” Dixon says. “We know all the players; we know all of the vendors, contractors, and business partners that are here on a regular basis.”

The safety team, a proprietary force, went from about 45 members to 80 in the last two years. Many of these full-time employees, called public safety officers, come from law enforcement, loss prevention, or corporate security backgrounds, Dixon explains.

The philosophy at Javits, he says, is to provide employees with the tools they need to be successful. “When it comes to training, we take it very seriously,” he says, noting that each safety team member receives 40 hours of hostile surveillance training from

Israeli firm AS Solution. They also learn verbal de-escalation methods and undergo active shooter training.

Javits has even changed the appearance of the guard staff to create a more hospitable environment. “We’ve moved from uniformed supervisors and managers to suits and ties,” Dixon notes.

“In a lot of ways, we’ve increased the credibility of our team by taking steps like that.”

Rather than large radios that hang off their uniforms and are loud enough for anyone nearby to hear, guards now sport a covert two-way radio earpiece.

Lost and found. With tens of thousands of people moving through its doors monthly, many who come to the Javits Center accidentally leave belongings behind or misplace them.

In 2015, the safety team implemented a new software tool to manage the wealth of lost and found items that are turned in—since then, the center has experienced a 28 percent increase in lost and found items reported.

“We follow New York state guidelines for lost property, and we have a chain of custody for every item,” says Dixon, explaining all lost items are logged into a database and put in tamper-proof evidence bags. Security has reunited owners with everything from misplaced iPads to wallets full of cash.

He adds that people are more likely to report that they have found a lost item when they feel deterred by their environment from stealing it. “There’s an interesting relationship between a good security posture within a facility...and a spike in lost and found,” Dixon says.

Not only are more items being turned in, but Javits has raised the level of lost items returned by 40 percent in the same time period. Because exhibitors and



Courtesy Javits Center

clients often come from other countries, security will ship items overseas to make sure they are returned to their rightful owners. “We’ve even returned

Continued on page 25



## THIS CENTURY'S TURNSTILES



**BOOTH  
#506**

Aeroturn designs, manufactures, tests, delivers and installs the **world's only Zero-Maintenance standard and custom turnstiles**. The highest profile end-users in the world agree with our approach and keep requesting Aeroturn to upgrade their facilities.

### WHY CHOOSE AEROTURN:

- Top Tier In-House Engineering Team
- 100% Secure & Reliable Turnstile Solutions
- 100% made in USA Turnstiles
- 10 Million Passages Guaranteed
- 5-year Zero-Maintenance Warranty
- Factory Direct Delivery & Installation
- 20-Year Minimum Expected Service Life
- On-site Training & Demonstrations Available

Visit **booth #506** to see live demonstrations of our unique turnstiles and see first-hand why our turnstiles are the only choice for perimeter protection.

Contact us at **203-262-8309** or **203-513-1124**, or visit **www.aeroturn.com** to learn more about our unique security solutions and schedule an on-site demonstration.

Represented Exclusively by:



Phone: 646-278-4588  
Email: sales@thinkreps.com



a cell phone to Sydney, Australia," Dixon says. "We will do everything within our means to get it back to that person."

Dixon says an act as simple as reuniting a client with a lost item speaks volumes to the customer service provided by Javits. "It really means a lot to us," he notes. "We take great pride in it, and we've actually become really good at reuniting lost property with its owner."

Dixon has even personally delivered items to their owners, including an expensive tennis bracelet left at a jewelry exhibition. "The next day we were able to return the jewelry to the owner in New York's Diamond District. He was thrilled," Dixon says.

More improvements are on the horizon for the Javits Center. In early 2016, New York Governor Andrew Cuomo announced a \$1 billion expansion for the facility, which will add 1.2 million square feet of additional space.

A major addition will be a new four-level truck garage to accommodate deliveries for events. This will reduce the need for tractor-trailers to circle around the city block again and again until a loading dock is available—they will be able to move in and out in a timelier manner.

"This expansion project will... really propel the convention center into the top tier of

convention centers nationwide," says Tony Sclafani, senior vice president and chief communications officer at the Javits Center. "With the new spaces such as new ballrooms, new

security upgrade really is an extension of the renovation and changes—it wasn't done in a vacuum."

As Javits anticipates even more improvements, the reinvented



Courtesy Javits Center

meeting rooms, and a rooftop event space, we believe that we will attract many major trade shows and conventions that normally would not consider New York."

Dixon adds that a huge proponent of the safety improvements was Javits Center CEO and President Alan Steel. "Through the board of directors, our CEO was able to obtain the necessary funding to help push all of this through," Dixon says. "He's been extremely supportive."

Sclafani adds that security will only be further strengthened as Javits continues to serve its customer community. "It's important to note that this

approach to security has paid off in measurable ways. In the last two years, the center saw an 86 percent decrease in overnight theft, and a 74 percent decrease in total theft on a year-to-year basis.

"There are a lot of risks that are associated with being the busiest convention center in the country, and with being located in midtown Manhattan," Dixon says. "We've tried to harden the Javits Center—to become more proactive and to do certain things that we think would deter anyone wishing to do us harm."

© 2017 ASIS International,  
1625 Prince Street, Alexandria, VA 22314  
Reprinted by permission from the August  
issue of Security Management magazine.



# Protecting NYC Houses of Worship: A National Model

By Vincent J. Bove, CPP

Although houses of worship in New York City and throughout America must have a welcoming and serene environment, this must always be balanced with sound security measures.

It is a different world and not making efforts to enhance security in houses of worship is naïve, irresponsible and irrational.

Our houses of worship are sacred places of prayer where we exercise our constitutional and human right to pray.

But we must be realistic, blending the spiritual with the practical, and do everything possible to protect our houses of worship.

All who seek solace, peace, and community within the hallowed halls of our houses of worship deserve our leadership, vigilance, and commitment to protect them.

## Houses of Worship: Security Practices

A U.S. Department of Homeland Security document titled "Houses of Worship Security Practices Guide" released in May 2013, deserves attention.

The document notes that there are approximately 345,000 religious congregations in America. These consist of about 150 million members from more than 230 denominational groups.

The guide stresses that the first step to developing a comprehensive plan for a religious facility is to identify threats and vulnerabilities.

According to the guide, the threats include natural hazards, accidents, targeted violence, improvised explosive devices (IEDs), vehicle-borne explosive devices (VBIEDs),



arson, chemical or biological attacks, assassination and kidnapping.

The guide continues with the importance of having a threat assessment team comprised with a combination of facility personnel, members involved with services, mental health professionals, and emergency responders.

This document is outstanding and should be a resource for training staff and enhancing security measures.

The guide also includes details on prevention, protection, mitigation, preparedness, and recovery.

## Recommended Best Practices: ASIS International

The collaboration of our houses of worship, law enforcement, and private security should include learning and implementing "Recommended Best Practices for Securing Houses of Worship" by ASIS International. Important tips include the following:

- Report suspicious packages to police and do not touch any suspicious package. Develop a suspicious package protocol with instructions on reporting to police as well as not touching or moving the item. Address this issue in emergency evacuation procedures.

- Request local law enforcement presence during high volume worship times and holiday celebrations.

- Include law enforcement in your security planning process.

- Consider hiring off-duty police officers as part of your security program.

Simply stated, a word to the wise urging vigilance: "To be forewarned is to be forearmed."

## Security Countermeasures: Some Additional Tips

A robust security program must be comprehensive, proactive, and continually updated. Security must never be piecemeal, negligent, or have its importance minimized.

Approaches to security in houses of worship, as well as in workplaces,

Continued on page 29

## One source, one contact for full spectrum security



### On-site Guarding

- Site & Industry-Specific Training
- Customized Site-Specific Tasks



### Remote Guarding

- Alarm Verification
- Employee Escorts
- Entry/Exit Management
- Patrol & Perimeter Protection
- Remote Patrol



### Mobile Guarding

- Mobile Patrol Tours
- Alarm Response
- Mobile Officer
- Tour Confirmation



### Electronic Security

- Consultation, Design and Installation
- Video Surveillance
- Service and Maintenance



### Fire & Safety

- Incident Response
- Fire and Life Safety Consulting



### Corporate Risk Management

- Investigations
- Crisis Management/Emergency Response
- Information & Intelligence Services
- Brand Protection & Intellectual Property

The Leader In Protective Services

[www.securitasinc.com](http://www.securitasinc.com) | 877.281.5543 | 1412 Broadway, New York, NY, 10018



## Trust Detex to help keep your guard up.



### After all, we've been doing it since 1923.

It all began right here in New York, with our legendary Newman and Guardsman mechanical watchman's clocks.

It continues today, with our GCS ProxiPen RFID-based guard tour system, which makes it so easy for officers to obtain accurate checkpoint readings that it has become an industry standard. It runs on one "AA" battery that you can change yourself; and it comes in a competitively-priced kit that provides everything necessary to quickly and easily set up your system.

Our Reliant PLUS is a rugged, dependable iButton® based system that offers premium performance at a value price point.



So if you want to be sure to keep your guard up, why not trust the company that's been there and done that since way back when it all started?

Always has been... always will be... *the best.*



800-729-3839 • 830-629-2900  
marketing@detex.com • www.detex.com

In New York: Central Time Clock  
(718) 784-4900 • www.centraletimeclock.com

In New Jersey: Force One Security  
(732) 921-7346 • www.forceoneusa.com

Visit us at Booth #501

Meeting New York's security needs since 1923

schools, campuses, and facilities, must include the following:

#### Security Vulnerability Assessments:

These are best when conducted by board-certified, reputable, and experienced public safety professionals in order to identify and evaluate areas of risk. The board certification of Certified Protection Professional (CPP) by ASIS International is a statement of professionalism, competence, and credibility.

#### Background Checks/Investigations:

This is an essential due diligence countermeasure that prevents hiring individuals who do not deserve employment or access. These checks must be made by qualified, licensed professionals who honor laws conducting background checks.

Background checks can include criminal history reports, drug testing, motor vehicle driving records, credit checks, liens and judgments, sexual offender registries, employment, and professional credential verifications. Investigations that are conducted by experienced, conscientious, and ethical professionals are critical to protecting public and private enterprises.

#### Training:

A critical component of security and safety is ongoing training that includes personal safety, substance abuse awareness, domestic violence, diversity, conflict resolution, ethics, situational awareness, Internet security, workplace violence, fire prevention, crisis management, emergency preparedness, loss prevention, economic crime, crime prevention, drills, evacuations,

sexual harassment, and awareness of warning signs and red flags.

#### Warning Signs:

Warning signs are critical to violence prevention. We must recognize warning signs and provide the necessary intervention, training, health care, and security measures necessary to prevent tragedies.

#### Physical Security:

This involves countermeasures preventing unauthorized access. Countermeasures include fencing, bollards, barrier arms, card access systems, ID cards, lighting, crime



prevention through environmental design (CPTED), defense in depth programs, locks, alarms, fire extinguishers, Automated External Defibrillators (AEDs), mass communication systems, and metal detectors.

#### Personnel Security:

Certified, well-trained, and licensed security officer programs involving reputable contract or in-house professionals with either armed or unarmed personnel are recommended. It is essential that training exceed the status quo criteria and is on-going. Training must also be motivational and customized according to the needs of the sites being served.

#### Procedural Security:

Drills deserve planning and evaluation with table-top exercises.

It is also essential to conduct partial and full-scale drills based on numerous possible scenarios. These must be complemented by the expertise and involvement of law enforcement, private security professionals, and first-responders.

Essential to training and drills is the Active Shooter program detailed on the FBI website titled RUN, HIDE, FIGHT.

#### Informational/Cybersecurity:

In this age of instantaneous global data at the fingertips of individuals anywhere, some with nefarious intentions, protecting information is vital to security.

Informational security must be effective and continually updated with ongoing training for personnel that empowers them with preventive techniques. This protects companies from breaches of information through the Internet, Ransomware, dumpster diving, and social engineering and can prevent unnecessary turmoil to companies, agencies, and employees.

#### Final Reflections

Safeguarding New York City's houses of worship demands our leadership, vigilance, and collaboration.

These are challenging times but we must rise to the occasion to secure our city. The principles of security implemented here can serve as a national model for houses of worship nationwide.

The houses of worship in New York City and throughout the nation deserve our dedication, and the time to begin is now.

*Vincent J. Bove, CPP, is a national speaker and author on issues critical to America.*



# PROTECTING THE MOST VALUABLE PROPERTY IN NEW YORK CITY...



Our security and support offerings provide unlimited possibilities for your property protection and service needs.

Integrated Systems & Technology • Remote Video Monitoring • Real Time Tracking & Reporting  
Fire Life Safety Training & Consulting • Autonomous Data Machines • Manned Guarding

866.825.5433 | [www.aus.com](http://www.aus.com)



## Managing Security Projects: Don'ts, Don't You Ever, and of course, Do's

By George W. Anderson

As a security director today, the breadth of responsibility that must be undertaken seems to increase every day. We need to stay current on trends in the threat environment, our budgets shrink with regularity, and technology marches on. But one thing remains the same, and that is the need to run projects effectively and efficiently in order to keep your security program alive and well.

Over the years, I've found that there is an art and a science to effective project management. I know there are whole certification programs on professional project management, and with all due deference to my colleagues who possess such certifications, I am going to take a stab in this column by sharing my own personal 10 steps to effective project management. I hope some of my own experiences,

successes and failures, can help inform the reader, if nothing else, about what I think is key to successfully managing projects large and small.

In retrospect, the title of this article may be a little misleading. In my time managing projects, and being on many teams delivering projects, it sometimes seemed like we were getting things out of order, hence the Ready! Fire! Aim! sequence. That is the major Don't of this tome—don't let yourself pull the trigger before you know where the bullet is going. But I hope you will find that this article is actually more about what to do rather than what not to do.

### **1. Begin with the end in mind.**

As leaders or managers, we must have a clear vision of where we

want a project to take us. If you don't, one of the first steps in successfully managing a project is to develop one. This can be a collaborative effort with the project team, or one which you develop yourself, but do have one. If you are upgrading your CCTV system, that is not, in my mind, the actual goal. WHY are you upgrading the system? What are you trying to achieve? Better resolution? More up time? Your team can find a better path if they fully understand what the project is trying to achieve.

