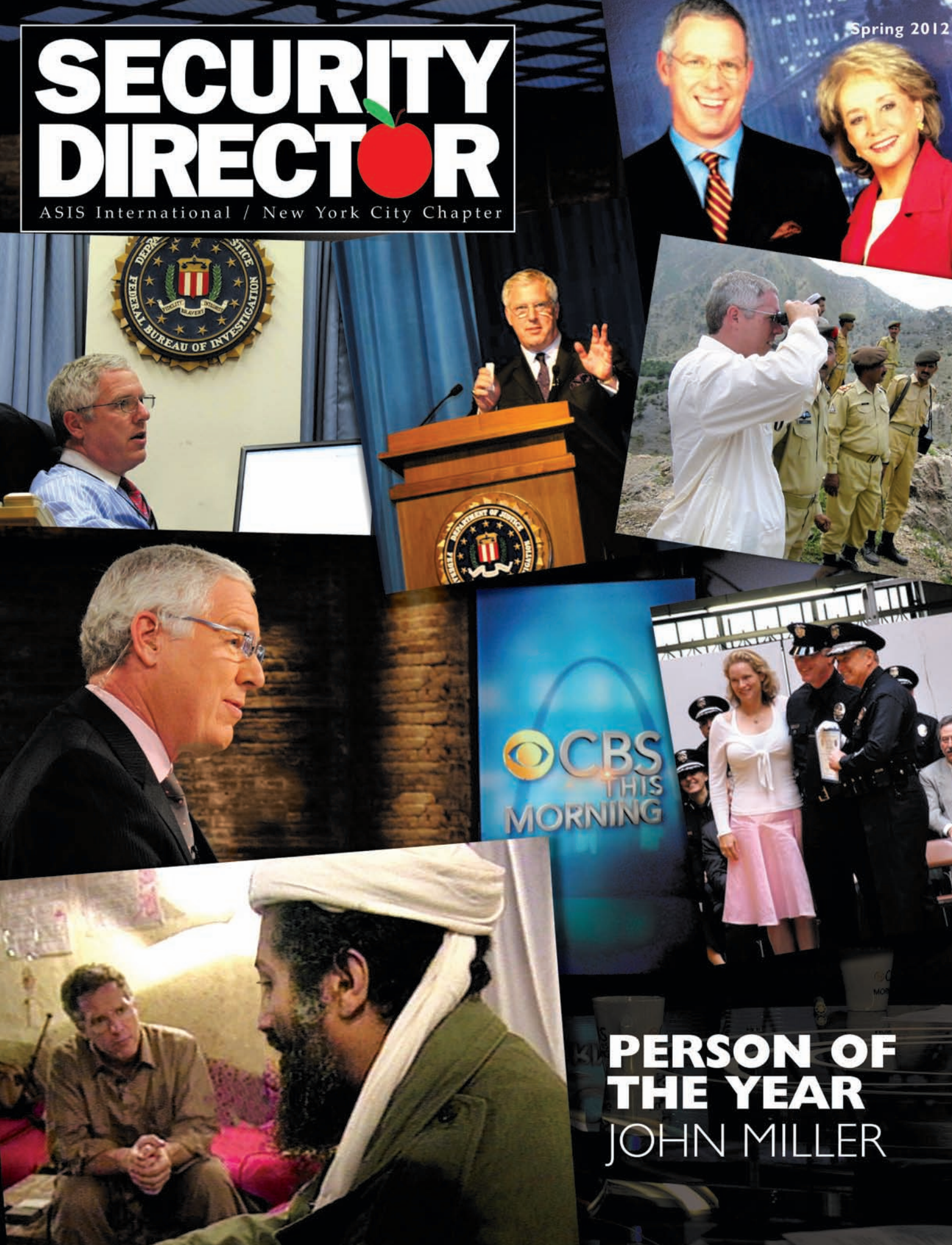
SECURITY DIRECTOR

ASIS International / New York City Chapter

Spring 2012



PERSON OF THE YEAR

JOHN MILLER

We started out in the guard business. How things have evolved.

Founded over 30 years ago, T&M today is a provider of premium security and investigative services worldwide.

- Security Consulting Services
- Executive Protection
- Security Officer Services
- Data Forensics & Information Security
- Technical Security Solutions
- Private Investigations
- Corporate Investigations
- Sexual Misconduct Consulting & Investigations
- Threat & Vulnerability Assessments
- Secure Transportation Services
- Special Event Security
- T&M Guardian
- Technical Surveillance Countermeasures
- Background Investigations & Due Diligence
- T&M Command Center

T&M Protection Resources

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

Visit us at
ASIS NYC
Booth
#225

THE BEST
KEEPS GETTING BETTER

STANLEY CSS IS GROWING TO SERVE YOU BETTER. Powered by a culture of continuous innovation, we're always looking to build on our industry-leading customer experience. That's why we're proud to announce the acquisitions of Niscayah and Microtec – an unmatched combination of leading-edge technology and customer service excellence. And we're expanding our reach with even more locations across North America, all with our signature local touch approach to doing business. At Stanley CSS, we're protecting what's important to you – now, better than ever before.

COMPLETE CUSTOMER TRANSPARENCY ■ SYSTEMS INTEGRATION ■ MARKET SOLUTIONS ■ BILINGUAL ULC MONITORING ■ eSERVICES

STANLEY®
Security Solutions

1-855-5-STANLEY
www.stanleycss.com

MICROTEC SECURITY SYSTEMS
NISCAYAH

Visit www.stanleycss.com/licenses.html for licensing information.

SERVICE EXCELLENCE

is Our Most Important Job

At U.S. Security Associates, our mandate is to provide service excellence every day of the year to the clients we serve. *We'll stop at nothing less.*

- Uniformed security officer services
- Loss prevention
- Background screening
- Training
- ISO 9001:2008-certified nationwide
- One of the world's top training companies (ASTD)
- Top 125 Training Company 2007–11 by *Training* magazine

Call us. We'll show you how we can improve your security.

1400 Broadway
Suite 2312
New York, NY 10018
212-867-7500

1560 Broadway
Suite 1209
New York, NY 10036
212-391-6957

550 W. Old Country Rd.
Suite 307
Hicksville, NY 11801
516-822-3800

26 Court Street
Suite 904
Brooklyn, NY 11242
718-855-0900

7–11 South Broadway
Suite 400
White Plains, NY 10601
914-761-7077

U. S. SECURITY ASSOCIATES

1-866-735-9418 • www.ussecurityassociates.com

COUNT ON US

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.

SECURITY DIRECTOR

ASIS International / New York City Chapter

CONTENTS

Uncover the hidden lies in security guard company proposals

We're the master of one trade - engineering Requests for Proposals (RFP) and a selection process that helps building managers choose the best-in-class security contractors for their guarding needs.

We add real value - help you cut the wheat from the chaff. With almost three decades of "insider" eyes of experience on the contractor side of the "fence" at the local, national, and international levels, we focus on the selection of ethical, worthy security contractors. We fine tune established RFPs for large corporations and improve their selection process. We extend personalized support to small organizations and stand-alone properties through our custom made RFPs, process guidance, and a security contract adaptable to their needs.

We add real value - help you avoid entering into contractual marriage with unethical or incompetent security contractors. Underperformance by your security guard contractor exposes the loopholes in your RFP process. Get the optimal security guard program that you deserve.

We add real value - help you assess the high cost of legal divorce hidden within contracts designed by security companies. Lowest cost is not identical with buying the best value. We save you from such potential traps and help you sort the "hype and fluff" proposals from the ones that have integrity, reliability, and competency as their backbone.

We add real value - help you recognize manipulative, empty proposal lingo and false incentives offered by profit-driven security contractors. With our experience and expertise, your RFP and selection process will be on track to hire security guard contractors that deliver what they promise. Why take a risk? Make the right choice.

RFP Security Services is led by owner Richard Baranowski, an accomplished executive, highly motivated and focused. He is polished and professional, driven by an intense propensity to succeed, to connect with people at their level, to gain their trust and confidence. He is at the very pinnacle of the who's who in the security industry in North America. I have worked with him on highly complex security proposals and was astounded by the depth of his knowledge, his attention to detail and relentless drive for perfection. I recommend Richard with no reservation to anyone needing the best in the business to help them with their physical security needs.

- Luc Ferland, Authorized Crestcom Licensee

RFP Security Services

The RFP specialists

Contact us at: RB@RFPsecurityservices.com
or visit our web site: www.RFPsecurityservices.com

ASIS International
New York City Chapter

Elected Officers

Chairman
Kevin O'Brien, CPP
Deutsche Bank
212-250-1699
Chairman@asisnyc.org

Chapter Vice Chairman
George Anderson
AlliedBarton Security Services
212.328.0133
George.Anderson@alliedbarton.com

Treasurer
Craig Schwab, CPP
Deutsche Bank
212-250-5719
craig.schwab@db.com

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

Advisory Board

Lawrence F. Loesch, CPP
lfloesch1@yahoo.com
(646) 831-4868

Raymond L. Dean, CPP
Stanley Convergent Security Solutions
718-937-0500
ray.dean@niscayah.us

Robert Ildefonso
718-916-9872
bobildefonso@msn.com

Patrick W. Kelly
Global Corp. Security Services
917-754-5953
patrick.w.kelly@verizon.net

Donald J. McGuire, CPP
914-329-1412
mcghome1@comcast.net

Wallace F. Millard
Millard Associates, LTD
718-225-8825
wally1415@aol.com

John C. O'Reilly, CPP
917-882-4548
rdny1077@gmail.com

Charles L. Scholl, CPP
Professional Security Guard Academy
845-825-9905
prosecguardacademy@yahoo.com

Joseph A. Spillane, CPP
914-771-9134

Sergeant at Arms
Kenneth McGuire
Michael Stapleton Associates
201-407-0154
kmcguire@mikestapleton.com

Luncheon Reservations
Richard Lieberman
WW Grainger
917-921-6300
rlieberman6@nyc.rr.com

Committee Chairs/Co-Chairs

CPP Continuing Education
Craig Schwab, CPP
Deutsche Bank
212-250-5719
craig.schwab@db.com

Law Enforcement Liaison
Patrick E. Kelleher
917-855-6876
ret1dc@yahoo.com

Chip Smith
Bank of New York Mellon
(212) 298-1322
chip.smith@bnymellon.com

Legislative Council Rep.
Michael McCann
McCann Protective Services
212-277-9623
mccann@mccannprotectiveservices.com

Program Chairs/Committee
Donald J. McGuire, CPP
914-329-1412
mcghome1@comcast.net

Keith Mulcahy
Michael Stapleton Associates
212-509-1336 x 235
keithmulcahy@mikestapleton.com

Kenneth McGuire
Michael Stapleton Associates
201-407-0154
kmcguire@mikestapleton.com

Don Francisco
Advanced Electronic Solutions, Inc.
374-386-2146
dfrancisco@nyaes.com

Trade Show Chairman
Raymond L. Dean, CPP
Stanley Convergent Security Solutions
718-937-0500
ray.dean@niscayah.us

Chapter Information Officer
Rich Patti, CISSP
Comtek Solutions
856-424-1223
rich@asisnyc.org

Placement
Erica D. Barr-Harrison, CPP
Aims Testing, Inc.
631-331-6001
erica.harrison@gmail.com

Don Francisco
Advanced Electronic Solutions, Inc.
374-386-2146
dfrancisco@nyaes.com

Membership
Andrew Turk
Turk Technologies, LLC
516-520-8875
andrewturk@turktechnologies.com

Regional Leadership

Senior Vice President
ASIS Region XVII
Joseph N. Masciocco
Security Integrations
518-452-3505
joem@securityintegrations.com

Vice President
ASIS Region XVII
Mario J. Doyle, CPP
Integratas
212-710-7880
mdoyle@integratas.com

Security Director Design
Don Blauweiss Advertising & Design
don@blauweissadvertising.com

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-III 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 III. He is also an ASIS International Board Certified Professional.

SAFEGUARDS INTERNATIONAL, INC.
Crisis planning and security. Play it safe.
914.771.9739 ▪ www.safeguardsintl.com

From The Editor's Desk

High Risk
High Stakes
High Technology
High Security!

When we set that as the theme for this unique 22nd ASIS International NYC Chapter's Security Expo, I didn't know what you'd choose to write about for *Security Director Magazine.* There were surprises!

Great phrases came from your writing, your phone calls and emails: statements that required rethinking how we deliver high security: "I pay for a room full of strategists… I get a room full of tacticians"; "When you hire [good] people to work for you, they deserve a great boss." High technology electronics designers floored me with terminology I'd never heard before and experts suggested how we can get our constituents to "take the blinders off" when it comes to risks presented by social media. Challenges came from younger professionals who were in private security and striving to enter law enforcement or working in the field now, before becoming attorneys.

Is there room in this magazine for everything we received? No, but the great material will not go to waste. The next issue of *Security Directions eMagazine* later this spring will have an abundance of hard-hitting articles and follow-ups to material that starts here in this magazine. Not yet a *Security Directions* subscriber? It's free! Get registered by dropping an email to me at: erica.harrison@gmail.com.

While you are browsing this colorful, information-rich issue of *Security Director Magazine* and checking information about the 2-day show and all the products and services highlighted on our pages, also read John Miller's article (he's our Person of the Year being honored at the April 26th Luncheon). You'll come away with some new insights into how his successful career spans the communications industry and law enforcement, and how his unique gifts and considerable talent bring benefits to both.

Certainly, we'd be out of touch to avoid addressing corporate security and the "Occupy" or similar movements whose focus is causing disruptions or worse. This topic isn't going away, so it will pay to have a multi-pronged approach for your facilities and personnel. People will be dealing with the products of unrest here and abroad while economies remain in turmoil world-wide.

Sometimes I have to be dragged screaming and cursing into new technologies, before I "get it." An example: If you haven't tried Google Voice, you are missing something extraordinary that blends traditional phone service with programs that translate your voicemails into [understandable] emails and screens your calls automatically! Who knew... and the service is free… Yes, all my data is being tracked and collected everywhere I go on the web and you can see my house from a satellite… but that's sort of old isn't it?

As always, I welcome your input and couldn't do any of this work without you. So, keep me on my toes for the coming year and surprise me with all the exciting developments that keep our industry thriving.

Remember if you haven't subscribed [free] to the *eMagazine, Security Directions*, now is the time to do it. And if you don't get Action Digest, you are missing all the free and low cost training announcements that can help you remain prepared all year long.

Drop me an email at: erica.harrison@gmail.com.

Now is a great time.

Erica

Karen Williams | Site Supervisor

Focus | Partnership

Great security means staying a step ahead.

AlliedBarton Site Supervisor Karen Williams understands the unique needs of management and tenants. As an active partner in day-to-day operations, she responds to changing situations and brings suggestions to enhance the security program.

Providing solutions. A part of your team.

ALLIEDBARTON® SECURITY SERVICES

Local Response | National Support

THE MOST HONORED SECURITY OFFICER SERVICES COMPANY®

CHAIRMAN'S MESSAGE

Kevin O'Brien

George Anderson

Dear Members,

This is perhaps the most exciting change that we have been able to bring you in terms of annual security expositions and seminar programs. By partnering with ASIS International's headquarters organization, we present for you a full 2-day exposition program focused on delivering enough security-intense information that you will walk away with: plenty of continuing education credits, information on new products and services that are just hitting the market and easy to learn about in the Exhibit Hall. Networking opportunities abound on an expanded scale —It's all unprecedented in our chapter's history and you will not want to miss the afternoon cocktail receptions both days in the Exhibit Hall.

If you recall in the editorial page last year, we mentioned that change was at hand. Sometimes, to keep us moving forward we alter older operating paradigms so we can better serve you, grow the chapter and take into account the new realities that the economic upheaval of the last several years has delivered to our industry and the country. We welcome your comments about this event and will work to keep improving what we do for you.

Our Person of the Year Luncheon honoring John Miller on Thursday, April 26 is something not to be missed. John is a rarity — combining a long, noteworthy law enforcement career with outstanding journalist credentials. His commentaries and presentations bring an insight and balance that make his material compelling and valuable. John began his news career in New York City and now, after success in all venues, he's returned to our locale. This is a 'be there' POY celebration.

Please review the entire show schedule, *Security Director Magazine,* information about certification review courses taking place right here in NYC on April 27 and 28th , and maybe it's not too late to give a call to some of your associates who haven't yet registered to attend. The booths are open all day.

You will see George here for the Show, to greet and meet everyone. Unfortunately I am on business out of the country, but looking forward to catching up with everyone in May.

Enjoy SECURITY EXPO 2012 from ASIS International's NYC Chapter in coordination with ASIS International!

Sincerely,

Kevin O'Brien,
NYC Chapter Chairman

George Anderson
NYC Chapter Vice Chairman

Richard Patti

Richard G. Patti CISSP, Information Officer for ASIS International NYC Chapter, has been instrumental in moving much of our communication to the internet. He's spearheaded our chapter's website enrichment so that we have a valuable method of sharing the newest information and updates with membership and interested security professionals around the world.

In selecting Rich Patti as our Eugene Casey Award winner, we are recognizing the importance that digital information plays in our daily lives. His depth of experience in managing digital content has been significant in ensuring that ASIS NYC Chapter is able to present well designed and accurate material for all who view our webpage and digital communications.

Rich is also a member of the NYC Chapter tradeshow committee that produces the annual NYC Security Expo at the Javits Conference Center.

Starting in engineering with NY Telephone, Rich has enjoyed a diverse career in marketing, business development and product engineering with several technology companies. He is currently a Director at Comtek Solutions specializing in information security for the financial services industry.

He has also served as VP of Marketing for SightLogix, the manufacturer of one of the first intelligent video surveillance cameras for outdoor security. He has also served as VP of Marketing & Business Development for LuxN Corporation, a manufacturer of fiber optic communications equipment. Rich was a pioneer in data networking, participating in the early development of several IEEE 802 network standards which are the basis for many of today's communications networks.

Rich grew up in Brooklyn, NY and received his BSEE at Manhattan College and a MSEM at Drexel University. He is an active member of ASIS and holds a CISSP certification in information security.

John Miller

John Miller, our Person of the Year, has a distinguished career working in both the law enforcement community and in television journalism. As a correspondent and author, John's skill communicating complex and sensitive information along with a global understanding of serious challenges we face this century, makes him an invaluable contributor to our industry and an authoritative voice bringing in-depth analysis to critical news issues.

John Miller was named a senior correspondent for CBS News on Oct. 17, 2011. In this capacity, Miller reports for all CBS News platforms and broadcasts, including "CBS This Morning" and occasionally for "60 Minutes."

Beginning in 2005, Miller served in the Office of the Director of National Intelligence, ending his tour as Deputy Director of the Analysis Division. John worked across the Intelligence Community with the CIA, NSA, FBI, and other agencies.

Before joining the FBI, he served from 2003 to 2005 as head of the Counterterrorism and Criminal Intelligence Bureau and the Major Crimes Division of the Los Angeles Police Department, overseeing both LAPD's Major Crimes Division, Hazardous Materials Unit and its Bomb Squad.

In 2002, Miller, along with co-authors Michael Stone and Chris Mitchell, wrote "The Cell: Inside the 9/11 Plot," and "Why the FBI and CIA Failed to Stop It," an investigation into the September 11 attacks, that drew on relationships developed with intelligence and law enforcement officers in the many years he spent as a journalist covering Al Qaeda as it grew into a global terrorist operation.

From 1995 to 2002, Miller was an ABC news correspondent. In 2002, he became co-anchor of the ABC news broadcast "20/20."

In 1998, he secured an on-camera interview with Osama bin Laden. His diligent investigative reporting over his career earned him nine Emmy Awards, two Peabody Awards, and an Alfred I. DuPont-Columbia Award.

Miller served briefly as New York City Deputy Police Commissioner from 1994-1995, after working as a television journalist at various networks and television stations from 1973 to 1994.

TOUGH QUESTIONS INSIGHTFUL ANSWERS

Our Person of the Year, John Miller, was kind enough to let us ask some tough questions and he took the time to deliver insightful answers. EDH

How is your television audience different today than say, in the 70s when you first were broadcasting in NYC?

When I started out in television in the 70s, most people got there news from morning papers and then at the end of the day from evening news broadcasts.Today, it is a very different audience. They get their morning news from TV shows like CBS This Morning while they get dressed. Then they see it on the internet; news alerts pushed to their phones and images on YouTube and flashes on Twitter and of course, the 24 hour cable shows that play in many offices all day. By the time they get to the evening news, you better have something original, or just plain smarter than what they've been hearing all day. That's one of the great things about CBS This Morning. We are getting the first crack at it at 7:00 AM.

Since you are presenting more complex and in-depth reports than just a typical newscast, what are some of the approaches you've taken to getting so much information to people and still keeping the delivery compelling?

The great, late, Don Hewitt who pretty much invented "60 Minutes" said it all boils down to four little words that we all learn as children: "Tell me a story". What Don meant was, if the story is a good story, if the characters are interesting, it won't need all the bells and whistles that today's TV sometimes adds to the point of distraction. I always say the secret to success is to find a villain, find a victim and find a hero — preferably in the same story, and you can't go wrong. So, in the end, how long it is, how complex it is will be trumped, if you have picked the right tale to tell.

Recently, Bill Bratton has been emphasizing the need for collaboration between the law enforcement community, the public and the private sector. Could you elaborate about how that approach was incorporated into your work with him in Los Angeles?

Commissioner Bratton's new book, with Harvard's Zach Tumin actually has a chapter about what it took to open the Los Angeles Joint Regional Intelligence Center (or, J-RIC, as it's called). It meant getting the LAPD, LA County Sheriffs, the FBI and the 44 LA County police chiefs to agree on where to locate the center, who should be in-charge and how to make that all happen from five different finding streams. It stated out pretty rough. Everyone's first take was that they should be in charge, and handle the money and locate the center in their shop. It took a lot of negotiating but the key was not forgetting the real goal: The success of the intelligence fusion center had little to do with who ran it or handled the money and everything to do with how good the intelligence coming out of it would be. At the time — this was not long after 9/11 — there was a real gap between the intelligence the feds had, and how that translated to what the state and local police needed to do their jobs. The chapter on the making of the J-RIC in Bratton's book is a great example of how much you can get done when the driving force is collaboration and not who gets credit.

As a recognized spokesman and public relations leader in the television journalism and in the various aspects of law enforcement, you've had significant accomplishments. Could you share how you've met some of the daunting challenges such as bringing data tracking and accountability to the various agencies where you've worked? What are the challenges you've considered most significant? [in any aspect of your work]

My first job at the Office of the Director of National Intelligence was Analytic Transformation and Technology. That job was all about developing systems and policies that would allow analysts from 16 different intelligence agencies to collaborate. Should a warfighter in Afghanistan or a policymaker in the White House have to read 19 pieces of analysis from different agencies to understand a problem? Were the analysts working together? Did they have access to the same intel? The answer was mod often, "no". The ODNI has made some improvements, but in a town where information is power, there is still a ways to go on collaboration. Even 10 years after 9/11.

At the FBI, the problem was the sheer scope of the place. We had 56 field offices spread across the country and twenty different divisions at headquarters. Trying to bring change both in process and in policy to meet the needs of a post 9/11 world offered a unique set of challenges. How do you communicate that to the field? One thing I was able to add there, at Director Mueller's request was an internal communication unit. We tried to put as much effort and creativity into getting the right messages to our employees as we did with the public. In the end, we adapted a tool from the NYPD (and Bratton): COMPSTAT. Now the Director has the FBI divided into regions and once a month, the Special Agents in Charge (SACs) find themselves on the other end of a classified video conference looking at the screen and seeing the Director. The Director wants to know, one SAC at a time, (1. What are your top known threats in your region? (2: How did you determine those threats and prioritize them? (3: Now, tell me your strategy to deal with those threats. Getting a COMPSTAT-like process into the Bureau has been very useful.

As you've reached out to the Muslim community, are there some issues you see that have not received the attention or publicity they require?

I think the Muslim community has struggled in many ways, especially since 9/11. It's struggled to achieve an identity as an American community, not a community apart. One of the stories that has not received enough attention is just how much effort police agencies and the FBI have put into some very skilled outreach efforts to the Arab, Muslim and Sikh communities across the nation. It's a "good news" story, so it tends to get buried but it is community policing at its best.

Our thanks to John Miller, ASIS International NYC Chapter's Person of the Year.

HIGH RISK, HIGH STAKES, HIGH TECHNOLOGY... HIGH SECURITY!

What has high technology done for you lately? Possibly it's been critical in your security work or it may simply make some tasks easier to manage. For many, it's meant: newer, faster, more complicated.

Our contributing writers tackle different views on high risks, high technology and high security. You'll even find different views on similar situations. The same territory yields different information when seen through various perspectives.