### **2. Ensure you have all of the hearts and minds of the stakeholders.**

Projects succeed or fail for a lot of reasons. Be sure you have thought of all the stakeholders who will be

clients of the project and have taken into consideration their needs when designing the project and what the end state will be. Stakeholders come from all walks of life; and they include your boss(es), other departments in your organization, true clients if the project is undertaken to benefit people to whom you are providing a service. Be exhaustive in seeking the input of as many as possible who will be touched by your efforts. But at the end of the day, remember step 1! Take all that input and boil it down to what YOU want the project to achieve.

### **3. Take Note! Or, more properly, take notes!**

Projects need to be well-documented. Develop a project management matrix. At meetings, ensure you have a scribe, or do it yourself. Record discussion points, major decisions, assignments and due dates. Publish those notes to all participants in the meeting and to those not at the meeting who need to know what has been decided and how the project is developing.

### **4. Guide well but don't be the smartest gal (or guy) in the room.**

Projects serve several purposes. They achieve a worthy goal (hopefully) by implementing your vision developed in step 1, but they also serve as a learning and proving ground for the project participants. Allow your team to chew on problems. Depending on the maturity of the team and its members, laying out every step, in detail, stifles creativity and can also result in better solutions being ignored. Engage your team

in problem-solving and let them suggest solutions. Know when to step in to assert your will, but if the team's solution will achieve the desired result, even if not necessarily the best way, I find it is helpful to allow the team the success of developing the solution.

### **5. Waste time! Have a meeting!**

Yes, there is no shortage of funny memes about this topic, so I'll keep this brief. My personal secret to effective meetings is to have them when needed. And in a project, they are needed on a regular schedule to keep things moving. Use the notes you develop in step 3 as the agenda. Keep the meeting focused on the team reporting progress. If detailed discussions on pieces of the project are needed, I usually suggest to the team members involved to take the detailed discussion off line and develop their solution, as to not waste the time of the team members not involved in that problem at a progress meeting. And again, produce updated notes from every meeting and ensure you are noting timelines.

### **6. Be prepared for delays and set-backs.**

Depending on your boss's temperament, you need to think about when a project can be realistically accomplished, and then add a little time. Under promise and over deliver is usually the best course of action. Why was Scotty the Engineer from Star Trek such a miracle worker? Because he doubled all his damage repair estimates! When exogenous factors delay projects, be sure to document what things outside

your control are impacting on goal achievement but don't whine about it. Own it and try to keep things moving, nonetheless. Move to an aspect of the project that you can move forward, if possible.

### **7. Have a timeline and track to it.**

Fundamental to steps 1, 3 and 5 is developing a project timeline and keep to it as much as possible (see step 6). Know when your vision needs to be achieved (the project delivery date), work backward from that date determining the phases of the project and how long they will take. When you've finished, evaluate your original due date for whether it is still a reasonable goal and adjust if needed.

### **8. Identify strong performers and nurture them.**

During the project's execution, you will interact with the team. One of the important goals as an effective leader is to always look out for talented people and help them strengthen their skills. Use the project to do both. And, of course, don't overlook the opportunity to coach everyone.

### **9. Be sure to engage in all the phases of a project:**

- Enthusiasm
- Disillusion and Disenchantment
- Panic
- Search for the Guilty
- Punishment of the Innocent
- Praise and Honors for the Non-Participants

One of the great leaders in my past had this sign over his desk, so I couldn't resist adding it to my list.

Continued on page 72



## CONFERENCE PROGRAM



**May 16-17 2018**  
**Jacob Javits Center**

**GSX**  
GLOBAL SECURITY EXCHANGE

POWERED BY **ASIS**  
INTERNATIONAL

**SEPTEMBER 23-27 | 2018**  
LAS VEGAS | NEVADA

# Strategies for Security **MULTIPLIED.**

Security professionals need a trusted network to stay at the forefront of today's rapidly evolving threat landscape. The ASIS International Global Security Exchange (GSX), formerly the Annual Seminar and Exhibits, builds off more than six decades of event distinction by uniting the full spectrum of security—allied partners, service and solution providers, and security professionals across all industry sectors—for one powerful global event.

From AI and AR to active shooter and asset protection, GSX will deliver the latest technologies and innovations in both physical and cyber security, as well as the expert-led education and world class networking you expect from the security industry's flagship event. The world of security is moving quickly. Multiply your efforts to stay ahead of it.

**REGISTER TODAY >> [GSX.org](http://GSX.org)**

**#GSX18**

### **Wednesday, May 16**

**8:00 am–9:00 am**

**Keynote: Emerging Trends**  
**Speaker: Scott Morrison**

Managing Director, Head of Global Crisis Management/Command Centers and North America Security JPMorgan Chase & Co.

Scott Morrison will be discussing current and emerging risks and threats abroad—from terrorism attacks to kidnappings and cyber security to intellectual theft. His keynote will explore what we can do to protect our organizations, assets and people, while working alongside our partners in law enforcement, intelligence, First Response, Emergency Management and private sector security. Scott will give a high-level overview of

emergent threats from a strategic to tactical level; the associated challenges or opportunities; and the so what in terms of mitigating these threats.

**9:00 am to 4:00 pm**  
**Exhibit Hall Opens**

**9:00 am to 10:00 am**  
**Continental Breakfast – Exhibit Hall**

**9:30 am to 10:30 am**  
**Session 102: Aerial View of Drone Technology from All Angles**

This panel discussion will provide opinion and open discussion on a number of issues and items regarding drones and drone technology.

**Panelists will include:**

- Law enforcement
- Private and public sector Security professionals

- A company that provides drone prevention technology
- A company that provides drones used for security

The existing threats will be discussed, along with avenues to mitigate those threats with the use of technology and existing law.

**Panel Discussion:**

**Bobby Long, VP of Sales, Dedrone**

**John Daniels, Chief Strategy Officer, Aptonomy**  
**Scott Morrison, Managing Director, Head of Global Crisis Management/Command Centers and North America Security, JPMorgan Chase & Co.**

**Special Agent Janet Ambrisco, Federal Bureau of Investigation - Joint Terrorism Task Force, JFK Airport**

**Detective Shawn Russell, Port Authority Police Department – FBI Joint Terrorism Task Force, JFK Airport**

**11:00 am–12:00 pm**

**Session 103: Get a Seat at the Table: Implementing ESRM**

Security’s role is a strategic function, involving budgeting and managing security assets as well as prioritizing, communicating, and reporting tactics. These security responsibilities should be aligned with an organization’s strategy. Enterprise security risk management (ESRM) means strategic security decisions are made by the right person, with the right authority and accountability, and for the right reasons based on defined risk principles. Through the lens of ESRM, security gains a “seat at the table” and becomes a roadmap for meaningful effective enterprise risk management. Join an interactive discussion on the value of ESRM and the evolving role of security strategy.

**Speaker:**

**Brian Allen, CPP, Principal, Security Risk Governance Group, has more than 20 years of strategic experience in the security field, most recently as the former chief security officer for a major critical infrastructure company. He is an expert in the field of enterprise security risk management (ESRM), has authored two books and numerous articles on ESRM, and has spoken globally on the topic.**

**12:00 pm to 2:00 pm**

**Exhibits and Lunch on Your Own**

**2:00 pm to 3:00 pm**

**Session 104: Securing an Open Office Environment**

Learn how Facebook developed its global security program based on the company’s values. The result has enabled Facebook to secure an open and collaborative office environment while mitigating risk through an intelligence-based layered approach. The over-arching goal has been to protect the company’s vast global infrastructure, people, and brand.

**Speaker:**

**Speaker: Nick Lovrien, Chief Global Security Officer, Facebook, is responsible for the overall leadership of Facebook’s Global Security Organization. His team is committed to enabling the business while protecting the people, assets, and reputation of Facebook's family of apps and services, including Instagram, Messenger, WhatsApp, Oculus, and Workplace**

**4:00 pm**

**Exhibit Hall Closes**

**Thursday, May 17**

**8:00 am to 9:00 am**

**Session 201: Active Threats and the Security Culture**

Participate in an in-depth discussion of today’s security culture at various organizations. Explore the difference between an organization that values security spending versus those that look at the security department as an expense worth reducing.

**Speaker:**

**Mike Biller, President and COO, Tomahawk Strategic Solutions, recently retired as a Navy SEAL with the Naval Special Warfare Development Group. After ten deployments across the world, Biller was medically retired. Currently, he prepares corporate leaders to provide safer and more secure environments for their employees and communities.**

**9:00 am to 3:00 pm**

**Exhibit Hall Opens**

**9:00 am to 10:00 am**

**Continental Breakfast in the Exhibit Hall**

**9:15 am to 10:15 am**

**Session 202: Vehicle-involved Active Assailant Attacks: Strategies for Safety and Survival**

From 2014 through 2017, 23 terrorist vehicle ramming attacks were reported, resulting in 204 deaths and 861 injuries in the U.S. and abroad. Such attacks have become the tactic-of-choice for homegrown violent extremists because they provide a low-cost, low-tech weapon of mass destruction. The Transportation Security Administration has warned that, “No community, large or small, rural or urban, is immune to attacks of this kind by organized or “lone wolf” terrorists.”

In their efforts to assist clients and communities, security professionals must know how to define this form of violence and how best to detect and deter would-be attackers.

**Speaker:**

**Steven Crimando, Principal, Behavioral Science Applications, leads a training and consulting firm specializing in violence prevention and intervention. With nearly three decades of front-line crisis response experience, Crimando worked on the 1993 and 2011 World Trade Center attacks, participated in New Jersey’s Anthrax Screening Center, and has been involved with other major disasters and acts of international terrorism. He serves as a consultant and instructor for multinational corporations, government agencies, major city police departments, and military programs. He has also served as an expert to the media and the courts on crisis prevention and intervention**

**11:30 am to 12:00 pm**

**Pre-Luncheon Networking (Hosted Bar)**

**12:00 pm to 2:00 pm**

**Person of the Year Luncheon Honoring His Eminence Timothy Cardinal Dolan \$75 per person**

**3:00 pm**

**Exhibit Hall Closes**

## A

**A+ Technology & Security Solutions, Inc**  
**Booth: 412**

1490 North Clinton Avenue  
Bay Shore, NY 11706  
+1.631.675.2237  
www.aplustechnology.com

**Access Systems Integration**  
**Booth: 404**

+1.347.675.7363  
www.AccessSI.com

Access Systems Integration (Access SI) is a full-service electronic security organization providing best-in-class fully integrated security system technologies and support - protecting our clients' most valuable resources and assets, minimizing risk exposure and safeguarding proprietary data and information.

Our company is led by veterans of the security industry with decades of collective experience and an unmatched knowledge of today's state-of-the-art security systems integration solutions that deliver a meaningful difference for Access SI clients.

**Aeroturn, LLC**  
**Booth: 506**

15 Hurley Road, Suite 2C  
Oxford, CT 06478-1047  
+1.203.262.8309  
www.aeroturn.com

100% Made in USA Oxford, CT location, Aeroturn has been offering integrators and end users this century's turnstiles that include a comprehensive range of turnstile products. With an engineering team that is second to none; the team has been together for over two and a half decades in the product design, development and manufacturing field and continues to lead the way in the security industry. Since its inception in 2001, Aeroturn offers every customer a 5-year warranty, zero maintenance mechanisms, 10 million passages guaranteed, site specific cabinets, 10,000 cycle factory burn-in, and industry unique-factory direct delivery & installation.

**Aiphone Corporation**  
**Booth: 115**

+1.425.455.0570 x 8109  
www.aiphone.com

For over 60 years, Aiphone has solidified its position as one of the world's leading providers of communication and intercom systems. The Aiphone brand has become synonymous with innovation and outstanding quality which has placed the company and its products at the forefront of the security and communication market. Aiphone remains committed to providing unmatched customer service by offering customized solutions tailored to support any intercom application.

**Allied Universal Security Services**  
**Booth: 405**

330 W 34th Street, 18th floor  
New York, NY 10001-2406  
+1.212.328.0209  
www.AUS.com

**Alpha Technologies**  
**Booth: 419**

3767 Alpha Way  
Bellingham, WA 98226  
+1.360.647.2360  
www.alpha.com

Alpha Technologies provides power solutions for security, traffic monitoring, communications and data networks worldwide, earning a reputation for reliability and performance. With the launch of our next-generation AlphaGateway product line, our new solution provides critical network power, high capacity backhaul, and the necessary installation real estate to provide power-over-Ethernet to devices such as Wi-Fi radios and surveillance cameras. Each AlphaGateway model allows for flexible, strategic placement of interactive devices in virtually any environment. In addition to AlphaGateway, Alpha's full line of power products includes standby, non-standby and uninterruptible power supplies, surge suppressors, enclosures, batteries and powering accessories.

**Altronix Corporation**  
**Booth: 318**

140 58th Street, Bldg A-3W  
Brooklyn, NY 11220-2521  
+1.718.567.8181  
www.altronix.com

A global leader in power and data transmission, Altronix designs and manufactures innovative solutions that maximize overall performance and efficiency. Our power products and peripherals, feature the quality, reliability and unparalleled customer support that have been associated with Altronix for over 30 years. Made in the U.S.A – Lifetime warranty

**Ameristar Perimeter Security**  
**Booth: 410**

+1.918.835.0898  
www.ameristarfence.com/en/site/  
ameristarfence.com/

Ameristar Perimeter Security manufactures an array of perimeter security products, including vehicle barriers, bollards, gates, and security fencing. Ameristar's fence systems provide security, strength, and protection while combining an open aesthetic appearance for the highest level of perimeter control. Ameristar can be a single source solution for a physical security project. Company personnel will assist in selecting the product most appropriate for a specific application.

**ASIS International**  
**Booth: 334**

1625 Prince Street  
Alexandria, VA 22314  
+1.703.519.6200  
www.asisonline.org

ASIS International is the world's largest membership association for security professionals. With more than 235 chapters globally, ASIS is the premier source for security learning, networking, standards and research. Through board certifications, award-winning Security Management magazine, and Annual Seminar and Exhibits—the profession's most anticipated event—ASIS provides the security community with the intelligence to protect their people, property, and information assets.

**ASIS Career Center**  
**Booth: 235**

1625 Prince Street Alexandria, VA 22314  
+1.703.519.6200  
Always a popular destination, the Career Center offers free resume reviews and career coaching.

**ASIS Councils**  
**Booth: 335**

1625 Prince Street Alexandria, VA 22314  
+1.703.519.6200  
www.asisonline.org/get-involved/councils

Have a question about one of our ASIS councils, or want to learn more about volunteer opportunities? Stop by to talk to one of our volunteer council members.