What you'll read here will provide insights on everything from social engineering to port security; from searching attaché cases without touching them to "the internet of things "; from surviving an out-of-control protest to redefining "need to know " and even wearing 'better' technology! You won't be bored; you'll gain some new strategies to use and perhaps it will also inspire you to write about your area of expertise.

We didn't have space for all the contributions to this print edition of *Security Director Magazine* which is also ASIS NYC Chapter's Show Journal. But, the additional articles will be in your hands within the next months in the next *Security Directions e-Magazine*.

Last year, I started an independent e-publication: *Security Directions* (summer, fall and winter issues) so that you as security experts have a vehicle to reach your audience on a regular basis. Sign up for *Security Directions* e-magazines for free and use the opportunity to get your own work in print. Email me at: Erica.harrison@gmail.com. Meanwhile, please keep in touch even if it's with a string and two empty cans instead of the iPad 3!

Erica Harrison, CPP

STARTING POINT

By Andy Goldstone

The year is 1976 and it's where my story begins. Many of my current ASIS associates reading this, were either not yet born or not in the security workplace. (Of course, Joe Spillane, our former chapter chairman, then security director at Celanese, was always a favorite of vendors in the tech area.

I started that year as a salesperson for RUSCO Electronics, one of only 3 manufacturers in the ACCESS CONTROL market. It was before many of the inventions and innovations that help us supply high levels of passageway security, something we take for granted today in most of our facilities.

This was before HID, Wiegand and 'bit' structures… We were selling barium ferrite cards with a 5x8 matrix that contained the cards' encryption. My competitors were Schlage (where the focus was on proximity cards and readers) and Cardkey.

How different it was: although many buildouts were in the works for companies with significant assets, it wasn't a given that every new space would be outfitted with video surveillance or sophisticated access control. Organizations such as Con Edison, JCP&L, and Three Mile Island (the nuclear power plant) required what was 'high-tech' access control at the time. Other new prospects were few and far between. I had to physically demonstrate this "new" technology. So there I was, walking up and down the streets of Manhattan with three large cases, filled with card readers, a controller, a [big] printer and all the connecting cables so I could show how the equipment really worked. People were often amazed when I showed them how a card could work in DOOR 1; not in DOOR 2 and then could be programmed out of all 3 doors. This was sort of a 'mission impossible' presentation; some people still not believing that the system really worked.

Organizations such as Con Edison, JCP&L, and Three Mile Island required what was 'high-tech' access control at the time.

Data management centers were among the most likely new customers we'd come across. So, when I saw an ad in the New York Times for a data manager for Lone Star Industries, I called them up. "You must have a data center," I said, "and you need a 'CARD in LIEU of a KEY' to secure access and get a printed record of who comes in and when." Those were the "leads" of the day. Now, its 2012 and I am still doing the same… sans schlepping the cases.

Andy Goldstone is VP Strategic Sales for IDESCO Corporation and can be reached at: 800-336-1383 or by email at: a goldstone@idesco.com.

EMERGENCY PREPAREDNESS: 9/11, ELEVEN YEARS LATER

By Allan Schwartz, CPP

Eleven years later, as we reflect on the 9/11 tragedy we remember horrendous details… we were caught off guard by the unanticipated. Even when we've had some warning such as before Hurricanes Katrina and Irene, or prior to the earthquake and tsunami that devastated nuclear power facilities in Japan, it hasn't been enough.

Untested emergency plans just pulled out when the crisis is upon us, like loose-leaf binders filled with 'what to do and how to do it' instructions, are not going to offer the protection we need. Even in small disasters, (downed power lines and local flooding), than we have to strategize how we get buy-in and participation for crisis response and recovery.

Sometimes security practitioners are seen as worry-warts. Risk managers may not even agree to expend resources to prepare for a 'possibility' when there are so many realities calling for the same scarce dollars. Consider putting a 'dollars and cents' evaluation on what a catastrophe

continued on page 16

will cost if poorly met. The figures can be estimated with a little research and are worth the time expended.

Where IT departments are almost 'on automatic' with catastrophe response plans built into their system designs, we don't have the same expectation for organizations as a whole. It's High Risks and High Stakes when we cannot operate our businesses in normal mode. As security professionals we are acutely aware of related high costs associated with "down-times" and worse, loss of lives or total loss of facilities.

Surveys show that concerns about emergencies have been relegated to lesser importance. Perhaps it's the lagging economy or denial. Yet reality dictates that it is no longer a question of if you can expect a crisis, it's a matter of when one might occur.

It's High Risks and High Stakes when we cannot operate our businesses in normal mode.

Get out those written emergency plan and business response/recovery plans. Re-examine them with specialists who know your business. Update as necessary.

Be convincing in your work with management and actually do what the plans state.

Establish an emergency command center and a crisis management team that will activate the approved and tested plan in the event of a disaster. Work through the details over coffee, or at regular team meetings. Don't put it off.

Make training engaging for employees and staff. (They may never have paid attention to the plan's contents or implementation procedures.) Get buy-in and bring in specialists if you find that's what it takes to get their attention. Ask for feedback after periodic drills during the year so new issues can be addressed as they occur.

Has the contract for the off-site data center changed since last drill? Who checked the emergency generators last week? What factors are we adding into decisions about facility re-entry? How are we using cellular technology to assist us now that we have a new service provider? What backs us up if the cell service or radio service fails?

Get tested emergency preparedness plans that deal with emergencies of all proportions. Our lives and our livelihoods probably depend on it.

Allan Schwartz, CPP, CHS-III *is president of Safeguards International, Inc in Yonkers NY. He can be reached at: 914-771-9739 or at: safetrak3@aol.com.*

HIGH TECH GETS UP CLOSE AND PERSONAL

By Dan Mendelson

When we think of technology, we often think about tangible devices we can feel and touch — computers, tablets, and iPhones. But technology now plays a role even in security uniforms, though it's not as readily apparent. New shirt fiber blends that have wicking properties similar to workout gear help the wearer remain dry and professional looking even in hot, humid environments.

For security managers who have officers in critical high temperature environments, such as at loading docks or on

exterior patrols during the summer, keeping them comfortable can make a measurable difference in performance. In a recent study nearly 2/3 of respondents complained that typical tasks can take up to 25% longer under excessively warm conditions.

Technology now plays a role even in security uniforms, though it's not as readily apparent.

Now, there are several uniform garments that help alleviate heat-related issues without breaking operational budgets. 5.11 Tactical has incorporated these advances in a number of their products.

Patrol Duty Uniform (PDU)

PDU's are traditional formal uniforms that now in a blend of 65/35 poly-cotton, can be functional and comfortable. The garments are treated with Teflon® for stain and soil resistance and don't fade as easily as other garments.

Built-in features combine comfort, utility and safety. Shirts have bi-swing shoulders for freedom of movement. The flat-front styling and permanent creases on the pants make them professional-looking. But what makes them most durable is the diamond-gusseted crotch — they'll last longer without the seams busting up, cutting down your replacement costs. And when these uniforms are dirty, employees can wash them rather than requiring dry cleaning. That can add up to measurable cost savings each year.

Stryke Pant with Flex-Tac™ and Performance Polo

In locations where officers can wear less traditional, "softer" uniforms, pants made with Flex-Tac™ a proprietary product that has a 'cotton-like' feel, can be a good solution. They're lighter weight, stretchable without spandex, breathable and comfortable for full shifts of tough work in warm locales. Like the PDU, the Stryke Pant is soil, stain and fade resistant, and comes out of the wash ready-to-wear.

When a full button shirt is not required, the Performance Polo offers a useful alternative. The shirt fabric is moisture wicking, fast drying and keeps the wearer cooler. It's also antimicrobial, preventing the growth of odor causing bacteria. You can reinforce your brand by adding an embroidered logo that increases visibility and boosts image.

Nowadays, there's no need to get hot and bothered by a rise in temperature. There are numerous products on the market that keep employees cool and comfortable, reducing risks of heat-related illnesses and lost productivity. And they're available at many price points. Talk with your uniform supplier to find the garments that are right for you.

Dan Mendelson *is president of Unitex Direct — a national uniform provider for the contract security market. He's a former treasurer of ASIS International Detroit Chapter. Reach him at: 800-682-1606 x 230 or at: dan@unitexdirect.com.*

NINE CAREER RISKS YOU CAN MANAGE — NOW!

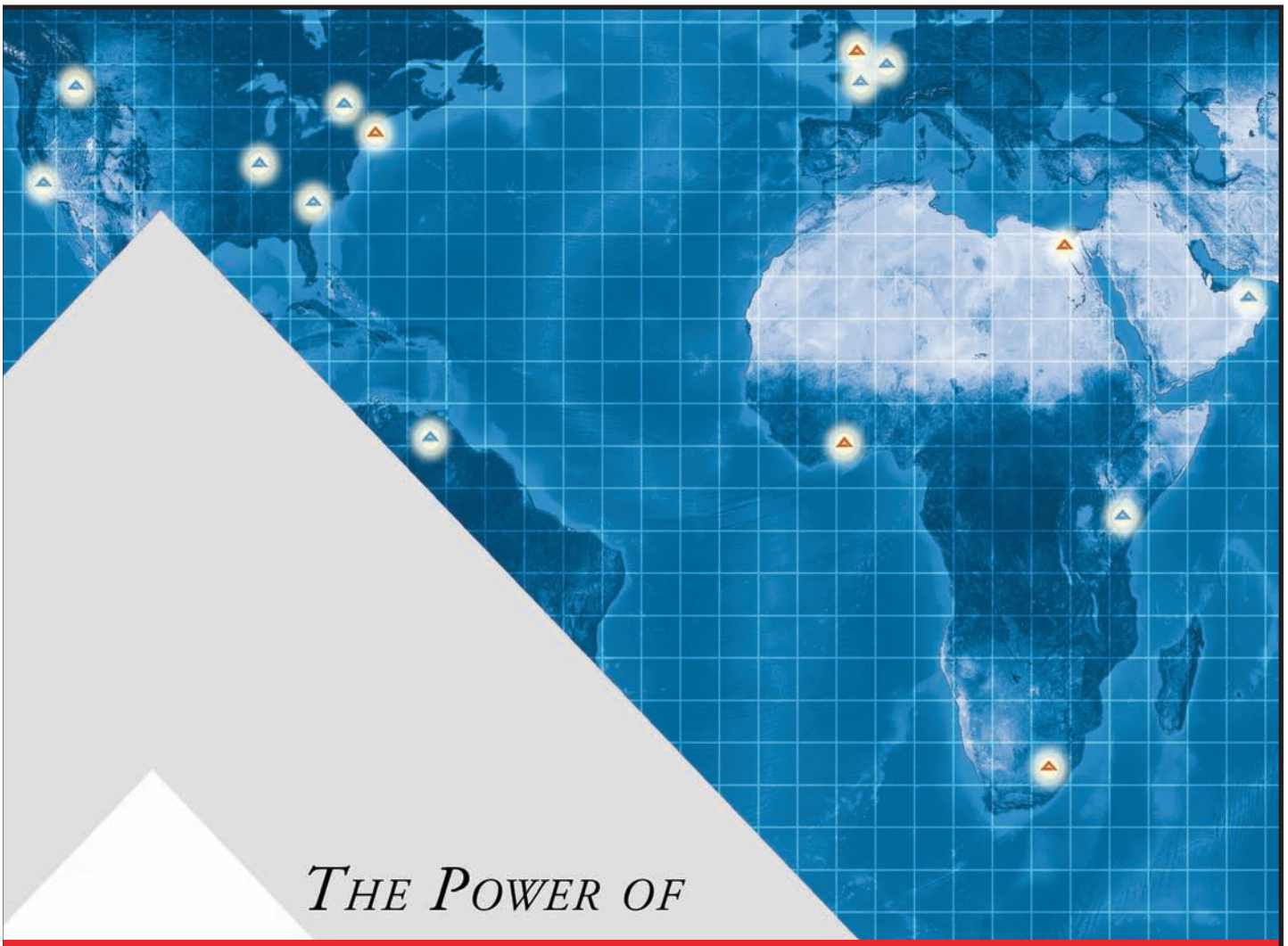
By Kathy Lavinder

Security managers are expected to be proactive, anticipating threats and managing risks. It's beneficial to apply the same approach to security practitioners' careers. Here are nine career risks for every proactive security manager to keep in mind:

1) Leaving too soon. When the economy was robust, frequent job changes were not always an issue. Now employers are placing a premium on loyalty and prefer individuals who have demonstrated commitment, seeing things through to completion.

2) Moving simply for more money. Money is a powerful lure, but making a career move just to see a bump in compensation may be disappointing or worse. Let your new role offer long term professional challenges and a compatible environment. Today the cliché "look before you leap" is a truth.

continued on page 19



The Power of

Personal Service

QUALIFIED UNIFORMED SECURITY SERVICES

INVESTIGATIONS

EXECUTIVE PROTECTION

SECURITY CONSULTING & PLANNING

APOLLOSECURITY®

A Tradition of Quality℠

212.742.8600

www.apollosecurity.com

LOCAL, REGIONAL, NATIONAL & INTERNATIONAL CAPABILITIES

3) The opposite: staying too long and getting too comfortable is not a better strategy. "Retiring in place" can be risky. Employers want maximum productivity and a positive return on investment. Being closed-off or unreceptive to new opportunities can be equally short-sighted.

A broad overview is good sometimes, but we live and work in an age of specialization.

4) Being unprepared. There's significant volatility in both the public and private sectors. Governments keep trimming and companies continue to pare costs. Have your parachute packed and ready to go. Polish up the resume and keep a recruiter's business card in your back pocket.

5) Letting your professional network languish. Most positions are filled though networking. Even if you're not looking for a new job now, don't ignore networking opportunities. You'll pick up useful Intel, discern industry trends, and probably hear what the competition is doing.

6) Having last century's approach to security. Security has moved way beyond guards, gates, and guns. The intersection of physical and information security is key to what's happening today.

7) Being a generalist. A broad overview is good — sometimes, but we live and work in an age of specialization. Develop expertise in specific areas of security — especially those that can serve your employer. If you aren't learning something new, you are falling behind.

8) Releasing too much information. Over sharing on LinkedIn, Facebook, Twitter, and other social media sites can be perilous. Think before you post; you never know who is paying attention.

9) Reputational risks. The top end of the security industry is actually a small, tight-knit group; don't burn any bridges.

Kathy Lavinder *is Executive Director of Security & Investigative Placement Consultants LLC, a retained recruiting firm specializing in placing security management professionals. Kathy can be reached at: klavinder@siplacement.com.*

CRITICAL INFRASTRUCTURE PROTECTION

By Erik O. Ronningen

Do you know those 60,000 people coming through the gate?

"How are you protecting your critical infrastructure?" was the question posed six months post 9/11 by every regional transportation agency security director and law enforcement command in the New York City metropolitan area.

Imagine an executive conference room filled with smartly attired executives and four star Police Chiefs, and see each individual privately shrug his answer of uncertainty. The question did not refer to perimeter fencing

and CCTV, but rather, "How are we evaluating the character of an individual to assure a safe

continued on page 21

Century Protective Services Inc.

Security & Risk Management

WWW.CENTURYPROTECTIVE.COM

- PROFESSIONAL SECURITY AGENTS
- FIRE SAFETY DIRECTORS
- CONCIERGE AND MAILROOM PERSONNEL
- COMMAND CENTER OPERATORS
- EXECUTIVE PROTECTION SPECIALISTS
- PATROL VEHICLES
- TRAINING
- INVESTIGATIVE SERVICES
- PRE-EMPLOYMENT BACKGROUND SCREENING
- CONSULTING SERVICES
- ELECTRONIC SYSTEMS DESIGN
- PHYSICAL SECURITY ASSESSMENTS

CALL US TODAY FOR A FREE CONSULTATION

PHONE: 914 683 6100 FAX: 914 683 5608
150 GRAND STREET, WHITE PLAINS, NEW YORK 10601

NEW YORK · NEW JERSEY · CONNECTICUT

and threat-free environment?"

How indeed? How do you evaluate the character of an individual? Where do you start? What is the standard? What does it cost? Are there economies of scale? How do you get regional buy-in?

Due diligence provided the answers. A felony background screening answered the first question. Capitalizing on TSA requirements for access to secure areas of our nation's Class X airports and seaports, I standardized the felonies by taking the most stringent of 49CFR 1542.203 and 49CFR 1572.103. Economies of scale required a web-based system that shared a cleared member in real-time throughout the region at no additional cost to the end user. Regional buy-in came automatically as agencies realized the increased life safety, security, and risk management benefits this program brought to the World Trade Center Construction site and our airports, tunnels, bridges, terminals, and transit facilities.

After much sharing of information with other transportation agencies, and writing a concept of operations, I wrote a publically advertised Request for Proposal (RFP). From 29 respondents, the selection committee awarded the contract, which the Port Authority of New York and New Jersey Board of Commissioners approved.

Secure Worker Access Consortium (SWAC) became the critical infrastructure protection personnel assurance and credentialing program that provides a high degree of assurance of the security threat on individuals requiring access to designated secure areas of critical infrastructure.

Beginning our sixth year of operation, enrollment exceeds 60,000 members, 2,500 companies, and buy-in from the majority of the New York/New Jersey local labor unions. The Metropolitan Transportation Authority (MTA), New Jersey Transit (NJT), New York State Thruway Authority, New Jersey Turnpike Authority, and other public and private sector stakeholders are sharing in this community of trusted members, each capitalizing on the economies of scale this program brings to the region.

This program has gained national recognition from DHS, TSA, and most recently by the FBI. With the integration of the Transportation Worker Identification Credential (TWIC), our Personnel Assurance Critical Infrastructure Protection Program has been proofed-out to be truly multimodal in scope and application in the New York/New Jersey regional transportation sector. Next steps are to address and integrate the National Infrastructure Protection Plan (NIPP). With the award of a U.S. Government grant to supplement this program, this scalable, regionally managed and controlled program — the largest with Federal endorsement and support — is positioned to set a national model for personnel assurance and due diligence in the private/public sector.

Erik O. Ronningen *is the Personnel Assurance Program Manager for the Port Authority of New York & New Jersey, Office of Emergency Management. Reach Erik at: eronning@panynj.gov.*

SECURING AMERICA'S SEAPORTS — ONE MINUTE AT A TIME

By Robert Dunn, URS New York and James Gregory, URS Seattle

This last decade, seaport security has become far more sophisticated as we work to prevent terrorism and criminal activity. The stakes are high and so is the security.

With new technology and specially designed electronic systems, what once required a huge staff to screen vehicles and containers entering/leaving ports, can now be accomplished

Seaport security has become far more sophisticated as we work to prevent terrorism and criminal activity.

continued on page 23

INCIDENT MANAGEMENT
FROM EVERY ANGLE.

Dispatch Officers.
Report Incidents.
Manage Investigations.
Spot Trends.
Deliver Metrics.

Software for all your Incident Reporting and Investigation Management needs.

Perspective™
by PPM 2000

Discover Perspective by PPM 2000 at ASIS NYC Booth #411.

When you think 'Incident Management'—think PPM. **PPM 2000 Inc. 1-888-776-9776 www.ppm2000.com**

digitally at gated access points in under a minute per vehicle. Further, the best engineered systems can support information sharing with government and municipal systems to augment efforts to prevent raw materials for weapons of mass destruction and high value cargo from falling into unauthorized hands.

Expertly designed systems have benefited container terminals by streamlining the flow of vehicles and containers while taking a multi-pronged approach to gathering data to help detect fraud, theft and unauthorized access as it happens. In addition modern terminal gates mitigate incidents and reduce truck idling time, thus limiting associated emissions.

Our specialized gate components include: automatic Transportation Worker Identification Credential card readers to verify driver credentials entering the terminal; RFID readers and Automatic License Plate Recognition software to identify truck cab and trucking company, locate transaction, verify pre-filed transaction and appointment compliance; Optical Character Recognition software identifies container and chassis equipment and correlates with transactions; electronic container seal readers verify that container doors have not been breached; weigh-in-motion scales; radiation scanning (via Radiation Portal Monitors) and on-site container imaging identifies suspect cargo through the DHS Automatic Targeting System.

In our designs, everything identified through the gate-located systems gets monitored at a Security Command and Control Center which is tasked with managing port-wide security. The Center combines and displays surveillance and monitored data from all the port area facilities and the surrounding locale. Designed with leading-edge technology, it enables real-time information sharing among the Port's security partners at local, state and regional levels. The systems also provide controlled access to documentation, plans and other security-related information for use in vulnerability and consequence management drills and exercises.

A Joint-Agency Container Inspection Facility (JCIF) at another port uses our detection systems for hazardous materials including chemical, biological, explosive, radiological, and nuclear weapons (CBERN), plus a business model that self-sustaining. The design includes networks and interfaces between all of the location's container terminals, where currently more than 18 million TEUs (twenty-foot equivalent units) are handled annually.

A guard with a mirror on a long handle, checking under a truck's chassis and trailer's

continued on page 25

RADIANT
TRAINING & CONSULTING, LLC
PROTECTING YOU THROUGH EDUCATION

TRAINING SERVICES

NYS SECURITY GUARD LICENSE SERVICES
PRE-ASSIGNMENT SECURITY COURSES
ON-THE-JOB SECURITY COURSES
ANNUAL IN-SERVICE SECURITY COURSES
AMERICAN RED CROSS/CPR-AED
FIRE GUARD FOR IMPAIRMENTS F-01
FIRE SAFETY DIRECTOR F-58
EMERGENCY ACTION PLAN DIRECTOR F-59
BUILDING OPERATION RECERT FOR FSDs
FIRE SAFETY COORDINATOR F-24
SUPERVISION OF FIRE ALARM SYSTEMS S-95
EXCLUSIVE PRIVATE CLIENT TRAINING

CONSULTING SERVICES

FIRE SAFETY AND EVACUATION PLANS
EMERGENCY ACTION PLANS
BUILDING INFORMATION CARDS (BICs)
FLOOR PLANS PREPARED
FSD & EAPD ON-SITE PREPARATION
FIRE & EAP DRILLS
FIRE SAFETY & EAP STAFF TRAINING
FIRE SUPPRESSION SYSTEM RISER DIAGRAMS
FDNY PLAN EXPEDITORS
MANUALS AND LOG BOOKS

JOIN OUR IMPRESSIVE LIST OF CORPORATE CLIENTS

PROTECTION SERVICES:	T&M Protection Resources, FJC Security Services, Carney Security, Allegiance Protection, Harvard
MEDICAL CENTERS:	Maimonides Medical Center, Memorial Sloan-Kettering Cancer Center, Hospital for Special Surgery
NOT-FOR-PROFITS:	Women's Prison Association, Little Flower, Bay Family Center, Samaritan Village, The Bridge
HOSPITALITY SERVICES:	Novotel, Mansfield, Eventi, Hotel Chandler, Millenium Hilton, Gershwin, Shoreham, RoomMate
UNIVERSITIES/EDUCATION:	Long Island University – Brooklyn Campus, New York City Department of Education
PROPERTY MANAGEMENT:	Alma Realty Corp., Housing & Services, Inc., Shorenstein Properties, National Property Services
PRIVATE FIRMS:	Skadden Arps, Intrepid Museum, Church Pension Group, Beck Street Capital, Durst Organization
ORGANIZATIONS:	Metropolitan Club, International House, Jewish Community Center, VIP Community Services

We are committed to our mission to protect people from harm and property from loss through education

www.RadiantTrainingLLC.com

14 East 39th Street, 2nd Floor, Manhattan | 212-213-3434 | f: 212-213-3433 | info@radianttrainingllc.com

undercarriage might have been sufficient security measures last century. Today, we look at protection from a global perspective. We are incorporating the most advanced electronics and the most sophisticated analysis into the most rugged systems to withstand brutal salt water environments and 24/7 operating requirements.

The goal: to ensure that high security and high operational efficiency work hand in hand to keep port operations safe and profitable.

***Robert Dunn CPP** and **James Gregory** work at URS and can be reached through Robert at: 212-896-0279 and robert.dunn@urs.com.*

EMPLOYEE SAFETY IN PROTESTS AND CIVIL UNREST

By Steven Crimando

2012: Another Year of Mass Protests?

With significant high profile events throughout 2012, [the political conventions in Tampa and Charlotte, the G-8 in Chicago, and Summer Olympics in London] it's likely mass gatherings and demonstrations will grab headlines and present challenges for those charged with keeping facilities and personnel safe and secure.

Most protests are peaceful, but peaceful gatherings can be disruptive due to sheer numbers, even without the presence of agitators.

When organizational management and individual employees work together on mitigating hazards and developing feasible ways to reduce risk in crowd and mob situations, everyone benefits.

Organizational Safety

Whether it was responses to the

Occupy movement that disrupted lobbies and downtown environments across US cities, or dealing with dangerous "flash mobs/flash robs" where multiple-offender robberies were coordinated through Twitter, text and other social media, there were lessons learned.