**ASSA ABLOY Americas**  
**Booth: 406**

100 Sargent Dr  
New Haven, CT 06511-5918  
+1.203.909.1008  
www.assaabloy.com

ASSA ABLOY Door Security Solutions combines the expertise of the industry's most knowledgeable door opening professionals with the comprehensive product offering of leading door and hardware brands to provide complete solutions to partners and end-users in commercial, retail, multi-family, government and institutional facilities. Coupling innovative technologies with insight on specifications, design, support, training and code compliance, ASSA ABLOY Door Security Solutions works closely with the architectural, security, facilities and integrator communities to address the many challenges they encounter serving and securing their customers. Visit [www.assaabloydss.com](http://www.assaabloydss.com).

**Avigilon Corporation**  
**Booth 507**

4001 East Plano Pkwy  
Plano, TX 75074  
+1.888.281.5182  
www.avigilon.com

**Axis Communications**  
**Booth: 309**

300 Apollo Drive  
Chelmsford, MA 01824-3629  
+1.978.614.2000 x3017  
www.axis.com

Axis offers intelligent security solutions that enable a smarter, safer world. As a global leader in network video, Axis is continually launching innovative network products based on an open platform and delivering high value to customers through a global partner network. Axis has long-term relationships with partners and provides them with knowledge and ground-

breaking network products in existing and new markets.

## B

**BEST Access Solutions, Inc.**

**Booth: 330**  
+1.856.404.0024  
www.bestaccess.com

America's favorite hardware brands, BEST, PRECISION, & STANLEY have represented tough, versatile, high-quality door hardware for more than 90 years.

**Building Intelligence Inc.**  
**Booth: 430**

50 Main Street, 10th floor  
White Plains, NY 10606  
877.353.3377  
www.buildingintelligence.com

## C

**Comtrend**

**Booth: 119**  
+1.949.608.2214  
www.us.comtrend.com

Comtrend, with more than 25 years of experience, has become one of the leading global providers of advanced networking solutions. Comtrend designs, manufactures, and markets a range of networking equipment and software. The company is known for its innovative technologies such as the G.hn Powerline Adapter with PoE that makes IP camera installation fast and easy.

## D

**Dahua Technology USA Inc.**

**Booth: 218**  
23 Hubble  
Irvine, CA 92618-4209  
+1.949.679.0930  
www.dahuasecurity.com/en/us/

**Databuoy Corporation**  
**Booth: 505**

+1.703.865.8220  
www.databuoy.us

Databuoy has developed a proprietary gunfire localization system called ShotPoint. The platform senses gunfire, accurately locates the source, and transmits shooter location alerts to systems that can cue cameras, inform responders, and warn the

public. ShotPoint saves lives and reduces damage by providing responders with the critical information required to accelerate tactical response, neutralize threats, and deploy emergency medical services.

**DETEX Corporation**  
**Booth: 501**

302 Detex Drive  
New Braunfels, TX 78130-3045  
+1.800.729.3839 x 4372  
www.detex.com

Detex Corporation manufactures life safety and security door hardware. The ECL-230X-TBD-DX3 is a code compliant six-point lock, which has been tested to withstand 16,000 pounds of force. Detex also offers delayed egress and weatherized exit hardware as well as door alarms, optical turnstiles, and tailgate detection equipment. Used as stand-alone units or configured into a system, Detex products can offer life safety and security for doors, gates, and other access points.

**E-LINE by DIRAK**  
**Booth: 423**

22560 Glenn Drive, Suite 105  
Sterling, VA 20164-4440  
+1.703.955.3220  
www.elinebydirak.us

After decades of leading the mechanical hardware industry with innovative designs for racks and enclosures, DIRAK integrated electromechanical, network, and software components to create the premier security solution, E-LINE by DIRAK. Increasing security, mitigating risk, and ensuring compliance exemplify E-LINE by DIRAK's mission of manufacturing the best access control solutions for racks and enclosures. Now, with more than fifteen years of experience in physical security, we are continuously evolving based on the changing demands of each industry we serve –enabling our customers to stay ahead of new risks and the increasing costs associated with data and physical theft.

## F

**F.M. Valenti, Inc.**  
**Booth: 319**

5 Bourbon Street  
Peabody, MA 01960-1339  
+1.973.570.8717  
www.fmvalenti.com

## FAST-PASS VISITOR MANAGEMENT

**Booth: 215**  
3595 Fiscal Court  
West Palm Bch, FL 33404-1782  
+1.561.691.0050  
www.siscocorp.com

FAST-PASS Visitor Management by SISCO has been putting security solutions first since 1984. An industry leader in electronic and identity management. The company is introducing the next generation in technologies. FAST-PASS and APASS. The solutions can cross check against internal and external watch lists, are easy to use, and complete the process in seconds without hindrance to the flow of commerce. FAST-PASS solutions are the choice for healthcare, education, commercial buildings, government and law enforcement for those seeking a customizable solution as a frontline deterrent, eliminating the opportunity for undesirable to act on their intentions.

## FST Biometrics

**Booth: 508**  
+1.972.374.68374

FST Biometrics' IMID software utilizes a fusion of visual identification technologies, including facial recognition and behavior analytics, to provide accurate non-intrusive and seamless identification. IMID simultaneously identifies multiple authorized individuals from a distance and in-motion. There is no slowing down or stopping for the users, as our system recognizes those authorized for entry quickly and efficiently, providing identification at the speed of life.

## G

### GardaWorld

**Booth: 131**  
Dubai 482069  
United Arab Emirates  
+971 (0) 453 8500  
www.garda.com

Business solutions and security services for a complex world GardaWorld is the world's largest security company, offering secure transportation and cash vault services, physical and specialized security solutions, and via the Crisis24 portal, real-time, vetted international security alerts. GardaWorld is a partner of choice for private companies, governments, humanitarian organizations, and multinational corporations with

employees around the world. GardaWorld employs more than 62,000 dedicated and highly qualified professionals who serve a diverse clientele in North America, Africa, Asia, and the Middle East.

### Gentec

**Booth: 415**  
2280 Alfred-Nobel Blvd, Suite 400  
Montreal, QC H4S 2A4  
Canada  
1+514.332.4000www.genetec.com

Genetec, Inc. is a technology company with a broad solutions portfolio that encompasses security, intelligence, and operations. The company's flagship product, Security Center, is an open-architecture platform that unifies IP-based video surveillance, access control, automatic license plate recognition, communications, and analytics. Genetec also develops cloud-based solutions and services designed to improve security and contribute new levels of operational intelligence for governments, enterprises, transportation applications, and communities. Founded in 1997, Genetec serves its global customers through a network of resellers, integrators, certified channel partners, and consultants in more than 80 countries.

## H

### HAIX North America, Inc.

**Booth: 411**  
+1.859.281.0111  
www.haixuse.com

HAIX® is a leader in the manufacture of footwear for hardworking professionals. The company's European-made products fill the high-level requirements for quality, comfort, and design. HAIX® is committed to providing the best footwear in the market for safety, fire and rescue, and law enforcement industries.

### Hanwah Techwin

**Booth: 418**  
+1.201.325.6951  
www.hanwhasecurity.com

A leading manufacturer in the security industry, Hanwha offers video surveillance products, including IP cameras, storage devices, and management software found in world-class optical design, manufacturing, and image processing technologies. The company offers end-to-end security solutions

and has achieved global success across a range of vertical markets, including retail, transportation, education, banking, health-care, hospitality, and airports. Hanwah recently introduced the Wisenet line of security products that demonstrate the company's commitment to value and technology. Products include 12 MP cameras, intelligent video analytics, and H.265 support.

### Hikvision USA, Inc.

**Booth: 407**  
+1.909.895.0488  
www.hikvision.com

## I

### IndigoVision, Inc.

**Booth: 327**  
300 Broadacres Drive  
4th Floor, Unit 415  
Bloomfield, NJ 07003-3153  
+44.131.475.7370  
www.indigovision.com

IndigoVision has more than two decades of experience developing end-to-end security surveillance solutions. From IP cameras and network video recorders to security management software and hardware coupled with intelligence video analytics and cyber-security features, the company's products are trusted globally across multiple markets, in high-profile sites, and harsh environments. With the reliability and compatibility of a closed system, IndigoVision products use an open technology with integrated modules and ONVIF conformity so third-party systems can be added effortlessly.

### Intelligent Security Systems (ISS)

**Booth: 519**  
1480 U.S. Highway 9 North, Suite 202  
Woodbridge, NJ 07095  
+1.732.855.1111

### International SOS

**Booth: 526**  
+1.267.398.2094  
www.internationalsos.com

International SOS is a leader in medical and travel security risk services that cares for clients across the globe from more than 1,000 locations in 90 countries. The company's 11,000 employees are led by 1,400 doctors and 200 security specialists. Teams work night and day to protect members and to deliver emergency assistance during critical illnesses, accidents, or civil unrest and to

## J

### Johnson Controls Security Solutions

**Booth: 211**  
2450 Boulevard of the Generals  
Norristown, PA 19403  
+1.610.635.1407  
www.johnsoncontrols.com  
Johnson Controls Security Solutions helps companies with a need to deploy complex, enterprise-wide security solutions. By seamlessly integrating electronic security solutions into existing IT infrastructures, the company helps enterprises become safer, more secure, and more sustainable. Follow the company @JCI\_Buildings on Twitter.

### Johnson Controls Security Products

**Booth: 306**  
6 Technology Park Drive  
Westford, MA 01886-3140  
561.939.3164  
www.tycosecurityproducts.com

Johnson Controls' Building Technologies & Solutions is making the world safer, smarter and more sustainable. Our technology portfolio integrates every aspect of a building – security systems, energy management, fire suppression or HVACR – ensuring we exceed customer expectations at all times. JCI operates in more than 150 countries through our network of branches/distribution channels, helping building owners, operators, engineers and contractors enhance the lifecycle of any facility. Our arsenal of brands includes some of the most trusted names in the industry, including Tyco®, now the leading brand in the JCI security portfolio. For more information, visit www.johnsoncontrols.com or www.tycosecurityproducts.com.

## L

### Lightcast

**Booth: 526**  
PO Box 538  
Pell City, AL 35125  
+1.678.339.2326  
www.lightcastinternational.com

If you are interested in a radar video camera system. Our 6 years' experience has moved us to the forefront of this technology, its daily Research and Development to improve the solution that got us here and recently

on national TV. We have a low powered DVR/CAM + radar systems that in many cases can run with existing radar sign batteries, radar and solar panels or a small increase panels on some signs. Our show speed of vehicle and with LPR the plates in short triggered videos. These are recorded and available in real time views.

### LPC Inc.

**Booth: 229**  
7100 New Horizons Blvd.  
N. Amityville, NY 11701  
1.631.321.7600  
www.lpcny.com

## M

### Metrocom NYC

**Booth: 512**  
33 E. 33rd Street, Suite 807  
New York, NY 10016-5370  
+1.212.532.7400 x 823

Metrocom has been providing two-way radio communications equipment, systems and services in the New York area since 1979. Metrocom offers two-way radio solutions that include 24/7 emergency service. Whether you need to communicate within a building, across town or across the country, we have the right two-way radio solution that will fit your need. Metrocom also offers, pick up and delivery service as well as rental radios for any event size. Please call and arrange for a no cost demonstration of the latest products.

### Milestone Systems

**Booth: 313**  
+1.503.277.0533  
www.milestonesys.com

Founded in 1998, Milestone Systems is a leader in open platform IP video management software dedicated to delivering high-quality business video platform software with a community of hardware and software partners that can integrate video solutions for security. The company's objective is to provide the community's customers with improved organizational processes and safety levels through the management, integration, and distribution of digital video data.

### Morse Watchmans, Inc.

**Booth: 219**  
2 Morse Road  
Oxford, CT 06478-1040  
+1.203.264.4949 x537  
www.morsewatchmans.com

Morse Watchmans is a leader in high-quality, cost-effective guard tour and key control solutions. Specializing in state-of-the-art management that includes KeyWatcher Touch, KeyWatcher Illuminated, AssetWatcher (RFID lockers), TamperProof key rings, and the PowerCheck Guard Tour System. The company's products are modular, reliable, easy to use, and scalable to meet specific needs. Products are designed and manufactured in Oxford, CT.

### MSA Security

**Booth: 307**  
+1.212.509.1336  
www.msasecurity.net

MSA Security is a leader in high consequence threat protection, explosives detection, intelligence analysis, specialized training, and investigative services for corporate and government clients. The company's technology and robust security solutions protect people and property every day, delivering peace of mind, enhanced operational efficiencies, and minimized business disruption.

## N

### NAVCO

**Booth: 329**  
1041 N. PacifiCenter Drive  
Anaheim, CA 92806  
+1.714.339.3839  
+1.800.788.3779  
www.navco.com

For video, alarms, access control, and analytics, NAVCO is a value-added business partner with more than 45 years of experience installing and repairing electronic security systems nationally. NAVCO helps clients know that their business, employees, customers, and property are secure. The company's technicians fix problems with parts already on their trucks, with a 95 percent success rate. NAVCO is dedicated to enhancing the value of a business while maximizing the return on its security system investment.

**NYPD SHIELD****Booth: 228**1 Police Plaza, Room 1109  
New York, NY 10038

NYPD SHIELD addresses private sector business on both an industry-specific and a geographic basis. This enables the NYPD to best serve the unique needs of each constituency. NYPD SHIELD provides training services to assist public and private sector entities in defending against terrorism. In addition, information specific to a particular sector is transmitted directly to those affected by one of several methods:

- In-person intelligence and threat briefings conducted by Counterterrorism Bureau personnel
- NYPD Website postings
- Shield Alert e-mail messages.

NYPD SHIELD keeps our private sector partners informed of developing situations, preparations for upcoming events, and new intelligence and threat information

**O****On-Net Surveillance Systems Inc. (OnSSI)****Booth: 107**1 Blue Hill Plaza, 7th Floor  
Pearl River, NY 10965-3104  
+1.845.732.7900 x 7951  
www.OnSSI.com

On-Net Surveillance Systems, Inc. (OnSSI) was founded in 2002 with the goal of developing comprehensive and intelligent IP video surveillance management software. OnSSI's Ocularis IP security and surveillance VMS platform increases security, reduces operational costs, and helps organizations move closer to prevention. Ocularis delivers open architecture, flexibility, and scalability for a range of applications including education, gaming, government, health-care, manufacturing, public safety, transportation, and utilities.

**P****Panasonic****Booth: 420**+1.713.581.9296  
www.security.us.panasonic.com

Panasonic provides a range of integrated security and video surveillance solutions to help security officials enhance their surveil-

lance systems and maximize coverage while lowering the total cost of ownership.

**Pivot3****Booth: 518**221 W 6th Street  
Austin, TX 78701  
+1.720.245.6350

Pivot3 is the premier provider of enterprise IT infrastructure for the Security and Surveillance industry. With innovative solutions built specifically for global organizations with demanding, data-intensive video surveillance environments, Pivot3 delivers high-performance, ultra-dense, highly resilient solutions that reduce risk, eliminate downtime and data loss, and simplify scale and management. Our broad ecosystem of industry partners and our flexibility to support any camera, VMS, or security application on a single platform helps organizations keep pace with explosive data growth and integrate with the latest analytics, AI, Cloud and data security technologies. Visit [www.pivot3.com](http://www.pivot3.com) to learn more.

**R****Rave Mobile Safety****Booth: 226**50 Speen Street, Suite 301  
Framingham, MA 01701-1802  
+1.508.832.8979  
www.ravemobilesafety.com**RightCrowd Software, Inc****Booth: 231**+1.858.356.2005  
www.rightcrowd.com**Riverdale Mills Corp.****Booth: 421**130 Riverdale Street  
Northbridge, MA 01534-0200

WireWall® by Riverdale Mills is a virtually impenetrable, high security fencing material that is nearly impossible to climb or cut. Requested by security and safety experts, WireWall® lines the U.S. border with Mexico, guards the Kuwait-Iraq border and protects military bases, nuclear facilities, refineries, airports and prisons at over 1,000 sites around the world.

WireWall® is made in America by Riverdale Mills, the industry leader of engineered welded wire mesh fabrics for the security industry.

**S****Salient****Booth: 206**4616 W. Howard Lane  
Building 1, Suite 100  
Austin, TX 78728  
+1.512.617.4800  
<http://www.salientsys.com>

Salient is a leading provider of enterprise video surveillance management systems (VMS). CompleteView VMS provides scalability, a fully open architecture, ease of use, and low cost of ownership. CompleteView provides a simple path to move from analog to digital video, and the power to control security installations from a single platform. Salient delivers an innovative pricing model when deploying its video surveillance capabilities. The company's solutions can be found in numerous industries, including K-12 and higher education, retail, financial, manufacturing, healthcare, and commercial real estate

**SAM-Inc.****Booth: 426**+1.570.516.5941  
www.sam-inc.org

Service Access & Management, Inc. (SAM) is a not-for-profit human service organization serving communities throughout the United States. Many of the services which SAM provides are designed to assist companies, organizations, school districts, government and human service agencies advance their mission by offering support and expertise in a wide variety of service areas including Act of Violence Response Training (Active Shooter in the workplace and school), De-Escalation/Safety Training, Fieldworker Safety & Awareness, Drug & Alcohol Awareness, Mental Health Case Management, Crisis Intervention, Truancy Remediation, Administrative Entity Support Services as well as Fiscal, Technical & Administrative oversight, HIPPA Compliance Training and IT support services.

**Secure Worker Access Consortium****Booth: 207**23 Royal Road, Suite 204  
Flemington, NJ 08822-6001  
+1.908.782.6010  
www.secureworker.com

Unknown workers, vendors, and visitors pose a real threat to workplace security and safety. The Secure Worker Access Consortium (SWAC) is a program that delivers comprehensive personnel assurance technologies and services to risk managers or critical infrastructure, sensitive facilities, and places when the public gathers. SWAC unifies the efforts of public agencies, private corporations, labor groups, and contractors to assure that all members comply with security and safety requirements. The real-time, need-to-know sharing of certified personal data validates members' trustworthiness, eliminates widespread duplication of effort, and continually protects members' privacy rights.

**SecureWatch24****Booth: 414**One Penn Plaza, Suite 4000  
New York, NY 10119  
+1.212.729.5403  
www.sw24.com**Securitas Security Services USA, Inc.****Booth: 304**500 Bi County Boulevard, Suite 110  
Farmingdale, NY 11735  
+1.646.720.0674  
www.securitasinc.com

Securitas USA is an international company that specializes in protective services based on people, technology, and knowledge. The main service categories are on-site, mobile, and remote guarding combined with electronic security, fire and safety, and corporate risk management. Whether clients conduct business internationally or around the corner, they can count on Securitas resources.

**Securitech Group, Inc.****Booth: 205**54-60 46th Street  
Maspeth, NY 11378-1037  
+1.718.392.9000  
www.securitech.com

Established in 1983, Securitech® is an independent manufacturer of high-security door locks. Originally founded to create and produce multi-point door locks, the company quickly added automatic deadbolt locking and electric locking solutions to its catalog of products. All Securitech® product designs are driven by the needs of end users, security directors, and architects.

**Sentinel Consulting****Booth: 127**1 Penn Plaza, 36th Floor  
New York, NY 10119-9380  
+1.888.793.9380  
www.sentinelgroup.us**Siedle****Booth: 326**750 Parkway  
Broomall, PA 19008-4212  
+1.800.874.3353  
www.siedleusa.com**Sielox, LLC****Booth: 321**+1.856.861.4570  
www.sielox.com

Since 1979, Sielox has designed, engineered, and manufactured intuitive security management systems through a network of select business partners to a variety of end users. Sielox solutions include Pinnacle 10 Advanced Access Control, 1700 Intelligent Controller, Sielox AnyWare (trademark) browser-based access control, and Sielox Class (trademark) Crisis Lockdown Alert Status System for today's demanding security environments. The products integrate with Allegion wireless locks, Conekt Mobile Credentials, Farpointe readers, and other OEM security manufacturer's products.

**Singlewire Software****Booth: 113**1002 Deming Way  
Madison, WI 53717  
+1.608.661.1140  
www.singlewire.com

We are the developers of InformaCast, a leading emergency notification system. Singlewire is dedicated to helping organizations keep their personnel safe through mass notifications that can be sent to any device. Our InformaCast solutions can help

you page groups of Cisco phones, notify people of an emergency, communicate via mobile devices, automate existing systems, and more. We are dedicated to developing reliable notification solutions and personal relationships that create peace of mind. We do this by connecting people when and where it matters.

**Skopenow****Booth: 431**+1.800.252.1437  
www.skopenow.com

Skopenow uses social media and open web data to detect fraud and evaluate risk. The company offers a free 7-day trial and works with financial institutions across the world. Skopenow aims to save investigators time by automating social media investigations.

**T****TEAM Software, Inc.****Booth: 322**+1.402.952.4318  
www.teamsoftware.com

TEAM Software has been a leading provider of software solutions in the contract security industry for nearly 30 years. The company offers a host of fully integrated solutions from operations, financial, and workforce management to employee and customer self-service to time and attendance products designed to help customers profit from efficiency.

**The LTI Group****Booth: 427**14 Federico Dr  
Pittsfield, MA 01201-5518  
+1.413.637.5001  
www.ltisg.com

The LTI Group is a quality-driven manufacturer of glass-clad and laminated polycarbonates for secure structures that include bullet resistant glass. The company is a leading provider of laminated glass and polymer products to a variety of industries around the world, such as architecture, automotive, airline, marine, security, and industrial applications. The LTI Group offers Smartgard, a glass-clad polycarbonate and laminated polycarbonate to the corrections and detection industries.

**TOA Electronics, Inc.**

**Booth: 227**  
 +1.650.452.1200  
 www.toaelectronics.com

**Tymetal Corp**

**Booth: 328**  
 +1.800.328.4283  
 www.tymetal.com

Tymetal Corp. is the leading national manufacturer of security gates & operator systems; closing openings from 4' to 400' with thousands of installations all over the USA. Products include US DOS certified crash gates, aluminum Fortress® cantilever slide or swing gates, gate operators, pedestrian gates, vertical lift gates, box frame roller gates, and telescoping gates. Tymetal's PAS 68 tested and certified permanent and removable crash bollards, and PAS 68 tested and certified crash block solutions bring world class security, performance and aesthetics to this critical market need.

Come and experience Tymetal's:

- No cost design, engineering and specification services
- Unmatched technical support
- Best warranty in the business
- Quality Focused - Customer Driven- Performance Tested

**U**

**Unipro Uniforms**

**Booth: 208**  
 390 Nye Avenue  
 Irvington, NJ 07111  
 973.622.8100  
 www.UniproUniforms.com

UniPro International is a minority woman owned business. Established in 1997, UniPro Int'l is a privately held company that owns and operates its own mills, manufacturing, warehousing and distribution facilities. As a vertically integrated company, UniPro Int'l has a definite advantage in the managed program uniform industry, because we control the quality, workmanship and the logistics of our goods.

**U.S. Postal Inspection Service**

**Booth: 503**  
 +1.212.330.3344  
 postalinspectors.uspis.gov

As one of the oldest federal law enforcement agencies, the U.S. Postal Inspection Service is a highly specialized and professional organization, performing investigative and security functions essential to a stable and sound postal system.

**V**

**VIVOTEK USA Inc.**

**Booth: 413**  
 2050 Ringwood Avenue  
 San Jose, CA 95131  
 +1.408.773.8686  
 www.vivotek.com

Founded in early 2000, Vivotek is a global manufacturer of IP Video Surveillance Solutions. Headquartered for North America in San Jose, CA, Vivotek provides a wide range of network cameras, switches, recording and video management software, all designed to provide customers with superior value and award-winning performance. Our complete line of video surveillance solutions will meet all your security monitoring needs, from small setup inside a small business to the most demanding requirements inside a large corporation.

Exhibitor	Booth	Exhibitor	Booth
A+ Technology & Security Solutions, Inc	412	Lightcast	520
Access Systems Integration	404	LPC Inc.	229
Aeroturn, LLC	506	Metrocom NYC	512
Aiphone Corporation	115	Milestone Systems	313
AlliedUniversal Security Services	405	Morse Watchmans Inc	219
Alpha Technologie	419	MSA Security	307
Altronix Corporation	318	NAVCO	329
Ameristar Perimeter Security	410	NYPD Shield	228
ASIS International	334	On-Net Surveillance Systems Inc. (OnSS)	107
ASIS Career Center	235	Panasonic	420
ASIS Councils	335	Pivot3	518
ASIS NYC Chapter	340	Rave Mobile Safety	226
ASSA ABLOY Americas	406	RightCrowd Software, Inc	231
Avigilon Corporation	507	Riverdale Mills Corporation	421
Axis Communications	309	Salient	206
Best Access Solutions	330	SAM	426
Building Intelligence, Inc.	430	Secure Worker Access Consortium	207
Comtrend	119	SecureWatch 24	414
Dahua Technology USA Inc.	218	Securitas Security Services USA, Inc.	304
Databuoy Corporation	505	Securitech Group, Inc.	205
Detex Corporation	501	Sentinel Consulting	127
E-Line by DIRAK.	423	SIEDLE	326
F.M. Valenti, Inc.	319	Sielox, LLC	321
Fast-Pass Visitor Management	215	Singlewire Software	113
GardaWorld	131	Skopenow	431
Genetec	415	TEAM Software, Inc	322
HAIX North America, Inc.	411	The LTI Group	427
Hanwah Techwin	418	TOA Electronics, Inc.	227
Hikvision USA, Inc	407	Tymetal Corp	328
IndigoVision, Inc.	327	Unipro Uniform	208
Intelligent Security Systems (ISS)	519	U.S. Postal Inspection Service	503
International SOS	526	Vivotek USA Inc.	413
IronYun	311		
Johnson Controls Security Solutions	211		

*List as of April 18, 2018*

# Announcing ASIS New York Chapter SECURITY EXPO: MAY 9, 2019

## You told us what you wanted and we listened.

We're returning to our traditional format of a one-day show. 8 AM to 5 PM.  
 We'll still have our Person of the Year luncheon and a cocktail and raffle reception after 5 PM.  
**For more information: call Ray Dean, 917.592.9091 or Craig Schwab, 646.231.1466**





**DOYLE SECURITY SERVICES**  
At Your Service in New York,  
New Jersey & Pennsylvania

**PROTECTING YOUR PEOPLE, YOUR PROPERTY AND YOUR PEACE OF MIND.**



*Selecting Doyle Security Services means:  
competitively-priced service that's tailored to  
your requirements and meets your exacting  
specifications. It's delivered by a team that's easy  
to reach, easy to work with and focused on  
continuing relationships.*

**(877) 377-7749 • doylesecurityservices.com**



# BEYOND BOLLARDS

**By Mario J. Doyle CPP**

**T**here was an ongoing discussion within the security community about improving the protection of the New York City metropolitan area long before Mayor De Blasio's January 2, 2018 announcement about adding 1500 new bollards to try to prevent vehicle ramming attacks on NYC walkways and adding \$52 million to NYC's security infrastructure. What to do and how to do it are questions that provoke some of the deepest conversations.

Those involved in traditional security tend to work from assumptions that no matter how good our intrusion barriers and detection systems are and no matter how many people we have on our teams, there will be breaches. We plan for them and train to address them. When we don't catch them, they can be embarrassing. In late January 2018, it was the Bloomberg Building visit. Three young men penetrated security and climbed the building's 800-

foot tower. They became instant social media stars, prancing around a tiny platform at the tower's top.

At one time, breaches seemed something that could be controlled by firewalls, encryption, etc. on the IT security side; however, this appears to be an illusion as millions of public and private records get hacked, stolen and misused, making headlines over and over again.

During a recent discussion with

colleagues, several issues were discussed including the following:

- What are we now assuming about terrorists that may keep physical security plans from being the most effective? If we use bollards to narrow walkways to prevent pick-up truck attacks, are we now inviting motorcycle attacks so bollards themselves assist in injuring people?
- Are we engaging our constituents in the overall security perspective? It isn't a new concern but has to be revisited. Sometimes employees' comments



about our security programs surprise us and something as simple as changing where officers are posted improves how an entire department is perceived.