Some useful ideas can be adopted by security leaders and decision-makers now including:

• Have a practiced plan for managing demonstrations and protests that target, or are nearby your facilities

• Develop a shared skill set for crowd management across all involved disciplines in your organization

• Coordinate plans and actions with local law enforcement and emergency management agencies

• Share information with the workforce about the nature and location of nearby protests, ways to reduce their risks, and resources to help them ensure their safety

Consider providing employees with updated neighborhood maps showing protestors' locations, alternate routes to and from their work site and specific information to help reduce chances they'll get caught up in crowds.

Individual Safety and Survival

Employees who navigate crowded streets or endure the taunts of protestors can benefit from some basic crowd safety advice and crowd survival information. This includes:

continued on page 27

CARNEY SECURITY SERVICE INC.

Quality Provider of

Uniformed Guards
Plainclothes Security
Fire Safety Directors
Investigators
Security Guard Training

Jeremiah J. Howard, Jr.
President
j.howard@carneysecurity.com

4 New York Plaza / New York / NY 10004
212.684.4888 / Fax: 212.684.1479

Safety

• Walk around, not through crowds

• Anticipate insults and taunts; Avoid taking the bait, remember it's not personal, and just keep moving

• Don't wear clothing or accessories that can become pulled or tangled in a tight crowd

• Wear shoes that will stay on and help you move fast if necessary. This means thinking twice when dressing before work, avoid high heels or loafers that can slip off or result in a twisted ankle. Double-knot laced shoes.

Most protests are peaceful, but peaceful gatherings can be disruptive due to sheer numbers, even without the presence of agitators.

• Avoid standing near temporary structures, like stages, that may collapse if overloaded. Don't stand against immovable objects, such as walls, doors or barriers, where you can become pinned.

Survival

In rare instances where crowds ignite into dangerous mobs, know what and what not to do. To survive a surging crowd or mob:

• Don't stand still or sit down. Stay on your feet and keep moving diagonally with the crowd, slowly pushing toward the outside where the flow is weaker.

• Try to maintain some "elbow room" around you to allow for free breathing and movement.

• If you drop something, unless it is critical, just leave it. Bending or squatting low to the ground can result in you being pushed down by the surge.

• If you are knocked down in a crowd, try to get back to your feet as quickly as possible. Don't be afraid to reach up and ask for help.

• If you can get up, crawl in the direction of the crowd until you sense a lull which may allow you to get back to your feet.

• If you can't crawl, duck and cover. Curl into a ball, back up, protecting your head and face with your arms and hands.

Recognizing a New Reality

Groups, crowds and mobs are likely to be a prominent part of the landscape for 2012. Preparing your organization and educating your workforce about risks and responses to mass gatherings can help minimize business disruptions and improve employee safety but as with all risks, the time to take action is now, not when crowd shows up on your doorstep.

Steve Crimando, *is Managing Director of the Extreme Behavioral Risk Management division of All-Sector Technology Group, Inc., a NYC-based consulting/training group. Contact Steve at: (212) 366-8343 or steve@xbrm.com.*

TAKING OFF THE BLINDERS — Defeating Social Engineering Where it Bites!

By Joseph Castellano, CPP

Technology in our daily work environment has meant virtual workplaces become reality and emails, texting, instant messaging and all the other great advances enable mobility. But we are also more vulnerable to cybercriminals.

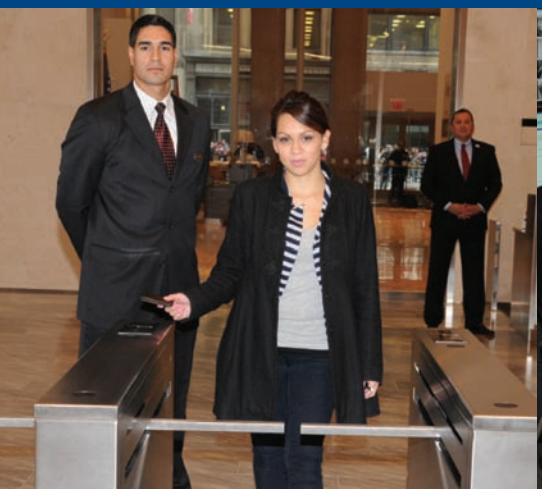
With every step forward to protect our firms from cyber attacks, we risk a step backwards with freedom of use and access. The middle ground requires security professionals engage everyone in the work environment so we all help ensure growth while limiting unnecessary exposures and risks.

Exactly how do we get blinders off co-workers who are steeped in technology in all their activities? The risks may scarcely be apparent in well devised social engineering schemes!

Social engineering is essentially a new spin on the long standing confidence game. "It's the art of manipulating people into performing actions or divulging confidential information to gain access to buildings, systems or data by exploiting human psychology, rather than by breaking in or using technical

continued on page 29

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

11 Penn Plaza New York NY 10001 212-563-0500 www.MulliganSecurity.com

hacking techniques." (Goodchild, Joan, "Social Engineering: The Basics," January 2010, csoonline.com) Social engineers rely on getting you to lower your guard and gaining your trust and, although they may have been called other names, they've been with us from before Charles Ponzi in the early 1900s and likely long past Bernie Madoff in 2008. The substantive change: using technology and social networking media.

There are still twists on the famous "Nigerian Letter " email scams of the 90s. New phishing scams reach millions with the aid of social networking. People expose their own personal data [Facebook anyone?] and literally hand over vast arrays of resources for perpetrators to exploit.

Social engineers targeting your firm may look for a new employee who has posted the good news on, say Twitter. It takes under five minutes internet research or cold calling to find her number. Then with or without a spoofed caller ID, add some sense of urgency and the classic "Jane, you must be new... I NEED this information now — don't blow it in your first few days..." and likely I can get any details I want from her.

People also post company information, vacations, birthday/event dates, relatives and relationships on sites. A spin on the above example could be when Jane answers her line she states "Jane Doe, how can I help you?" I can say: "Jane Doe, are you Johnny Doe's sister... I know Johnny for years; we just stopped out for his birthday before he went to the Bahamas..." Did I gain her trust... we're practically related!

The potential for disaster is in our email boxes: it's executed via links or malicious programs embedded in downloads. "Look at this video" or "Have you seen this picture of you!" and one click… is all attackers need. Another popular scam is the seemingly panicked woman who approaches you on the street, begging to use your cell phone to reach her family or children due to an emergency... You hand her your phone; in seconds, while it appears she's making a call, she's downloaded an app, and has successfully cloned your device. Every text, email, picture or action on your phone is visible to her remotely.

People expose their own personal data and literally hand over vast arrays of resources for perpetrators to exploit.

Whether bad guys wear a maintenance shirt, push a cart, or come in an expensive suit, if their hands are full, or they appear confident, someone will hold a door… It's in our nature and social engineers prey on it. With a confident gait, and a friendly greeting to the guard, I've gained entry during penetration testing by displaying a NYC transit metro card. We need to teach or employees to be on suspicious first, rather than distraught afterwards.

Many still consider people the weakest link in the security chain. Sophisticated social engineering can circumvent most, if not all, of the high-tech security measures we have in place. Go to the US Department of Homeland Security Computer Emergency Readiness site for tips and pointers to use with your workforce now.

Awareness training is often ignored or shelved but it is what will make the difference. From receptionists to senior partners, we need to remove blinders and incentivize the "clean desk" and proper denial of information/access. Test and train weekly, quarterly whatever works for your firm. Keep it interesting, concise, easy to absorb and easy to apply. Use the "family" hook if it works! Add an education piece to your drills; prepare a piece for "take the kids to work" day. Get everyone in the firm involved in internet and technology security. Help them 'see' the big picture!

***Joe Castellano, MPA, CPP**, is a Senior Manager with Pricewaterhouse Coopers US Security. Joe was an NYPD Commanding Officer, Homicide Division on SI; task*

continued on page 31

Protecting Your Peace Of Mind

SECURITY OFFICER SERVICES

- 24/7 Physical Security Options
- Fire Safety Services
- Concierge/Lobby Reception Services
- Security Command Operations
- Full-Service Aviation Security

INVESTIGATIVE SERVICES

- Background Screening
- Fraud/Employee Theft Investigations
- Auditing and Compliance Monitoring
- Litigation Support
- Surveillance

EXECUTIVE PROTECTION

- High-Level Executive Protection
- Threat and Vulnerability Assessments
- Special Event Security
- Security Consulting
- Security Training and Seminars

SUMMIT

1-800-615-5888
www.summitsecurity.com

New York • New Jersey • Connecticut • Florida • California

force assignments included Drug Enforcement and NY-FBI Asian Organized Crime Task Force. His MA in Public Administration is from Marist College.

BACKGROUND SCREENING — GETTING ALL THE RELEVANT DATA AND THEN KNOWING HOW TO USE IT!

By Joseph W. Biondo and Kimberly Bentley

Would you Risk $1M?

Your potential employees have impressive resumes, interview well, and are definitely qualified for the positions — however what they fail to mention could leave you, as the employer, exposed. Recently, the Roman Catholic Archdiocese of New York learned this lesson the hard way. An employee who worked in the finance office allegedly stole nearly $1 million from the Church. Compound it: she had twice previously been convicted of fraud against employers! Since the Archdiocese failed to conduct a background check on their new hire, this record was never discovered.

Pre-employment background screening is a critical tool in today's hiring process. With current technology, these screens can reveal a wealth of information about a person's past, but technology only offers half the picture. Astute human analysis of results offers the missing piece. Otherwise employers just get data on a page which may or may not reflect hiring criteria for particular positions. Background screening at its best is the analysis of that data, so employers know what the information actually means and the important material is highlighted.

There is no "one-size-fits-all ". A DUI two years ago may not be an issue for a payroll assistant, but it would be for a new driver. In turn, a receptionist may not require the same level of scrutiny as the new executive. Under today's regulations, the risk to employers for not hiring someone based on a lack of understanding of background screening data, is just as large as hiring someone without an adequate pre-employment background check at all.

States are moving to regulate background screening. It behooves practitioners to take necessary steps to avoid greater government intervention so self-regulation can preclude adding layers of difficulty and paperwork to the process. Otherwise, we may see background checks going the way of polygraphs in the 1980s.

We've found that membership in and staying active with associations such as ASIS International and the National Association of Professional Background Screeners (NAPBS) helps practitioners stay current on changing laws, industry trends and advances in technology. We also have to continually hone our data analysis skills and our understanding of unique risks at different employment levels because this is critical to executives who hire us. Due diligence is more than simply providing all the data obtained.

We reduce some high risks in background screening by providing fair, accurate analysis and data evaluation while working within the appropriate laws/regulations. Our goal is to help employers avoid high risk on their end by providing substantive information that helps them make informed hiring choices. In turn it is all about maintaining appropriate [high] security all the way around!

Staying active with associations such as ASIS International helps practitioners stay current on changing laws.

Joseph W. Biondo *is Managing Partner and* ***Kimberly Bentley*** *is Director of Investigations at Summit Security Services, Inc. (www.summitsecurity.com), which is headquartered in Uniondale, NY. Email: jbiondo@summitsecurity.com; Phone number: 516-240-2411*

DATA PRIVACY: THE "NEED TO KNOW" PRINCIPLE

By Tom Robertson

continued on page 32

Prompted by the global shift towards cloud computing and the resulting ancillary regulatory requirements around protecting personal information, corporations are increasingly asking their security departments to participate in and often lead the development and execution of client data protection and privacy programs.

The core of privacy issues and perhaps the single question that underlies developing a successful program is: "Who needs to know this information?" The default position is: if there is no need to know, there is no access.

Key in the process is defining the "need" as a concrete business requirement. It reveals the critical distinction between "needing to know" and simply being "allowed to know." Whereas the former is essential to job performance, the latter is simply about meeting a set of criteria such as job band, skills and qualifications, or a given level of IT access or security clearance.

For example, Claims Adjusters in an insurance company may be authorized electronic and physical access to medical information for a corporate client's employee base. They are allowed access by virtue of their positions. However the authorization only translates into "need to know" when certain conditions are also met, most obviously the processing of medical claims for particular employees. No such condition and access is prohibited.

Ideally, prohibition is from both physical and electronic access when the 'need' condition isn't met. More realistically: communicate the policy; deliver it with training; establish a Code of Business Conduct and get sign-offs from all who are allowed access, reinforcing that everyone involved is at least aware of what's acceptable.

When it's properly implemented, many unintentional breaches can be short-circuited and help keep private information out of the public arena.