- What are our channels for obtaining feedback/observations from the thousands (or dozens) of eyes and ears within facilities we cover? How do we encourage

“See Something – Say Something?” We'd rather have too much input than miss something critical

- Once we engage artificial intelligence (“AI”), we no longer control it. Remember Space Odyssey: 2001, and HAL the computer?
- Given the dark web and hackers' abilities to reach into and alter systems, how are we verifying data that are crucial to emergency responses?

In August 2016, Forbes carried an article by Earl Perkins of Gartner, Inc., in which he

summarized what he saw as the: “Top 10 Security Predictions Through 2020”. Several are worth including:

- Expect that by 2019, passwords and tokens in medium-risk cases will drop 55%, as new recognition technologies are introduced.
- Through 2018, more than 50% of Internet of Things (“IoT”)

device manufacturers will not be able to address threats from weak authentication practices.

- Employ metrics to assist in identifying risks to enterprise architecture as the use of IoT increases.
- By 2020, more than 25% of identified enterprise attacks will involve IoT, though IoT will account for only 10% of IT security budgets.
- As IoT usage grows, vendors will favor usability over security and IT security practitioners remain unsure of the correct amount of acceptable risk.
- An enterprise must assign business ownership of IoT security and target selected areas of security budgets to manage IoT risks.

In addition, The Information Security Forum noted, we've seen automated misinformation and distortion gain instant credibility; privacy regulations get in the way of monitoring insider threats; and as stated earlier, deploying AI can lead to unexpected outcomes.

The challenges for security professionals are right in front of us. Some are as tough as steel bollards sunk in cement; others are invisible yet materialize in even harder-hitting ways. There is never a dull moment and like you, that is probably why I chose this industry.

*Mario J. Doyle, CPP, is COO at Doyle Security Services, Inc. (DSS)*

# SURVIVING MOTHER NATURE

## Case Studies in Successful Emergency Management

By Glenn Sandford, CPP and Art Boyko

From earthquakes in Latin America to tsunamis in Asia and Category 4 hurricanes in the United States, it seems to be more and more common to hear about or directly experience devastating natural events that have caused entire regions to scramble resources and respond to save lives, provide aid, mitigate damage and recover from the effects of Mother Nature. Over the course of our company's history, AT-RISK International has been involved with a number of these efforts. Last year alone, we responded to evacuation needs in Houston, Texas, after Hurricane Harvey and barely a month later, we deployed several teams to Puerto Rico in the aftermath of Hurricane Maria. Both operations resulted in solid successes for our customers as well as for AT-RISK, but there are always things to be learned. It is these lessons that we wish to share so that you can evaluate opportunities to strengthen your emergency management plans.



1. Timing your response to the affected area is critical. In a best-case scenario for a weather-related catastrophe, you may have 7-10 days' notice as to

2. With regards to being properly equipped, we cannot stress enough the importance of having tangible resources available for your team. Critical



where and when the weather event will strike. As you know, weather can be unpredictable and in a worst-case scenario you may only have 48 hours or less to react. In the case of the latter, it will be extremely challenging, if not impossible, to deploy and equip a quality team. Proper planning is essential to a successful mission. When feasible, consider staging your team as close as safely possible before the event. This can help reduce response time from days to hours. Make sure that they travel with the gear and supplies they will need or that they have the means to acquire those items while in route to the deployment point.

items such as vehicles/trucks, ATVs, flat bottom boats, jet skis, etc., will help ensure safety for your team and the people in need. Don't forget to have a trailer and/or appropriate hitch, including DMV registrations for the trailers, to transport your rescue vessel around. In addition to the required transportation items, make certain you have other supplies. This does not mean clean out the shelves of your local Costco or Sam's Club. Too much gear can be cumbersome and an unnecessary travel burden. Make your best estimate on the length of stay and the type of assignment and bring just enough supplies for that duration. Water, hygiene items,

easy to carry food such as bars and other choices rich in carbohydrates and protein are sufficient.

3. Moving away from the practical aspects, it is worth highlighting how important it is to have the correct relationships in place. After both Hurricanes Harvey and Maria, our team had an outstanding rapport with the local police, including Incident Commanders, who conveyed important daily matters regarding road closures, curfews, hospital details, shelter capacities, crime reports, etc. Possessing, conveying and using that information allowed for a safer and more efficient response and generated confidence among victims and corporate leadership alike. Other types of relationships are important as well. Those may be internal to your organization, such as finance and purchasing departments, or external resources such as vendors, travel agencies and other service providers that you may need to support or augment the team being deployed. Ideally, these relationships and resources will have been established and tested prior to an emergency response. As the saying goes, "better the devil you know than the devil you don't know."

4. If your deployment is likely to be particularly challenging due to length or harsh conditions, maintaining high spirits and keeping your team motivated is an aspect well worth considering. Sometimes you need more than just financial

incentives to help your staff maintain positive attitudes and best efforts. As we saw in Puerto Rico, some of the security team in the field were working 12+ hour days, 7 days a week for upwards of 2-3 months. Although that amount of work may look great in the bank account, careful supervision is needed to maintain quality coverage. Complacency, illness and burnout are common consequences of long-term or difficult deployments. Even when staff don't want to rotate out, an experienced supervisor will know that mandated breaks are in everyone's best interest. Having a corporate leadership presence can also produce a lot of mileage. Motivational comments from senior management have far greater value when given face-to-face and in the same environment as the deployment. Local supervisors or managers can also keep morale high by breaking away from administrative functions to participate in the day's work, stepping in to help with routine tasks or standing a post while the staff member takes a 15-minute break. Other positive support tools such as a "good work" letter that is read to the team at the morning briefing can help to generate revitalized energies and increase motivation among workers.

5. Timely and effective communication can help avoid many problems and keep small issues from turning into big problems. During an emergency response deployment, the value of effec-

tive communication at all levels of the operation cannot be overstated. Amid times of crisis, communicating effectively can be challenging for a variety of reasons, whether it be due to time, technology or simply being overloaded. Some of the best emergency response managers state that they prefer to be bombarded with unfiltered information rather than risk being unaware of a critical detail. While that places a great deal of burden on the manager, it is a best practice that works well when the manager is one of the calm, cool and collected types that is not easily flustered. When possible, communications



should be in writing, so that the recipient does not have to rely on notes or memory. Consider that with all the various options available, it's usually not hard to send off a text, IM or email. If you have the luxury of wordsmithing, that's fine; however, don't lose

precious time. If you can't decide whether the communication is timely or necessary, it's probably better to send it than sit on the information.

There has been much written about emergency management planning and there are any number of fine resources to which you can turn to find information about writing, testing or updating a response plan. It was our goal in this article to detour away from the conventional material and provide some real-life insights into the practical aspects of preparing and managing a quality emergency response team. While it is our hope that the information shared here is

relevant and useful, it is our greater hope that you will never have a need to put it into practice.

*Glenn W. Sandford, CPP, is Director of Operations, LATM and Art Boyko is Manager, Operations for AT-RISK International.*

# PHYSICAL ACCESS CONTROL SYSTEM: Security Concerns and Best Practices

By Alex Alexandra

## I. Introduction

Physical access control refers to access to buildings, rooms and control gates, using Fob keys, access cards, mobile device applications (apps) or other tokens to allow access to these areas. An access control system allows the end user to manage and screen access to a particular area, entry or exit point in real time. In some cases, for example in restricting access to medical centers, companies and agencies are required to adopt access control systems as part of regulatory compliance. Hospitals are required to comply with state, local and federal requirements such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as well as with requirements set by independent, not-for-profit organizations like the Joint Commission for Regulatory Compliance. Additionally, some companies need to comply with security-conscious businesses compliance regulations (SOC 2) or be in compliance with Security Council standards (PCI). Any software that resides on a network and works alongside a variety of IP based devices is vulnerable to cybersecurity attacks.

This article will describe best practices for physical access control and will strongly suggest that the success of an access system depends upon its ease of use, communication with and training of

users and administrators, integration with other systems, and software and security updates.

## II. System description

Most access control systems consist of the following components: access control software, control panel or controller, credentials (contactless proximity or magnetic stripe cards, key fobs, bracelets, apps, passwords, biometric credential, etc.), lock (maglock or electric strike, wireless locks), readers (biometric, card readers with or without keypads),



a server (where the database resides), and a workstation. In an access control environment, an access point may be a door, gate, closet, or an elevator door where the system permits access. The access control software is the heart of every

meaningful system. The software usually handles a large number of access points, zones, different levels of users, calendars, time periods, time zones, and more. In addition, access control is



usually handled by web-based software (client-based or web-based application) that can be accessed from any workstation with the right credentials. Since the application is web-based, the interface between a user and the software may be accessed using the Internet or an Intranet through a browser.

The access control database or Access Control List (ACL) resides on a server and is accessed over a network. The control panel (controller or control unit) gives the lock the signal to unlock the door when it receives the request from the reader. Then, it verifies the request with the user's credentials, and if the credentials match, the controller signals to unlock the door. According to Stalling and Brown (2008), the credential identifies an individual during the human-machine interaction utilizing the following methods of authentication; "something the individual knows, something the individual possesses, something the individual is or something the individual does."

An example of a secure credential is a combination of a proximity card, (something the individual possesses), and a PIN number (something the individual knows). This is an illustration of a Two-Factor Authentication (2FA) authentication. For improved security, a 2FA or a Multi-Factor Authentication (MFA) is usually employed. According to The National Institute of Standards and Technology (NIST), MFA is sometimes

referred to as 2FA. Sarbanes-Oxley and HIPAA require that institutions establish strong internal controls to mitigate risks and protect data centers from data breaches.

The credential (fob keys, radio-frequency identification (RFID) cards, bracelets, apps, etc.) will vary, depending on the level of security and the level of usage. Credentials should offer convenience and ease of use and should be cost effective. Biometric authentication credentials sound and look more secure but consideration of their use should be based on accuracy factors, such as false acceptance rate, false rejection rate, and identification rate. In some cases, a mobile phone app using Bluetooth or Near-field communication (NFC) may be used as a credential for communicating between the mobile phone and the lock.

## III. Security concerns and risks

Any software that resides on a network and works alongside a variety of IP based devices (readers, locks and controllers) is vulnerable to



a variety of attacks. By compromising an access control system, a hacker would not only have access to its database, but could control all access points. The hacker could threaten to leak users' sensitive information, delete access data from users' profiles, and open every door or gate connected to the system unless the institution pays ransom. Many companies are turning to IP based access control systems but lack awareness and understanding about security vulnerabilities

Continued on page 54

that can lead to an attack. One problem is the lack of communication and collaboration that exists among the installers, the administrators who manage the systems and the IT security of the organization. As a result, IT security can overlook issues such as insecure software, firmware installation of the readers, controllers



and wireless locks, unprotected mobile app interfaces, insecure web interfaces and lack of transport encryption. They may choose to favor convenience over security by simplifying user names and passwords.

Another issue is that some software manufacturers do not provide follow up with IT security after installation. Furthermore, some components (readers, locks) come from third party vendors and run on outdated software/firmware. Hypothetically, an attacker could exploit all the above vulnerabilities to gain access to an organization's networks. Hacking techniques include packet-sniffers (e.g. Wireshark), where a hacker captures and analyzes data packets that can be used to obtain information like passwords, etc., and a man-in-the-middle (MITM) attack where the hacker eavesdrops on the communication between two targets using a separate computer that accepts traffic from each one. Security attacks become worse every year and will not lessen, especially when hackers know that organizations will meet their ransom demands.

#### IV. Conclusion and best practices

Physical access control technology has grown tremendously in recent years and is changing

how we use keys and locks. Wireless solutions, used with a variety of credentials, can secure many things besides just doors and gates. Smart homes integrate access controls, a variety of credentials, and a security system, along with closed circuit cameras, lighting and sound systems, under a single control panel that can be accessed from anywhere in the world.

Those using wireless solutions can expect an increase in IT vulnerabilities and data breaches. In the corporate environment, physical access controls, used with fire alarm systems, are becoming critical investments for every organization.

The choice of an access control system should be treated as a long-term capital investment. Two important criteria should be ease of use and the ability to be transformative to the organization. The system must have distributed intelligence and the ability to integrate with other systems, such as closed-circuit cameras, alarms, fire systems (fire and life-safety codes), etc. In addition, the system should be expandable and be able to handle additional users, devices and locations within one application. In the age of mobility, the system should be capable of monitoring and providing access using mobile devices (credential and monitoring apps). Furthermore, from a security perspective, the system should be able to use smart credentials like encrypted RFID card technology and biometric readers for additional security.

Finally, the manufacturer must be able to regularly provide critical software updates, including security and firmware updates, to the IT department of the organization. Any system by itself cannot survive unless the human element is involved. Communication with the vendor, manufacturer and the IT department combined with systematic training of administrators are critical for the success of the system.

*Dr. Alex Alexandra is an Assistant Professor in the Department of Security, Fire and Emergency Management at John Jay College of Criminal Justice.*

# CERTIFICATION PROFILE: CARESS KENNEDY, CPP

By Mary Alice Davidson

In her role as president of Allied Universal Security Services' Northeast Region, Caress Kennedy, CPP, keeps her focus and her team's concentration on "perfect service and keeping our clients for life," she says. The goal is to understand client needs and problems "so we can provide solutions that raise the level of service delivery and satisfaction."

Kennedy joined AlliedBarton in 2011 as managing partner of the New York/New Jersey region and grew the region to the company's largest in terms of revenue. She was promoted to her current post in 2016 with responsibility for eight states and more than 28,000 employees. That same year, Kennedy earned the Certified Protection Professional® (CPP) credential.

"My motivation was to be sure that I had the requisite skills to act as a consultant to my customers," she says. "The training helped expand my knowledge of security."

While Kennedy had a personal incentive to become certified, she had the same goal for her leadership team.

"I sponsored a large group of them, and we all attended a review session," she says. "I also established a contest to incentivize them to complete the exam." Several members of her team did pass the exam.



Kennedy was recruited into the security field while president of a staffing company. Prior to that Kennedy worked for AT&T, Xerox, and other Fortune 500 companies. One of her priorities at Allied Universal is to "select candidates with the best fit for our clients," she says. "And once they are hired, develop and reward them so they stay engaged."

Memorable moments for her happen when company officers or managers take on extraordinary duties. As one example during Hurricane Sandy, officers saved a passenger in a taxi from drowning in a flash flood by entering the water themselves and risking their own lives. In another instance, a manager and his team volunteer annually to provide security for a Pediatric Cancer Walk.

One aspect of her work that Kennedy finds especially satisfying is the opportunity to keep clients safe by recommending best practices and technology solutions

to enhance their programs. She encourages managers to be out in the field, and she leads by example—spending much of her time outside the office.

Kennedy makes a point to take advantage of the education and networking available through her membership in ASIS International. "The conferences and guest speakers at monthly meetings are outstanding," she says. To further round out her professional skills, Kennedy attained an MBA in management from Pace University and completed many other senior leadership courses.

In March 2017, Kennedy received the "Above and Beyond Award for Outstanding Women in Business" from New York's City & State Magazine. She was one of just five women to be selected in the Business category.

While she has forged an impressive career in executive leadership outside of and then in the security sector, she enthusiastically recommends the security field to others.

"It's a growing \$40 billion industry, and it helps people," she says. "What could be a better career?"

*© 2017 ASIS International, 1625 Prince Street, Alexandria, VA 22314. Reprinted by permission from the October issue of Security Management magazine.*

# SMALL UNMANNED AERIAL SYSTEMS:

## The Changing Face of Emergency Management



By John R. Morgan, CPP

It's an exciting time in the world of small unmanned aerial systems, hereafter referred to as drones, not the least of which are applications in emergency management. This article looks at the significance of this emerging technology providing support to the discipline of emergency management and addresses past, current, and future trends. For the purpose of this article, the author is referring to small quad-copter style drones weighing less than 55 lbs., also referred to as sUAS, which are aerial vehicles in which the lift is generated by four rotors and the pilot uses a remote control to control the drone.

There are roughly 770,000 drone owners who have registered their drones with the FAA, and there are about 80,000 certificates that have been issued by the FAA allowing for commercial and government drone use. The true number of drone owners is elusive; reportedly up to 2.5 million drones are flying over U.S. skies. The FAA categorizes drone use into three areas (1) public operations – government; (2) civil – non- government; and (3) model.

Drones can and do support all four tenets of emergency

management: mitigation, preparation, response, and recovery, but recently have received notoriety for use in the response phase of disasters worldwide, e.g. the 2008 Wenchuan Earthquake in China; the 2011 Fukushima Daiichi nuclear accident in Japan; the 2014 mudslide disaster in Oso, Washington, as well as during the 2017 Hurricanes Harvey and Irma to assess damage.

The use of drones in emergency management is encouraging since drones are versatile and can keep responders out of harm's way while assessing a disaster area. Drones are able to fly over dangerous terrain at low altitudes, as well as fly within remote locations and can be deployed quickly. The cameras attached to drones offer high resolution images and drones can be linked to sophisticated software, such as mapping software Drone Deploy or related software, depending upon the mission.

Drones in emergency management are not without challenges. The FAA currently mandates that a certified commercial drone pilot have line of sight of the drone, fly no higher than 400 feet, and fly during daylight. A drone pilot also needs to pay close attention to the battery life of an airborne uSAS, as battery life is very limited, usually twenty minutes or less. The demanding FAA standards of certification are well intentioned due to safety concerns but can also challenge a pilot who is looking to provide benefit to vulnerable populations when time is a critical factor.

Other challenges include instances of unauthorized flights that have resulted in jeopardizing the safety of emergency response personnel, such as in the 2015 San Bernardino County Fire in which five unauthorized drones were interfering with the safety of fire fighters. Officials had to call off their operations to drop water and flame retardant to avoid midair crashes. Fortunately the FAA is reportedly planning new regulations to address the interference by hobbyists as well as those who fly for profit. Those who fly for profit usually photograph a disaster in order to sell the video footage to news services or others.

Additionally, countries that do not allow drones to be used in missions related to international humanitarian aid pose challenges. Other challenges include disaster victims who may fear a drone because they do not understand its role or may perceive it as a threat to their privacy. Overcoming privacy issues and community

concerns over the use of drones ties into another emergency management concept called the three Cs: Communication, Collaboration, and Coordination. This is a significant consideration as the use of drones for emergency management intensifies and becomes more complex.

Besides flying safely, the successful outcome of flying a drone for emergency management purposes is to gather intelligence so that good decisions can be rendered. Dr. Robin R. Murphy, the founder of the Center for Robot Assisted Search & Rescue at Texas A & M University, has pointed out that the flight should result in gathering information and then disseminating the information to the needed stakeholders. Decision makers need actionable data that is accurate and timely.

In 2013, Kelly Cohen, a professor at the University of Cincinnati, predicted disaster management and public safety officials would be among the first to be licensed to operate drones in the national airspace. Since that time the FAA has allowed public entities, including public universities, to bypass the pilot certification exam and self-certify via a certificate of waiver. There are other predictions that the FAA will adjust the line of sight rule in the future so that medications can be delivered to disaster victims who are stranded as well as for other emergencies. Not only is the technology evolving but so are the regulations.

Finally, drone deployments for emergency management are expected to increase exponentially as drone related software, training of users, regulations, and drone equipment continue to evolve to provide support to a host of stakeholders, including but not limited to emergency managers, first responders, and Incident Command System personnel. As of 2017, the Center for the Study of the Drone at Bard College reported that 347 agencies, including state and local police, fire, and emergency management units had acquired drones in the last several years. FAA Administrator Michael Huerta said drones play a transformative role. Emphasis is once again placed on the data gathered by the drone that can potentially reduce the hours or days to provide disaster response, thus saving lives. This is appropriately referred to as 'data to decision' and will continue to change the face of emergency management.

**John R. Morgan, CPP is an FAA certified drone pilot, 14 CFR, part 107.**

When the **UNEXPECTED** Strikes

**EXPECT THE BEST  
FROM BROWNGUARD®  
INSURANCE**

65 years of meeting and exceeding our Security Industry clients' expectations.

When it comes to insurance, there are no surprises with Brownyard Group®. As the longest-running, family owned and operated specialty insurer, we set high expectations for ourselves – a continuing promise to apply our deep knowledge of security industry risks to deliver exceptional coverage, risk management and claims handling to Security Professionals.

Set high expectations for your insurance with BROWNGUARD – contact us for a competitive quote.

**Brownguard®**  
Insurance when you expect the BEST



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

*We Insure:*  
**Security Professionals, Private Investigators,  
Security Consultants & Alarm Services**



**PERSON OF  
THE YEAR**

**May 22, 2018  
Chateau Briand**

Hon. Errol Toulon Jr.  
Suffolk County Sheriff

Also Honoring:  
Arthur B. Colwin Jr.  
Memorial Security Officer of the Year

Young Professional Award  
William McGuire  
President/CEO  
Global Elite Group  
Cocktails: 6:00pm  
Dinner: 7:00pm  
Individual tickets : \$100

**ASIS International  
Long Island Chapter  
3280 Sunrise Highway #306  
Wantagh NY 11793  
www.asisli.org**

# Evaluating the Total Resilience Lifecycle: Mitigating Continuity Risk from Vendors

By Daniella Bove-LaMonica

Resilience is a current buzzword within the security industry. Many firms, particularly those subject to increased regulatory oversight, are in a race to prove to their investors, clients and business partners that they are more robust, more disruption-proof, more resilient than their competitors. But what defines a functional resilience program?

A great starting point is the British Standards Institute's ISO BS65000 "guidance" on organizational resilience, which champions "the ability to anticipate, prepare for, respond and adapt to events—both sudden shocks and gradual change." However, regardless of how robust the program, most firms fail to account for continuity risks related to their global vendor operations when building out their organizational resilience framework.

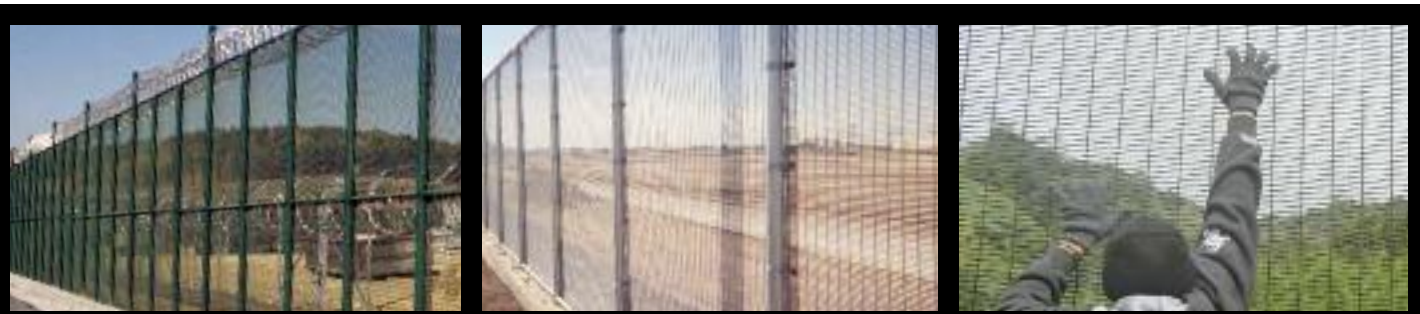
As we race to harden our corporate perimeters against the next Sandy, the next Barcelona, the next reputational challenge, we must acknowledge that we are only as strong as our weakest link. For many in the resilience

space, a major vulnerability point sits with the vendors. The challenge is this: When you consider your incident management/business continuity lifecycle, have you included your vendors within that framework? Have you extended your risk assessment and analysis program to include evaluating the level of preparedness of the firms providing your sourced work? And if not, how do you sell the idea to senior leadership?

Resilience is a nuanced and subjective concept, with a threshold that varies from firm to firm. The tolerance for business continuity planning (BCP), particularly when making a business case for spending money, depends on the organization's risk profile and its larger operational footprint. And, where resources are constrained or focused on the more profitable areas of the business, the idea of spending additional time or money that might never see a return on investment is not appealing to leadership. However, there are some simple steps that can be taken, with

**Resilience  
is a  
nuanced  
and  
subjective  
concept,  
with a  
threshold  
that varies  
from firm  
to firm.**

Continued on page 61



# WIREWALL®

## SECURITY STARTS HERE



**RIVERDALE** 1.800.762.6374 • +1.508.234.8715 • info@riverdale.com • www.riverdale.com



♦ ACCESS CONTROL ♦ FIRE & LIFE SAFETY ♦ CCTV ♦

♦ DATACOM ♦ COVERT ♦ TSCM ♦ DAS ♦ ARC ♦

**NY**  
**(TEL) 718.461.2600**  
**(FAX) 718.461.4060**  
**15-03 132<sup>nd</sup> Street**  
**College Point, NY 11356**

**CONTACT US**  
**For More Information**  
**OR**  
**Visit Us Online at:**  
**WWW.NYAES.COM**

**NJ**  
**(TEL) 201.796.0015**  
**(FAX) 201.796.3960**  
**295 Molnar Drive**  
**Elmwood Park, NJ 07407**

limited associated costs, which will vastly improve a firm's total resilience lifecycle.

First and foremost, it is imperative that an organization decree business continuity planning as a key corporate value. Placing BCP front and center within the organizational culture means employees will become hard-wired to account for it in their actions. The operations team cannot just carry this mantle; it has to cross business units as a collective company value.

A security manager or business continuity practitioner cannot be everywhere at once. Employees must know to account for BCP within their deliverables and question practices that do not meet the firm's threshold. If BCP is a core company value, it will be a natural part of contract negotiations. The contract stage with a vendor is a critical juncture point for resiliency and the one area where, most frequently, operations personnel are not in the room.

Second, those who own the relationships with vendors should understand their vendor dependencies at a fundamental level. A strong BCP program manager will provide guidance and training to those business functions that have external touch points on how to approach the vendor relationship from a business continuity angle. With the appropriate training, those that own the vendor relationship

can come back to the resilience planning team to map out a business impact analysis (BIA) specifically relating to the vendor's role within their business unit. Once all vendor BIAs are collected from across the enterprise, it is possible to tier out a vendor incident response program that is both accurate and responsive to a firm's larger resilience strategy.

It follows that once the critical vendors are identified, the business should work with these providers to understand the maturation levels of their continuity programs. Does the vendor have a corporate resilience policy? Does the firm train their teams on incident management and to what level? If this provider has a single site, how does it manage its continuity of operations in case of a business disruption? Are legal safeguards in place to protect the contracting firm from owning any financial risk related to a vendor's continuity issues? Working with vendors to provide a transparent accounting of their internal risk profile allows the contracting organization to improve plans for its own potential business disruptions.

Solving for the total resilience lifecycle need not be an insurmountable, expensive proposition. Of course, like anything in the security industry, the mitigation of vendor risk can be outsourced at varying levels of sophistication at a variety of

price points. However, it can also be managed internally at a lower cost through certain tools available for purchase or, if nothing else, simple elbow grease, checklists and a keen attention to detail. *Harvard Business Review*, in making a case for "prospering during business upheavals" speaks about fostering a "culture of

**First and foremost, it is imperative that an organization decree business continuity planning as a key corporate value.**

resilience" within organizations and individuals. The key here is anticipating all of the variables that can actually impact the bottom line. Expanding a firm's inherently narrow definition of resilience to meet the true reality of one's global operations drives forward a clear path to a successful continuity of business.

*Daniella Bove-LaMonica is the Business Continuity Manager for Global Data Operations at Bloomberg, LP.*



# Advancing Security in New York City and Beyond

By Ernest J. Pucillo

Is there a rubric for advancing security in America today? In the continental United States statistics indicate that the crime rate has fallen to lows not seen since World War II, according to a report published by the Pew Research Center in February of 2017. This analysis, however, does not translate into a perception of security across America. The perception held by Americans is that crime is rising. That perception is based on factors relating to global terrorism, mass shootings, and violent crime in urban areas that represent a new paradigm for those involved in safety and security.

Examining mass shootings in the United States over the last ten years shows how crime and disorder are changing our society. It is part of the problem that creates an atmosphere of fear and dread across the country.