Communicating the "need to know" principle to fellow employees and having them adopt it as critical mindset when dealing with sensitive information is a first step towards a robust data privacy and protection program. When it's properly implemented, many unintentional breaches can be short-circuited and help keep private information out of the public arena.

For additional information, contact ***Tom Robertson*** *at: robertsontom@hotmail.com.*

RFPs — BEAUTY OR BEAST?

By Richard Baranowski

The security guard services industry is estimated at over $53 billion in the US. Thousands of security firms compete for slices of this lucrative pie through the RFP process. During my 28-year tenure in the contract security business, both in Canada and the United States, I've come across 2 levels of Request for Proposal (RFP): those that demonstrate outstanding new thinking, raising the RFP bar; and those that are resurrected relics dressed up in the latest security lingo.

Many high-end RFPs tolerate minimal to near zero profit margins in addition to dictating pricing component costs. This heavy-handed approach forces security guard service providers to look for new ways to win RFP awards, let alone make sufficient profit to stay in business and fulfill their proposal commitments. The end result to a high-demand, minimal profit RFP may be less than what's promised and may not serve the buyers' needs. There is no gain for clients who have to settle for inferior performance; live with less than the best service or repeat the entire RFP and contracting process when their choice guard service can't deliver. No one can replace the lost time.

Here are some suggestions for balancing the RFP approach:

1. Ensure the RFP allows for a

reasonable profit level, otherwise vendors may be forced to recover needed profits in less desirable ways, e.g.: a) Submitting inflated benefits and overheads, and b) Extending employment probationary periods and inducing higher site-guard turnover rates to capture increased margins.

Many high-end RFPs tolerate minimal to near zero profit margins in addition to dictating pricing component costs.

2. Ensure there is a pragmatic alignment between dictated wages and what guards are required to do. Consider a tiered wage system if that is not already part of your approach. Higher hourly wages go to personnel at critical posts requiring mandated experience, excellent communication skills and higher training levels, e.g., control room operators.

3. Use the screening process and final interview to thoroughly test your prospective winners. Have them bring supervisors they've slated to serve at your company. Ask these individuals about how they'll handle specific situations you've identified as problematic at your facilities. Visit the guard company's office and reference sites at off-hours. Speak with former clients who no longer use their services. Vendors that avoid participating in this tough screening or where the projected image and the reality are far apart can be eliminated from the process.

I have seen the security guard services "pie" change. At one time, the "beauty" of the guard industry was that it was profitable, with years of significant recurring revenue after contracts were won. Today, it's transformed into a highly competitive and perhaps "beastly" playing field with drastic changes in both service providers and client demands. Striking a true balance that works for both sides is a difficult feat, and perhaps the subject for another discussion.

Richard Baranowski *is President of RFP Security Services, based in Seattle, WA and can be reached at:*

richardbaranowski@comcast.net

INTEGRATING TECHNOLOGY WITH THE HUMAN EFFORT

By: David Feeney

While there is no replacement for a quality security team, new technological tools can help increase the impact of even a single security officer while enhancing overall safety and security.

Today many organizations economize by having fewer or only one officer on-site and using technology to 'view' and measure what is going on in their buildings. Device signals, gauge readings and live video can get transmitted to remote control rooms where experts monitor the data on a continuing basis. If a 'problem' signal comes in, these experts can direct on-premises officers to address the situation quickly and resolutely. Net results: companies often avoid charges for false [burglary] alarms and swiftly address real emergencies.

When combined with appropriate personnel, technology can enhance security operations at a very different level.

If air conditioning fails in cold storage warehouses, technicians are summoned from the remote control room as the failure registers. The on-premises officers get immediate notification and can be in place to oversee access.

Between IP cameras, phone lines, cell signals and myriad monitoring and transmitting devices, including GPS and satellite communications, what we need to know is more acces-

continued on page 34

sible than ever before. When combined with appropriate personnel, technology can enhance security operations at a completely different level.

An integrated technology solution can be the answer to doing more with less, and a true security partner will make sure you are gaining additional value through technology. A comparatively small financial commitment if pursued through the right channels can easily create a meaningful return on investment. Sometimes, it means looking at a situation from a completely different perspective. Between upgrading the technology itself and engaging tech-savvy officers into the regular security program, asset protection can take on a valuable new dimension.

David Feeney *is the IT Director, Integrated Solutions at AlliedBarton Security Services. He can be reached at: 484-351-1540 or david.feeney@alliedbarton.com.*

OPEN-SOURCE WIRELESS SENSOR PLATFORM — INTERNET OF THINGS — Case Study: Radiation Sensor Integration

By Joe Jesson

Newest Revolution:
The Internet of Things

When I went to purchase Geiger-Muller radiation sensor tubes for a project I was working on last year, I was quickly informed that all GM sensors and Geiger counters were sold out. The Fukushima crisis drove engineers, technical hackers, and citizen scientists to quickly build and launch radiation-monitoring points throughout Japan. Many people did not trust the official government information and took control of sensing radiation throughout Japan. Within weeks of the Fukushima radiation incident, over 2,000 sensors were reporting to the revolutionary and pioneering open portal known as Pachube! Take a look at https://pachube.com/feeds?tag=radiation

The key to this speed in which these sensors were deployed is the selection of open hardware (open Arduino hardware was a favorite in monitoring this background radiation, and an open Portal, Pachube, integrated with code to quickly report and share radiation levels throughout). The systems do require an Ethernet or WiFi connection to the Internet in order to communicate to a portal, however, it establishes that the move to interoperability has significant value on a worldwide basis and can be put into use right now.

Additional security and threat detectors, e.g. gas and intrusion, could also be added quickly in the same fashion as described. There are three essential steps to the process: Select the appropriate sensors; Design the interface with a processor and communications board that will function in an open architecture setting; Write and debug the firmware. This last step will require expertise in writing "C " code and understanding hardware design. With a well commented source, you can accelerate this entire process as the post-Fukushima activity suggests.

The Fukushima crisis drove engineers, technical hackers, and citizen scientists to quickly build and launch radiation-monitoring points throughout Japan.

For some practical examples of how we've been able to implement the technology and how the open source platform makes a significant difference in cost, time and deployment, go to: www.xacttechnology.com

Joe Jesson *is CTO at XACT Technology LLC and can be reached at: 203-613-3344.*

CAMPUS ENTERTAINMENT VENUES: Template for Averting Lawsuits, Aggravation and Potential Disasters

By Karin-Jill Magaziner M.S., P.D., NCSP, Dipl.

When colleges and universities have hundreds, if not thousands of students available to augment campus security staff, why do

so many institutions choose to bring in professional security personnel who specialize in entertainment events?

At first, it seems a no-brainer to just use available manpower on campus. It's certainly an inexpensive approach. Yet today, many college management teams recognize the liabilities they avoid by bringing in experts when the public is invited to attend events or revenue-producing concerts and entertainment programs at their facilities.

Consider events where pat-downs might be required to ensure that weapons, alcohol or other prohibited materials remain outside the gates. Students who have either no or little training in these specialized procedures create a potential for accusations such as: "His hand went in my bag and now my money is missing". Trained eyes, ears, and hands can effectively de-escalate many such challenges.

In some cases, just having additional professionals who are familiar with handling medical emergencies in crowds and deescalating conflicts between attendees can mean that situations are addressed with speed and tact so public relations snafus are minimized and all the press is positive.

Student workers may not be the best choices when it comes to backstage access at any program. They are far more likely to allow their friends to pass through. This can put the college/university in a difficult position with performing artists. Students unless specially trained, will not be familiar with emergency management guidelines; their judgments in these unfamiliar, high-stress situations may create compromising situations and potential liabilities that far outweigh the cost of having professionals addressing these issues.

With programs open to the public where crowds, chaos and unknown elements may be entering the premises, it makes the most sense to contract qualified campus event security professionals. They often provide exceptional dividends in securing the reputation of the institution as a safe environment no matter what the event.

KJ Magaziner M.S., P.D., NCSP, Dipl. CFC *is a nationally certified*

continued on page 36

school psychologist who works with Green Mountain Concert Services. For more information, contact her at kjm@gmcsusa.com.

PROTESTS 2012-STYLE

By Tony Macisco CPP

In years past these terms were unusual to hear in general conversation: sleeping dragons, lock-ons, flash mobs, hactivism. Not anymore. With this year's 'Occupy' protesters the terms will probably become common as will seeing companies facing: sit-ins, non-compliant/non-violent traffic disruptions, noise and/or odorous assaults on/in buildings, and smear campaigns against board members and employees.

Distinguishing the differences between normal protest events and ones intended to cause property damage, employee intimidation, and business interruptions along with negative publicity, can help organizations avoid lawsuits for improper responses to the different types of protesters. But let's not ignore that quantities of individuals who now underpin the protest movement here are paid experts and not just disgruntled citizens. Some people in the movement, with criminal intent, have the demonstrators as their unwitting camouflage.

It appears that proficient protestors learn faster than security personnel and law enforcement; they often publish their results via the internet. Experienced protesters travel globally to lend their skills and experience to whatever demonstration supports the cause de jour. The professionals in the ranks with criminal agendas who want to avoid attention and preemption use information security to maintain secrecy. However everyone in the protest movement leverages social media effectively. It may not be easy to differentiate those with corrupt intent.

Successful management programs are proactive and involve all the constituents: security, legal, communications, human resources, training/operations as well as law enforcement. If your company is targeted, then protestors may attack both brand and physical infrastructure.We train our security personnel to remain calm during lobby 'invasions.' Now we also have to get buy-in from company employees so they understand their rights and responsibilities. The goal: preventing the protestors from being effective and minimizing their opportunities to create subsequent lawsuits.

Being able to forecast a scheduled demonstration is routine; a matter of internet search terms. The critical capability: understanding protester tactics and predicting which protest events will cause business disruptions or revenue losses; and which won't. The right answers save corporations needless expenses and allow target hardening when situations demand.

Sometimes, it pays to call in an expert to help make that determination.

Know your vulnerability. Be prepared. Be situation-aware and understand the threat types.

***Tony Macisco** CPP, is Director CIKR Security at The Densus Group. For details go to: www.densusgroup.com*

AND INSIDE THIS WALL...

By Chris Adams

Now, with a portable, hand-held device, you can 'interrogate' objects, parcels, bags, upholstery, vehicle interiors, and yes, walls, without opening or disassembling them. You'll be able to detect what is behind external coverings or inside suspicious or abandoned parcels. You'll even be able to detect hidden objects penetrated into and hidden in walls.

Equally impressive you can scan people for problematic materials concealed beneath their clothing and neither you nor your security team has to ever touch or put hands on the individuals.

The new millimeter wave security and detection wand discussed here has resolution down to several millimeters with a clear view screen that provides law enforcement or your lobby security personnel abilities to scan boxes without opening them and check bags and attaché cases without handling them or having them leave the possession of their owners.

You'll even be able to detect hidden objects penetrated into and hidden in walls.

Millimeter wave technology is the basis of this new detection system and is available from a number of providers. It has the advantage that it's been studied by experts at FDA, DOE, DHS and DOD and by a variety of academic leaders who all agree that it is safe to use. The technology emits minute amounts of energy in the ISM band similar to Wi-Fi and cell phone products. Because of the low radiation emissions users are not required to have licenses to operate these special cameras.

Detecting the problem before it can enter your facility or get distributed through your systems, and being able to do

continued on page 38

the detection without physical contact and without touching people or their possessions makes adding hand-held millimeter scanning devices ideal additions to your security program.

More details about the technology behind these lightweight, durable imaging devices is available from ***Chris Adams*** *at Walleye Technologies and he can be reached at: cadams@ walleyetechnologies.com*

GUIDELINES FOR HIRING PROTECTION TEAM MEMBERS

By Michael J. Scanlan, CPP & CST

During the 25 plus years I've spent providing protective services, I have hired many protection specialists, each with unique skills and qualifications, but all possessing certain attributes I believe are essential for success. There are four general criteria that I use in selecting excellent agents for work in the private sector. .

1. Professional Appearance

Appearance matters. In the protection services business, looking the part is essential in establishing credibility and instilling confidence, comfort, and trust. As service providers in a serious business, projecting a professional image can deter casual problem-causers. Perception is reality in first encounters, and prospective agents who arrive for interviews or report for duty unkempt or sloppily dressed do not inspire confidence.