- Blacksburg, Virginia – April 16, 2007, 32 killed, many wounded (Virginia Tech)
- Omaha, Nebraska – December 5, 2007, 8 killed (shopping mall)
- Kingston, Alabama – March 10, 2009, 10 killed
- Carthage, North Carolina – March 29, 2009, 8 killed (nursing home)
- Binghamton, New York – April 3, 2009, 13 killed, 4 injured (Immigrant Community Center)
- Fort Hood, Texas – November 5, 2009, 13 killed, 32 injured
- Appomattox, Virginia – January 19, 2010, 8 killed
- Seal Beach, California – October 12, 2011, 8 killed (Salon Meritage)
- Aurora, Colorado – July 20, 2012, 12 killed, 58 wounded (Movie theater)
- Newtown, Connecticut – December 14, 2012, 20 children and 6 adults killed (Sandy Hook School)
- Washington Navy Yard – September 16, 2013, 12 killed
- Charleston, South Carolina - June 17, 2015, 9 killed (Emanuel African Methodist Church)
- Roseburg, Oregon – October 1, 2015, 9 killed, 9 injured (Umpqua Community College)
- Orlando, Florida – June 12, 2016, 49 killed, 50 injured (Public Night Club)
- Las Vegas, Nevada – October 1, 2017, 58 killed, 500 injured (Harvest Country Music Festival)
- Sutherland Springs, Texas – November 5, 2017, 26 killed, 20 wounded (town church)

The list reminds us of casualties of war lists but in a war that continues over a ten-year period. Locations are towns and villages across America. The attacks are in schools, a movie theater, churches, shopping malls, at public events, and no place is immune or safe for citizens. As this war rages across America we are faced with a second front consisting of terrorists who are determined to punish us by killing people through jihad. The last two years alone show numerous attacks have been made to inflict mass casualties:

- September 17, 2016 – Stabbing of 10 people in shopping mall in Minnesota.
- September 17, 2016 – Bombing, Ahmad Khan Rahmi- Shrapnel filled pressure cooker bomb detonated in crowded space on West 23rd Street between 6th and 7th Ave. A second device was found at west 27th Street.
- Seaside New Jersey, a pipe bomb explodes at about 9:30 am, no injuries reported.
- November 28, 2016 – Vehicle attack, stabbing, 11 injured, (Ohio State University).
- October 31, 2017 – A man drives a rented truck down a pedestrian walkway on Manhattan’s west side; 8 killed, dozens injured.
- December 11, 2017 – Ahayed Ullah carries a pipe bomb into a crowded NYC Subway. The bomb explodes prematurely and Ullah is injured with severe burns. 3 other people injured in the attack.

This list is only a partial representation of terrorist attacks occurring across the country. It shows some varied locations that are targeted by terrorists. Some have personal

vendettas and others represent extremist jihadists.

The question at issue is how do we provide for the safety and security of people when the methods used and the targets selected represent such a wide array of public locations? What methods do we employ to enhance security in open venues for public events and private organizations targeted by terrorists? How do we enhance security in a maximum risk environment, and finally how did we get here?

We live in a country in which some immigrants come for a better life and some come to destroy the American way of life. We must adapt, like the Israelis have adapted, to a constant and present danger. Since our enemies utilize varied tactics our approach must be so as well.

Advances in technology have given us an ability to forensically identify perpetrators of crimes and their associates. The utilization of CCTV in many high-risk locations, license plate readers, and more importantly the ability to store and retain large amounts of data from these devices enhances our ability to quickly investigate crimes and apprehend dangerous felons. The utilization of smart cameras in public areas can help us identify suspicious packages. Department of Justice grants like COPS and Project Safe Neighborhoods helps foster information sharing from the local community to the police and vertically from local agencies to State and Federal partners in law enforcement. Continued advancements in communications networks help to provide warnings to students on university campuses and to local communities about threats that may exist. We have

learned through after action reports how to better defend against violence using counter surveillance techniques by security officers and police that may identify some pre- operational planning by criminals. We also need to remember that some level of “force protection” must be provided to visible officers that are the first targets for criminals attempting to take out our first line of defense. We need to continue to engage the community at large to help us identify suspicious activity. As Benjamin Netanyahu, the Prime Minister of Israel said, “Terrorism cannot survive in a democratic society for one reason, the people won’t let it.”

We need to continue to practice our response to violent incidents of mass destruction working with private industry in training and exercises to enhance our ability to save lives and recover from attacks on our communities.

It clearly shows that no one method provides a solution to our ability to advance security in a dangerous world. It is clear that the social dynamics we face in the future are different from those of the post-World War II era. As we are able to continue to advance in technological science and coordinate our efforts to support security operations, we will meet the challenges that we face.

*Ernest J. Pucillo retired from law enforcement after 37 years at the rank of Deputy Chief of the MTA Police Department in New York City. He currently teaches Criminal Justice and Emergency Management Response, Incident Command, at The Long Island Business Institute in Queens New York*

# Disruptive Technology is Vital to Staying Ahead of Today's Security Threats

by Michael O'Neil

When we think about today's technology, it is hard to argue against the benefits that cell phones, email and social media bring to our daily lives. They afford incredible convenience and a level of enhanced communication that we could not fathom even a few years ago. Unfortunately, it is this very same technology that has created the single most critical issue for enterprise risk and public safety. Terrorists now exploit online platforms and social media sites to radicalize and recruit, share information and rapidly advance the threat. Additionally, they are consistently innovating to circumvent current security technologies.

To successfully address the exponentially growing threats proliferating through terrorists' shrewd use of today's technologies, the public and private security industries need to advance more quickly. Terrorist tradecraft has continued to evolve in the area of improvised explosives, particularly with peroxide based and other homemade explosives. Trained

bomb makers continue to experiment at their own peril, synthesizing various chemical compounds in an effort to disguise explosives and enhance their strength. Through the use of online communication platforms, including social media, this information is dispersed to hostile actors around the globe who are using it to produce mass casualty events.

Sustaining technologies, those that rely merely on incremental improvements to already established solutions, will never defeat this threat. To be successful, the industry must develop and employ truly disruptive security solutions that innovatively blend state-of-the-art technology with trained experts. This combination is critical for success.

## X-ray Technology

X-ray technology is used by every major government institution and Fortune 500 company to screen deliveries

and mailroom packages for explosives. Tactically speaking, X-ray technology is not new or disruptive, but when you combine X-ray capabilities with the trained eye of a bomb technician, the value of the X-ray as a tool rises to a new level. SmartTech® is a technological solution that delivers this rare combination.

SmartTech® was modeled after a common medical industry practice. Physicians and clinicians around the world have long shared X-ray images and MRI scans in real time with one another to produce the best possible diagnosis and response plan. Similarly, SmartTech® allows questionable X-ray items



to be viewed in real time by FBI-certified bomb technicians who analyze, confirm or clear suspicious visuals in mere minutes. It creates an economy of scale which enables users to access expertise not available anywhere else in the private sector. It is important that we foster continued innovation in the vein of SmartTech® and look to peers in different fields to identify technologies and processes that enhance the security industry.

## Explosive Detection Canines as Technology

In many environments, a properly imprinted and trained canine is the most effective technology for explosive detection. Though the Pentagon's Defense Advanced Research Project Agency (DARPA) spent \$19 billion over several years to develop the next level of explosive detection, the Agency concluded that the canine remains the unrivaled tool. MSA's newly developed Advanced Alarm Resolution is a patented process that capitalizes on this canine detection capability, strategically blending it with uniquely-qualified subject matter experts to deliver an unmatched screening solution.

Within the air cargo sector, as an example, a canine might indicate – perhaps even on a harmless substance like black powder in a nail gun – while screening a Unit Loading Device

(ULD), pallet or other cargo container. Under the Advanced Alarm Resolution process, the suspicious package is immediately extracted and examined through on-site X-ray screening. The on-site screener can then utilize SmartTech® to securely transmit X-ray images in real time to a remote Emergency



Operations Center for immediate analysis and resolution by trained bomb technicians.

In addition to ensuring 100 percent screening of all cargo, this process of layered explosive screening, combining technology with human expertise, yields invaluable cost and operational efficiencies. Eliminating misinterpretation of suspicious items mitigates the liability risk that leads to service delays, business disruption, unnecessary evacuations or, in the worst situation, the mishandling of a true IED threat.

## Addressing Security Threats into the Future

For the security industry to advance in its mission to combat terror, disruptive technologies, instead of sustaining technologies and processes, must be developed and deployed. Explosive detection capabilities must continue to

evolve, and we must create innovative and strategic technologies and processes that counter radicalization through social media. The most successful security advancements that deliver the greatest protection and peace of mind will undoubtedly combine two critical components: robust technology and human expertise.

*Michael O'Neil is the Chief Executive Officer at MSA Security*



# HOW TO RESPOND TO WORKPLACE HARASSMENT ALLEGATIONS: AN ACTION PLAN

By Katherine A. Lemire & Amy R. Foote

Every Security Director should know how to respond quickly and appropriately to sexual harassment claims to protect their company and everyone involved. This article will help Security Directors, as well as Human Resources Managers, and C-Suite executives understand what sexual harassment is and what you should do if you learn of allegations.

Security directors and their teams are increasingly likely to serve as the initial point of contact for a

sexual harassment claim. Knowing how to recognize sexual harassment and knowing how to respond to reports of sexual harassment are essential to protect the accuser and the accused, as well as limit potential liability for the company.

## WHAT IS SEXUAL HARASSMENT?

Federal law recognizes two forms of workplace sexual harassment: “quid pro quo” and hostile work environment. Quid pro quo harassment occurs when the

submission to or rejection of unwelcome sexual conduct by an individual is used as the basis for employment decisions affecting such individual. A hostile work environment exists when unwelcome sexual conduct unreasonably interferes with an individual's job performance or creates an intimidating, hostile, or offensive working environment. The US Equal Employment Opportunity Commission (EEOC) defines sexual harassment in part as unwelcome sexual advances, requests for sexual

favours, and other verbal or physical conduct of a sexual nature when this conduct explicitly or implicitly affects an individual's employment, unreasonably interferes with an individual's work performance, or creates an intimidating, hostile, or offensive work environment.

Off-color jokes, sexually-suggestive compliments about bodies or apparel, unwelcome and insistent invitations, vulgar language, overly-familiar touching, standing inappropriately close, and conversations and innuendoes to sex acts or sexuality may qualify as forms of harassment. Sexual harassment can take the form of verbal conversation, texts, emails, social media postings, and shared photographs. When such actions are common in a workplace, they can add up to hostile environment harassment.

## WHAT TO DO IF YOU LEARN OF SEXUAL HARASSMENT

To protect yourself and your company, these tips can help in responding to and preventing workplace sexual harassment allegations.

**1. Hear a Rumor? Don't Wait. Act Immediately.** If there is some kind of allegation — even a hint — don't wait. Even if it is “just” a rumor, the onus is on you to act on it. Notify your company's General Counsel or make a report through your company's established reporting procedure. Stalling in response to complaints and failing to interview witnesses could expose your organization to liability and you could get blamed for dropping the ball. The longer an organization or its

supervisors and others in decision-making capacity have known about, allowed, and even fostered harassment without stopping it, the greater the potential liability if litigation ensues.

**2. Preserve evidence.** The preservation of key information is absolutely necessary. As a security professional, you may need to identify and preserve relevant evidence, including video and audio recordings. Ensuring you extract and save vital potential proof of harassment also protects your firm against allegations of not fully cooperating — or worse, a cover-up.

**3. Maintain confidentiality.** There are many reasons for limiting the number of people who know about a workplace sexual harassment allegation and investigation. First, the subject of the allegation can suffer a tarnished reputation if it turns out he or she did nothing wrong. Second, the complainant is vulnerable and must be protected from disparagement and retaliation. Lastly, as is true for any investigation, the inquiry will fare better if it is done discreetly and witnesses are approached without advance knowledge of the subject of the investigation.

**4. Consider an outside investigator.** Federal law requires a prompt, thorough, and impartial investigation. If the subject of the investigation is a manager, or perceived to have close ties to management, you may have extra challenges in ensuring the investigation is perceived as impartial. Outside consultants with

an expertise in harassment investigation may serve to protect you and your company from charges of favoritism and bias.

**5. Know company policies.** Your company's policies may define inappropriate behavior more expansively than federal and local law. Be aware of established reporting procedures to be followed if you witness or hear of workplace sexual harassment. Remember, too, that harassment can occur at off-site, work-related settings such as conferences, meetings, events, and



while traveling. Harassment by your company's outside vendors can also expose you and your company to liability.

**6. Train your staff.** A well-designed training program can be a solid first step towards eliminating sexual harassment from the workplace and minimizing damage if harassment occurs despite your best efforts.

*Katherine A. Lemire is the President & CEO, and Amy R. Foote is a Managing Director at Lemire, LLC. This article is intended for general information purposes and should not be deemed to constitute legal advice.*

# Is Your Mailroom Your Open Door?



By Gary Artinger, John Aizstrauts and Linda Esposito

An open door invites anyone to enter. An unsecured mailroom can allow anyone to enter your business as easily as mailing a package to you. An open door can also allow someone to leave your premises with something that is valuable to you and your company. One must only consider the amount of valuable and/or sensitive information that passes through your mailroom to realize the impact this could have on your business. An unsecured mailroom can allow important company assets to be stolen for personal gain or even greater nefarious purposes. This situation deserves your utmost security attention.

In our current security environment much attention is directed toward cybersecurity. Many companies know all too well the reality of having their sensitive information stolen by hackers. However, a computer hacker must possess highly specialized skills to gain access to the “open door” in your Information Technology Environment.

It takes no skill at all to deliver or remove an item through the open doors of your mailroom. Often, it is all too easy for that open door to allow a physical item that may cause irreparable harm or disruption of your operation to be delivered to your business. Your mailroom can be the open door providing an amateur attacker access deep inside your facility.

Just as cybersecurity employs elements such as complex passwords, firewalls and access restrictions to help prevent unauthorized intrusion into your network, mailroom security should utilize physical and procedural barriers to prevent something or someone from getting into your business. In today’s world, even letter-sized mail can contain dangerous substances that can disrupt or disable your business.

The United States Postal Inspection Service, the federal law enforcement agency of the United States Postal Service that is charged with protecting the US Mail, the postal infrastructure,

and the USPS employees and customers, offers Publication 166, Who Protects Your Mail? Guide to Mail Center Security as a security reference for businesses with mailrooms. It covers topics such as:

- Your Risk Level—Physical security of your workplace
- Your Mail Center—Employee roles and responsibilities
- Mail Theft—Securing your mail center from theft
- Letter or Package Bombs and Bomb Threats—Establish a security and bomb-screening plan
- Chemical, Biological, or Radiological Threats—Securing your mail center from hazardous substances
- References—Checklists and additional resources

An unsecured mailroom lacking adequate physical and procedural security measures can provide someone with an easy means to access and attack

your business. Their attack could be delivered through everyday handling of packages and/or mail. Depending on the nature of your business, your customers and your location, you may have varying levels of risk. If your business has international dealings or provides controversial products and/or services, it may attract unwanted public, political or extremist attention. By routinely reviewing your mailroom operations, layout, employees and tasks, you can begin to assess your risks and specific security needs.