2. Healthy Image

Protection is a physically and mentally demanding profession. It is essential that team members be in excellent physical shape to endure the rigors of the job and to enhance client perception of agents' abilities. In my experience, out-of-shape or overweight agents cast doubt in clients' eyes and decrease confidence in the agency they represent. Many protection specialists are stocky and strongly built, but a large stomach hanging over a belt does not impress potential clients.

3. Background/Experience

I look for prospective agents with a "balance" of field experience, involvement in on-going training, and a commitment to professional development.

Highly trained individuals with no field experience, or those with strictly field experience, are red flags in the selection process.

Highly trained individuals with no field experience, or those with strictly field experience, are red flags in the selection process. Individuals with military and law enforcement backgrounds who transition to the private sector often make excellent protective agents, but the most desirable candidates are those who continue honing their skills and acquiring new ones.

4. Positive attitude/Sense-of-humor

A positive attitude and a sense of humor characterize successful professionals the world over. These attributes help professionals accomplish difficult tasks and meet the unnerving challenges of protection work. I place a premium on agents who have a sense of humor and demonstrate a positive attitude regardless of the situation or obstacles.

These guidelines have helped me lower probabilities that I will select subpar performers. You may wish to adopt them as well when screening protection agents who will represent your organization and clients in the toughest and most challenging environments. After all, isn't that the bottom line?

Michael Scanlon *is a Detail Leader for The Global Elite Group. Email is: mscanlan62@aol.com and contact phone # is 917-345-2418.*

IRIS RECOGNITION Biometric Technology That Works

By Michael Wells

Iris scanning has proven to be one of the most accurate biometric technologies thus far. It provides

high confidence authentication quickly; it can be used in myriad applications and it works either for identification or verification.

Since the iris is unique to each person, although it can be copied onto a contact lens, our current iris measuring devices have been able to detect the minute differences that distinguish a 'real McCoy.'

Like a snowflake, the iris, (the externally visible colored ring around the pupil) exhibits a distinctive pattern that forms randomly in utero in a process called chaotic morphogenesis. In fact, it's estimated the chance of two iris (irides) being identical is 1 in 1078. This allows for more than 200 points of reference for comparison, vs. 60 or 70 points in fingerprints.

Iris scanning has proven to be one of the most accurate biometric technologies.

Just like a fingerprint, the iris is stable over time. And even if an individual is blind, as long as the iris is intact, it can be scanned accurately.

Iris scanning works well in large database situations and offers some protection/privacy that many other forms of credentialing don't.

It's also versatile for the One-to-Many, One-to-One, Wiegand and Token Environments. While initially designed to work in one-to-many search mode, iris recognition works well in 1-1 matching, or verification mode, making the technology ideal for use in multifactor authentication environments where PINs, or tokens like proximity or smart-cards are used.

In a token environment, many privacy issues related to biometric database management are moot, as the user retains control of biometric data — a small template of 512 bytes per iris.

As iris scanning has become more widespread, it doesn't always meet with the same resistance security professionals found years ago. People have adapted to getting close enough to iris scanners so the machines can work. Moreover, individuals no longer tend to fear that scanners will somehow damage their eyes. Iris recognition is a technology that has become cost-effective and is likely to find increased applications this decade.

continued on page 40

DEFEAT CORPORATE SPYING AND PROTECT YOUR PROFITS

By Michael F. Aiesi

My premise is simple: While we have all heard that we must protect our Intellectual Property from foreign governments and hostile intelligence services, no one has come up with an off-the-shelf plan to do it. Maybe it's that we are not focusing on what's really important. If the past is prologue, then a detailed review of past economic espionage cases gives us some real answers. I have reviewed a number of these cases and have come to understand some basic truths.

Know these 2 things and increase your chances of defeating internal corporate spies and ultimately protecting corporate profits: Know your employees, not just when you hire them, but continue learning about their behavior as they progress within your organization. Here, let's focus on espionage perpetrated by a single employee or contractor. Perhaps not as sexy as cyber-espionage, but to the company being victimized, it is just as fatal.

There are a substantial number of indicators; one or two standing alone might mean nothing. When total indicators start to rise to three or more, it may portend a serious problem. These indicators are similar to what the FBI and CIA screen for when doing internal checks for moles.

Three examples of questionable activities by employees: Frequent personal overseas travel; unusual interest in projects not within their purview; taking or sending sensitive corporate material home. It could mean nothing other than a serious policy violation for taking the material. However, it could also mean employees are being secretly enticed by a foreign competitor/government to steal specific data.

If you're not even aware of the indicators, you'll never know you have a problem until it's too late.

How do you know what you actually have? Since as security professionals we're paid to be suspicious, initiate a discrete internal investigation to determine the facts. If you're not even aware of the indicators, you'll never know you have a problem until it's too late. The way to spot this kind trouble is to be trained to recognize it.

The second significant issue is having a complete understanding of your corporate Trade Secrets. What is the enabling know-how that makes your corporate secrets valuable? This information pertains to materials and processes that combined make your company's product unique and therefore valuable. At one time or another, we have probably all had a Coke or a Thomas' English Muffin. However, none of us knows how to duplicate their unique tastes. Concentrate on who has access to that enabling know- how or who is trying to obtain access to it. That's where to spend your time to be most effective.

Michael F. Aiesi , *a former special agent with the FBI and former security director at Pfizer, Inc (formerly Wyeth) founded The Arxcis Group, Inc., providing counter-economic espionage training for American companies. Phone: 484-459-7400 or visit: www. thearxcisgroup.com.*

OPSEC FOR SECURITY PROFESSIONALS

By G. Wayne Tilman, CPP, Unit Chief, Federal Bureau of Investigation

The members of ASIS are among the most accomplished security professionals extant. We are the protectors that span the earth. We regularly instruct our constituents about how to stay safer, whether at home or in harm's way. But, do we do ourselves as we tell others to do? Do we maintain operations security, or OPSEC, ourselves?

Let's take a quick test.

Do you have a nearby business listed as "home " in your vehicle GPS instead of your real home address?

Do you use valet parking? If so, do you only give them the switch key? And, leave nothing

in the vehicle that could be stolen or used to exploit you?

Do you wear law enforcement or security logo wear or tactical clothing to the convenience store without the empowerment to back up any challenges it may engender?

We regularly instruct our constituents about how to stay safer.

Do you look for occupied vehicles with the engines running and at the register to see what is going on before committing yourself by going into that convenience store?

While we tell those for whose safety we are charged to have appropriate home security (you know the drill — deadbolts, lighting, alarms, proper height foliage. etc.), do you practice it all the time at your own residence?

Remember, fire is a common home emergency; do you have alarms, extinguishers, a family escape plan and a pre-determined rally point?

Social networking is becoming more pervasive in our lives. Do you or family members have information or photos on your sites that may aid stalkers, identity thieves, pedophiles or foreign intelligence agents in compromising you? Do a self-audit and check your security controls.

Dating sites… one ad says that one in every five relationships comes out of a dating site. Maybe I am paranoid, but the first thing that comes to mind is that credit card TV ad where the guy in Siberia answers the phone as "Peggy." Need I say more?

The Internet is a wonderful source for just about anything. But, it is largely unregulated, and anyone can proffer any "fact" they want on it. Do you consider most of what you find on the Internet to be raw intelligence until you validate it via reliable sources?

So, be honest. Did you pass every question? As a professional, you realize we did not even scratch the surface. But, hopefully, it got us all thinking about our own OPSEC.

continued on page 42

NOTE: The opinions herein are those of the author and not of the FBI or any government agency.

***Gary Tilman** is a Unit Chief with the Federal Bureau of Investigation and he can be reached at: Gary.Tilman@ic.fbi.gov*

THEY CAN SMELL A PROBLEM BREWING...

VWD Canines — Highly Effective High Technology

By Paul Stapleton

The emerging and ever-changing technology behind explosives detection has advanced from traditional bomb-dogs who sniff stationary objects to the latest called Vapor Wake Detection canines that can comb large areas without disturbing the environment.

Auburn University is home to the Vapor Wake Detection (VWD) canine program. Consider it as standard explosives detection canines (EDC) with additional abilities and training to detect carried or body-worn explosives. Students (canine and handler) get at least 10 ten weeks in basic explosives handler courses and then an additional 2 weeks in the Vapor Wake Detection specialty which includes intense training, written tests, proficiency checks and performance evaluations.

In action, it's clear that the canine is the leader of a VWD team. The dogs work large areas, detecting the plume of odors from people and objects they carry as they transit a location. To date, there is no technology out there that can as quickly clear a location and be as unobtrusive as vapor wake dogs. Even a report from the Pentagon in 2010 said the best bomb detectors were dogs.

It is well-trained handlers' ability to rely on their dogs' skills that make VWD an effective tool in high-demand. Amtrak is among the agencies successfully using VWD teams. Under the leadership of Inspector William Parker, Amtrak has invested in 14 teams that they deploy throughout the country along with their standard EDCs.

"Training daily is a way of life for our teams," says Parker. Running "exercises with and without explosives is an important part of that. Training teaches you if it isn't there, keep moving."

Auburn University's John Pearce, Associate Director of the Canine Detection Research Institute (CDRI) noted: "The handler's most perishable skill is the ability to effectively analyze canine behavior. Handlers must trust the dog's capacity to detect explosives. One effective way to maintain the skill is to run tests that are "blind" to both handlers and the dogs. The canine does not discriminate on people's image or body language — it is their super-human sense of smell that propels their success."

"We use a 4:1 ratio, four students with canines to one instructor," continued Pearce. "We also like to keep the training area population down to no more than 8 students with dogs per area. This lessens the wait time and gives the student and canine more repetitions… in their environment to make them expert at detecting explosives there."

Once training is complete at Auburn's CDRI, teams return to their operational environments. After a period, Auburn's instructors visit to ensure that skills have transferred effectively in work settings. Auburn continues to provide phone consultation or assistance as needed with re-certification required annually.

The (Washington DC) Capitol Police — use their teams to patrol the House of Representatives and the Senate. They train in differing weather patterns and various depths of crowds. Capitol Police also include inserting decoys into the dogs' working environment on an irregular basis.

In action, it's clear that the canine is the leader of a VWD team.

At Stapleton Group we've set up a training facility (our "camp") to expand on what we learned at Auburn University and to keep our teams fluent in explosive recognition and enhance conditioning for the dogs [and handlers] so they can work effectively for long periods of time.

If there is a recommendation that we share with John Pearce it is certainly that we all develop effective tactics for handling suicide bombers. Pearce stated: "I feel that is a huge mistake [not to do this]. Let's further develop this technology (Vapor Wake) and be ready to employ it when it's requested. "

For additional information on Vapor Wake Detection and the canines and handlers who have this special training, please call ***Paul Stapleton*** *at: 347-203-5602 or email to: PStapleton@tmprotection.com.*

GREAT TACTICS MAKE GREAT MOVIES... GREAT STRATEGIES NOT SO MUCH...

By Mario J. Doyle, CPP

Everyone gets excited by high-level heroics and subduing the bad guys —at least when it's portrayed in a motion picture. But in real life, that type of extreme tactical response is best when it's the back-up plan… Unfortunately, it means the strategy failed.

In contract security services, when we work with clients on superior strategies to avoid workplace disruptions, ensure security and safety on-premises, and provide a high comfort level for clients' employees, it may not look so exciting. But by bringing expertise to the table we prevent most problems from ever materializing and that makes the most sense.

Being able to develop effective prevention strategies means knowing the corporate cultures of organizations where we're contracted. It means coordinating with the company's security management and business management teams. Although basics have to be covered in terms of tactics employed by front-line security officers, how procedures are put in place, even how announcements are shared with employees can go a long way toward gaining compliance. In any business or NFP, preventing harmful situations is foremost though not glamorous.

Training for our security officers is about specific tactics that support strategies. They are taught and demonstrate successful

continued on page 44

approaches for working with obstreperous individuals at the lobby desk or addressing frustrated truckers at the delivery dock while vehicles go through inspection. We focus on giving officers skill sets that help them on the front-line so problems don't escalate and become distractions.

If we are very good at providing security, it may seem as if almost nothing happens. No one gets on the front page of the newspaper. Even if protesters are marching in front of the building, no one gets in a fight with them. But to create that environment; to keep everything running smoothly, means that those of us in the background are on alert all the time and making sure that our strategies continue to meet changing threats and new developments

By bringing expertise to the table we prevent most problems.