Some primary areas of concern are the manner in which packages and mail are received by your business and the number of locations where these items are received and dispatched. The fewer and more restricted these points, the more control you have over what enters and leaves your business. This also helps minimize the number of locations and people that can potentially be exposed if a dangerous shipment was to enter your operation.

The Postal Inspection Service believes that mailroom security is enhanced when employees understand and implement basic security procedures. It is essential to screen mail for signs that an item may warrant additional attention. Mailroom employees must know how to isolate a suspicious letter or package, how to report it, and how to identify the contents in a safe manner.

In Publication 166, Poster 84 illustrates examples of things that may tip you off to a suspicious item such as:

- No return address
- Restrictive markings like “Personal”, “Confidential”, “Private”
- Badly typed or written and/or misspelled words

- Excessive postage
- Oily stains, discolorations, crystallization on wrapper
- Strange odor
- Incorrect title or addressed only to title
- Lopsided
- Protruding wires

The Postal Inspection Service has specially trained Postal Inspectors who will respond to situations where something suspicious is found in the US Mail. They can determine if the item is hazardous and will handle the item accordingly. Mailroom security suggestions from Publication 166 can also help minimize the risks and business disruptions cause by suspicious items delivered via commercial delivery



services. Although Postal Inspectors will not investigate items delivered by commercial delivery services, the security procedures and protocols should be the same for all items delivered to your mailroom.

An open door can also allow someone or something to exit from your business. An unsecured mailroom can mean someone can easily exit with something that may be important or crucial to your business. Therefore, adequate mailroom security should not only protect against something hazardous getting in, but also protect against

something valuable getting out. Theft prevention is another key factor when considering the security of your mailroom.

Publication 166 also provides several design tips for mailroom physical layout, which in itself is a security measure.

- Make all work areas visible to supervisors
- Use one-way glass, CCTVs or elevated supervisor stations
- Eliminate desk drawers and similar hiding places
- Ensure adequate supervision, especially in high-value areas
- Restrict access to authorized persons by using keys, card keys, ID badges or biometrics

In conclusion, your mailroom is the door into your business. An open door can lead to significant loss or disruptions to business operations.

A properly secured portal will allow essential items to enter, restrict entry of dangerous items and prevent valuable items from being removed. Mailroom security needs to be addressed as part of any comprehensive security plan. While often overlooked and considered a minor

operation within a business, an unsecured mailroom can prove to be an Achilles Heel allowing important business assets to be attacked and/or stolen. In a world where communication is an essential part of business, mailroom security should not be overlooked.

**Contributing Authors:**

**Postal Inspector:**

**Gary Artinger, CPP, PSP, PCI**

**Homeland Security Coordinator:**

**John Aizstrauts, CPP, PSP**

**Physical Security Specialist:**

**Linda Esposito**

# ASIS NYC Chapter Annual Golf Outing Monday, June 11th



The Village Club of Sands Point  
516-944-7400  
Reservations on a first come  
first paid basis  
\$1200 per foursome  
Sponsorships: Platinum \$1000 -  
Gold \$750 - Hole \$300  
Breakfast: 8:00-9:45 am  
Start Time: 10 am SHARP!  
Lunch: on the course  
Cocktails and Dinner: 5 pm

Contact:  
Lynn Brown  
c/o Secure Access  
38 West Park Avenue  
Long Beach NY 11561  
Tel: 516-623-7500  
Cell: 516-384-9447  
Fax: 516-706-5530  
lynn@secureaccessds.com



## WOMEN IN SECURITY

By Denise Niles

*In the spring of 2004, a group of women in the New York City area held an event at John Jay College of Criminal Justice. The group originally named themselves "The Women's Group" since they were comprised of all women and the directive was to support women in the security industry.*

*The event included presentations such as "how to dress for success," "how to apply makeup tastefully," and "resume building." At the time, the number of women in security was limited and the group was asked to change the name to the "Women and Minority Group." The group agreed, and the name was changed. The event, for the most part, was a success; however, the group did not gain any traction and dissolved.*

*Fast forward 10 years and the ASIS Women in Security group was formed nationally. Locally here in NYC, this group, known as WIS, is exclusively for women, and*

*holds several events each year. The focus is no longer on how to apply your eyeliner but how we, as women, can work together in a predominantly male industry. We continue to see growth in attendance and participation at these events.*

*Some of our popular events include the annual self-defense class, held in the either fall or spring and usually at Berkeley College in mid-town Manhattan. The class is always over-subscribed, and we may be able to hold two sessions in the future.*

*Our summer brunch is another popular event and is held in late August. The atmosphere is light, the company excellent and it is a good place for networking. The brunch has grown over the past few years and we are happily looking for a larger venue to accommodate more attendees. We are also planning to add a CPR class for our members. In addition, we partnered with the Young Professionals (YPs) of the NYC Chapter of*

*ASIS on February 8, 2018, for a happy hour and networking social.*

*Today, we aim for networking and helping each other succeed. With the fantastic support of the Board of Directors of the NYC Chapter of ASIS we are able to reach and attract more women to our events. Despite our varied backgrounds and positions in the industry, our common goal is to unify and strengthen our commitment to support each other.*

*The opportunities for women in this industry are growing and more women are in positions of authority and decision making. Issues such as juggling home, work, and children are topics with which many women continue to struggle but together we are strong. We look forward to seeing you at our next event!*

*Denise Niles is the Liaison for Women in Security for the NYC Chapter of ASIS and is Vice President-Key Accounts at Advanced Electronic Solutions, Inc. (AES).*

## Trade Show Committees

### Trade Show Chairman

Raymond Dean  
Co-Chairman:  
Craig Schwab

### Executive Committee

Chairman:  
Lynn Brown  
Vice Chairman:  
Don Francisco  
Treasurer:  
Steve Sacchetti  
Secretary:  
Brian Reich  
Sergeant at Arms:  
Manuel Gomez

### Exhibitor Committee

Co-Chairs:  
Mark Berger  
Bernie Jacobs  
Member  
Charlie Scholl

### Show Coordination

Maria-DiCarlo Cofell  
Jim Kitchen  
Larry Seltzer

### VIP and Dais Committee

George Anderson  
Terence B. Hoey  
Steve Sacchetti  
Izabela Regula  
Joette Faherty  
Elisa Mula

### Security Director

Magazine &  
Media Relations  
Editor:  
Cynthia Webster

### Advertising, Design & Production

Don Blauweiss  
Diane Dudzinski

### Website Management

Rich Patti

### Acknowledgments

We gratefully acknowledge First Republic Bank and MG Security Services for their assistance with the Person of the Year luncheon and all of the other volunteers who worked tirelessly to make the 29th NYC-ASIS Tradeshow a success.



**SAFER**



**FASTER**



**BETTER**

For the Ultimate in  
Protection & Privacy  
...contact us today!



[www.yamaindustrials.com](http://www.yamaindustrials.com)

**Get your message in front of law enforcement and security professionals at the 2019 ASIS NYC EXPO**

**Advertise in**



**Early Bird Special Offer**

Send us your Insertion Order by July 13, 2018 and you'll get a **10% discount** on your ad.

Visit: [asisnyc.org/expo](http://asisnyc.org/expo)

Or contact Diane Dudzinski  
914.779.6846 or  
[diane@blauweissadvertising.com](mailto:diane@blauweissadvertising.com)

**Eugene J. Casey Award** continued

EOD Mobile Unit TEN and deployed to Office of the Secretary of Defense (OSD), detailed to FBI HQ and DHS HQ post September 11, 2001 for Operation NOBLE EAGLE; NSW Operational Support Team TWO (OST2); and SEAL Team EIGHTEEN. His military awards include: Meritorious Service Medal; Navy Commendations Medals (2); Navy Achievement Medals (2); Navy Expeditionary Medal; Global War on Terrorism Service Medal, and numerous other personal and unit awards.

He is also a two-time recipient of the prestigious FBI Director "Exceptional Service in the Public Interest" award. FBI Director Louis Freeh awarded Terence for his work during the TWA Flight 800 recovery and investigation. FBI Director Robert Mueller awarded Terence for his work as Command Master Chief to assigned Flag Officer while assigned to FBI HQ, National Infrastructure Protection Center (NIPC) post-September 11, 2001.

Terry is the founder and president of Hoey & Associates, Inc., a consultancy established in 1995 that specializes in security, crisis and emergency management. He lives in northern Westchester County, New York, with his family.

This year we recognize Terence B. Hoey for his outstanding and selfless contributions to the United States of America, to ASIS International and to the NYC Chapter of ASIS.

*The Eugene J. Casey CPP Award for Distinguished Chapter Service is a special award given in honor of one of the NYC Chapter's founding members.*

**Ready! Fire! Aim!** continued

But as we know, in most good humor there is an element of truth. Projects that go awry follow these steps, and as effective project managers, we must look for the symptoms of b and c and step in as needed to right the ship, lest the rest of the steps take hold.

**10. Debrief each project and apply what you've learned to the next project.**

With good notes, and whatever the outcome, every project provides a learning opportunity for the team and for the team leader (that'd be you). Take time to have a formal review session at the conclusion of the project and get everyone's input on what went well and what could be improved. It will be time well spent.

So, that is my list of 10 things about projects. I hope you found it worthwhile to spend the time reading, and more importantly, that you took one or two tidbits away to improve your own project management skills. And if not, I hope it at least gave you something to think about, to compare your own approach to, in what should be a life- and career-long journey, that of self-improvement. Now, get back to managing those projects and leading those teams!

*George W. Anderson is the Director, World Trade Center Security. He is a past chairman of the NYC Chapter of ASIS and currently chairs the Program Committee for the Annual Person of the Year Luncheon and is the Mentoring Coordinator for NYC ASIS.*



**New Product Features For ASIS NYC**

**iSERIES IP RECEIVER — Experience Total Management & Control Without A Traditional Alarm Panel**

Connects OPTEX's iSeries Wireless Detectors to Milestone's XProtect VMS using the OPTEX BTX plug-in software.



**Genetec™ Security Center RSA Surveillance Add-on**

- Monitor RSA surveillance events in real-time
- Live video associated to RSA surveillance devices
- Arm/disarm zones, track moving targets with speed & directional information directly on a map
- Monitor & arm/disarm zones through the intuitive widget in the dashboard

Available for:  
RLS-3060L, RLS-3060SH,  
RLS-2020i, RLS-2020S



800.966.7839 | [sales@optexamerica.com](mailto:sales@optexamerica.com)

[www.optexamerica.com](http://www.optexamerica.com)



[facebook.com/optexamerica](https://facebook.com/optexamerica)



[@optexamerica](https://twitter.com/optexamerica)



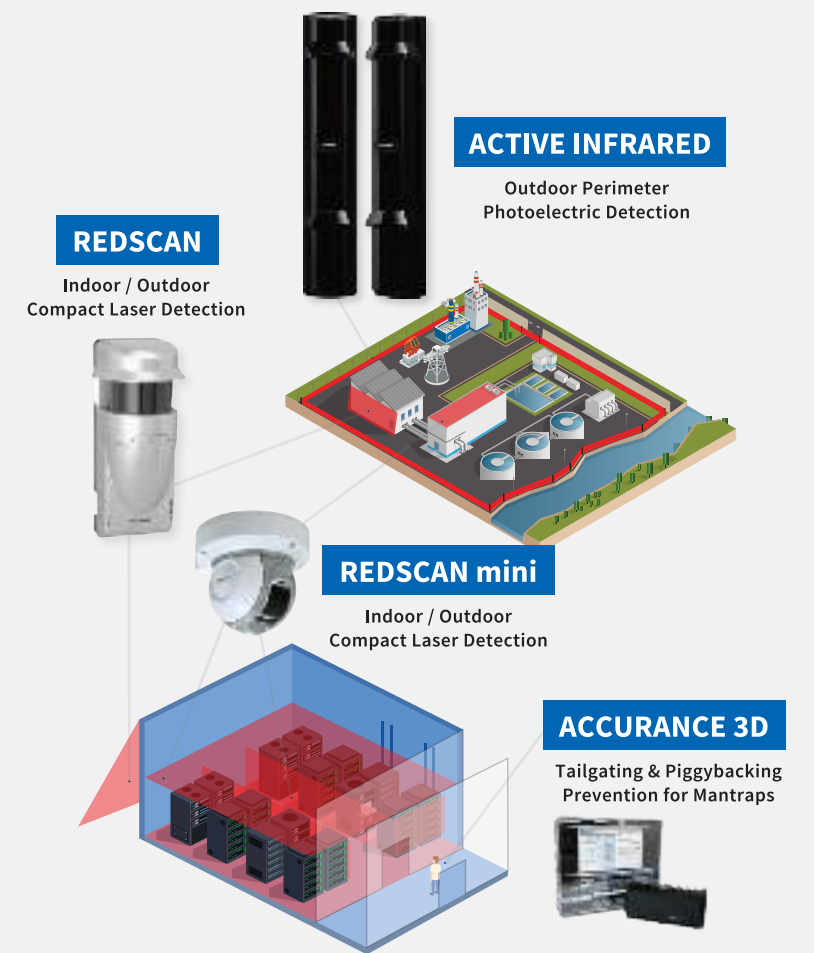
[linkedin.com/company/optex](https://linkedin.com/company/optex)



**THE WORLD LEADER IN SENSING SOLUTIONS.**

With indoor and outdoor detection solutions for every threat level, OPTEX sensors provide flexibility, performance, and guaranteed reliability. With almost 40 years of experience and over 25 companies in our global portfolio, OPTEX has established a worldwide reputation for quality, innovation, and technical excellence.

For Outdoor Perimeter Security, Indoor High-End Asset Protection, & Loss Prevention Applications





# DOYLE SECURITY SERVICES, INC.

At Your Service in  
New York, New Jersey & Pennsylvania

**PROTECTING YOUR PEOPLE, YOUR PROPERTY AND YOUR PEACE OF MIND.**



*Security Officer  
Services*

—

*Event & Life  
Safety Services*

—



*Executive Protection  
Services*

—

*Remote Monitoring  
Services*

—



*Mobile Guarding  
Services*

—

*Security Consulting  
Services*