Perhaps that means no highlighted starring roles on the silver screen but if our strategizing with clients means we're better prepared to offset crises, then that sounds like something worth cheering about to me. Please pass the popcorn…

Mario Doyle *is COO of Doyle Security Services, Inc www.dss-securitysolutions.com and can be reached at: 877.377.7749.*

HANDLING RESTRAINING ORDERS IN A HEALTH-RELATED FACILITY

By William Losefsky, CHPA and Joseph Bellino, CHPA, CHEM, CSE

Each year perhaps one million people are involved in workplace violence of some type. If you are in security management for a healthcare/health-related facility, you probably know that OSHA has designated our classification as a high risk industry. Creating practical SOPs for dealing with and managing restraining orders has helped us have adequate safeguards in place to protect employees while meeting federal requirements.

Chances are that you've already been approached by an employee who has been issued a restraining order against another person during your career. Here are some of the approaches we've taken to address risks and mitigate possibilities for violent confrontations within our buildings.

Initially, when establishing the procedures, we met with our local clerk of court and police agency to become fully familiar with how restraining order processes work in our area. We now keep government-issued pamphlets covering restraining orders in the security office as reference. For instance, in New Hampshire (where we first established the procedures noted

here) a police officer can obtain emergency temporary restraining orders telephonically from a judge 24/7. Temporary restraining orders cover a limited time frame, but give victims instant protection under the law until more formal court hearings are scheduled.

We cover restraining order processes in new employee orientation programs. In some instances HR wants to do the presentation. But whenever possible, information comes directly from our security leadership since it helps establish the necessary rapport with a matter this sensitive.

Restraining orders have expiration dates and if not refreshed, become invalid. We use a software program (REPORT-EXEC) and have added restraining orders as a category so officers can track on-going orders and expired ones for quick reference.

We also identify the nature of the threatening conduct. Obviously, weapons-use or threats of imminent bodily harm are noted and measures taken by security staff to protect themselves as well as employees. We fax a copy of these orders to local law enforcement with jurisdiction. We also fax to departments that would be "back-up" to the primary LE agency.

I always ask the victim for a picture of the person against whom the restraining order is issued and include it with the fax. Security officers, especially the ones from the "Nintendo Generation" are quite skilled at producing a picture for us after a thorough scan of sites like Facebook, MySpace, etc. You can also share this information with the "front desk" receptionist and department heads of areas where the employees work. That way, many other eyes are looking for the person along with your security staff. We place a clip board, listing all on-going active restraining orders directly above the security officer's duty desk station.

Many times, the defendant is very much aware of where the victim works and his/her hours and days off. Defendants may

continued on page 46

have even driven victims to work and may know the layout of our facility. In these cases, we've found it advisable to have security know victims' work schedules so officers can provide escort into and from the building. During restraining order periods, consider allowing special parking close to the worksite for victims along with the security escort. For us, this qualifies as a 'special needs' situation and adds another layer of "due diligence" on our part.

Our restraining order policy and procedures have gone a long way to professionalize the image of our security department.

We periodically check with victims as to any changes to their orders or increased threats from the defendants. Many times, victims are aware of a defendant's new vehicle, etc and we share updates with law enforcement.

Our restraining order policy and procedures have gone a long way to professionalize the image of our security department and have added greater protection for our staff while lessening liability for the organization. Your people are your greatest asset. So, pro-active security measures that you establish to create a safer environment for your charges, shape and enhance corporate culture.

William Losefsky, *CHPA is the CEO of Investigative Concepts, LLC and was the recipient of the IAHSS Lindberg Bell Award in 2010.* ***Joseph Bellino****, CHPA, CHEM, CSE is the System. Executive Security & Law Enforcement, Memorial Hermann Health System, Houston, Texas. He is the past president of the IAHSS.*

MSA X-RAY SCREENER TRAINING: "It Can't Be Seen if You Don't Watch the Screen"

By Kenneth McGuire

It's easy for screeners and lobby personnel operating x-ray machines to get distracted or

fail to "see" an IED if they haven't been fully trained and tested or have many functions to accomplish at the same time. Recent reports from the GAO and ASIS International point out the vulnerabilities. And in one case investigators were able to infiltrate 10 high-security federal locations with IED components in their screened bags or on their persons.

How do your screeners respond to distractions? Most failures in x-ray screening result from screener inattention to the items passing right through their machines.

We know that improvised explosive devices (IEDs) are common terrorist tactics; both the materials and assembly instructions are readily available for motivated operatives. One such case occurred in late 2011, as Jose Pimentel was arrested for allegedly building bombs to target NYC buildings and cars. A lone wolf actor, he reportedly acquired explosive ingredients and components to assemble at least three pipe bombs. He attempted to build a low explosive-filled pipe bomb device that incorporated a power source, initiator, explosive, and switch. Fortunately, unsophisticated IEDs such as these utilize components that can be easily recognized by an attentive x-ray screener.

Most failures in x-ray screening result from screener inattention to the items passing right through their machines.

MSA provides training programs to assist x-ray screeners learn to avoid distractions and our research shows that by giving screeners every possible tool to stay focused on the screen, we make a difference in their attention to this vital task. As an ongoing in-service training reminder, and to ensure screeners can most effectively do their job, MSA Security has developed a screener sticker with the reminder "It can't be seen, if you don't watch the screen." If you would like to incorporate this free sticker into your training program, please reference MSA Security's website at: http://www.msasecurity.net/training-sticker for ordering instructions.

'TIS THE TIP OF THE SECURITY INFORMATION ICEBERG

'tis the tip of the security information iceberg, all the articles you've been reading here that is. There are more and I'll get the additional material into print via e-publications early this summer and throughout 2012. So, keep writing and sharing what's on your mind. I look forward to giving it presence and making it part of our collective resources.

Over the years, it was sometimes difficult to get input from so many perspectives. I thank you all for changing that dynamic and giving voice to your ideas, your opinions and sharing advice that can be essential to someone else's security success .

Yours truly,
Erica
Erica.harrison@gmail.com
631 565-7122

SEE WHAT WE SEE.

INTRODUCING MSA WORLDVIEW

In our quest to maintain business-as-usual for our clients, high quality, reliable intelligence is critical. MSA Security employs the most well-informed, connected and skilled intelligence analysts worldwide.

MSA Worldview is a daily news briefing of domestic and global events selected, evaluated and distributed by our team of experts.

With Worldview, clients have access to customized intelligence gathering combined with insight that only MSA Security can provide. Try it out at worldview.msasecurity.net

IN THE BUSINESS OF BUSINESS-AS-USUAL.™

msasecurity.net

MSA SECURITY

PEOPLE IN THE NEWS

Frank Taormina, CPP announced that he's been named Co-Chairperson of the NYC Chapter, International Association of Healthcare Safety and Security (IAHSS.) He's also co-author on a publication that IAHSS will release later this year. Frank can be reached at: 917-301-0372

Kimberly Bentley now oversees operations and directs Summit Security's Investigative Division in their Uniondale offices. Previously, she served in the US Air Force in Europe, Washington D.C. and Operation Enduring Freedom. And Lisa Worgull now heads Summit's office in Orange CA as West Coast Regional Manager bringing over 15 years of experience in the background screening industry.

Mordecai Dzikansky, NYPD Detective 1st Grade (Ret.) announced that recently his textbook, co-authored with **Gil Kleinman** and **Robert Slater** was released by CRC Press. Titled: *Terrorist Suicide Bombings: Attack Interdiction, Mitigation, and Response*, it is his second book. The first was *Terrorist Cop* published in 2010.

Mario J Doyle, CPP, former Chapter Chairman for ASIS Long Island and current ASIS International Regional Vice President, has started Doyle Security Services where he is Chief Operating Officer. DSS is a full service security firm providing armed and unarmed security officers, executive protection, consulting and security technology services for corporate clients throughout the metropolitan area. Get an overview of his new venture at: www.dss-securitysolutions.com or reach him at: 877.377.7749.

Thomas K. Comerford, a program manager with the Port Authority of New York & New Jersey let us know that he earned his ASIS PCI (Professional Certified Investigator) designation in 2011 along with adding a Certified Biometric Professional board certification to his credentials. He's now: PSP, CPP, PMP, PCI, and CBP.

Jeff Kruse, General Manager at TransTech Systems Inc. announced that Matt Kronholm has been promoted to Eastern Regional Sales Manager for the company.

Exhibitor's List and Booth Numbers

Exhibitor	Booth
ADT Advanced Integration	101
Aegis Industries	343,
Aggleton & Associates	500
AK9I	533
AlliedBarton Security Services	408
Altronix Corp	306
AMAG Technology, Inc.	320
Ameristar Fence Products	515
ASIS Crime and Loss Prevention Counci	143
ASIS Crisis Management & Business Continuity Council	143
ASIS Fire & Life Safety Council	143
ASIS Global Trans., Pol. Instability & Intern'l Crime Cn'l	143
ASIS Healthcare Security Council	143
ASIS Hospitality, Entertainm't & Tourism Security Council	143
ASIS International	142
ASIS Law Enforcement Liaison Council	143
ASIS Military Liaison Council	143
ASIS NYC Chapter	443
ASIS Supply Chain & Transportation Security Council	143
ASIS Utilities Security Council	143
ASSA ABLOY	305
Avante International Technology, Inc.	200,
Aventura Technologies	207
Avigilon Corporation	620
Axis Communications	406
Babcock & Wilcox Security Solutions (BWSS)	102
Boon Edam	215
California University of Pennsylvania, Booth	541
Canon, Booth	416
CEIA USA	433
Covenant Security Services	419
DEA-Drug Enforcement Administration	435
Delta Scientific Corporation	537
Designed Security, Inc.	317
Detex Corporation	319
DORTRONICS SYSTEMS, Inc.	520
Exacq Technologies	121
Executive Protection Institute	241
F.M. Valenti, Inc.	325
Genetec, Booth	211
Global Rescue	104
Guardsmark, LLC	301
Guidepost Solutions, LLC	115
Hach Homeland Security Technologies	217
HID Global	309
IDESCO Corporation	506
IDV Solutions	516
IndigoVision, Booth	314
Intelligent Decisions	511
IPS RFID/Patriot USA	547
IPVideo Corporation	216
(ISC)2	243
ITVS	118
KratosIHBE (previously Henry Bros. Electronics, Inc.)	501
Kwantek	425

Exhibitor	Booth
LCA Sales Company	206
Lenel- A UTC Fire & Security Co.	112
Let's Think Wireless, LLC Booth	417
Marietta Sensors, LLC	237
Micro Technology Services, Inc.	509
Milestone Systems	133
Mobile Optic Adaptive Intelligence (MOAI)	632
MSA Security, Booth	109
NAVCO	209
New York State Police	135
Niscayah,Booth	225
NOVA Enterprises LLC	442
NY Association of In-House Locksmiths	235
NYC Dept. of Environmental Protection Police	116
NYC Fire Department	519
NYPD Crime Prevention Section	318
NYPD SHIELD	136
NYS Dept of State - Division of Licensing Services	106
NYS Div. of Homeland Security and Emergency Services	608
NYS Division of Criminal Justice Services	434,
ONSSI	414 .
Owl Computing Technologies, Inc.	221
Paladin Sales Group	610
Parabit Systems, Inc.	437
Paperless Proposal	233
PPM 2000 Inc.	411
Qual-Tron, Inc.	521
Quantum Secure	518
Real-Time Technology GroupSafeMail New York, Inc.	336
Salient Systems	332.
Samsung/F.M. Valenti, Inc.	325
SecureWatch24	210
Securitas Security Services USA, Inc.	201
Secure Decisions	614
Security Director News	140
Security Tronix	600
SISCO and GTBM-InfoCorp.	110
Speco Technologies	400
Stanley Convergent Security Solutions	225
Stapleton Group	137
Summit Security Services	321
Team Software	316
Thomson Reuters	107
TOMST	606
Total Recall Corporation	407
TSA - Transportation Security Administration	108,
TSG Solutions, Inc.	602
Tyco Security Products	401
U.S. Coast Guard	117
U.S. Coast Guard Auxiliary	119
U.S. Postal Inspection Service	219
U.S. Secret Service	616
U.S. Security Associates	510
Xcaper Industries	334

Trade Show Committees

Trade Show Chairman
Ray Dean

Executive Committee
Chairman:
Kevin O'Brien
Vice Chairman:
George Anderson
Treasurer:
Craig Schwab
Secretary:
Lynn Brown
Ray Dean
Rich Patti
Erica Harrison
Larry Loesch

Attendee Relations
Co-Chairs:
Lynn Brown
Wayne Vodar

Exhibitor Committee
Chair:
Bernie Jacobs
Co-Chairs:
Mark Berger
Jim Kitchen
t

VIP and Dais Committee
Co-Chairs:
Don McGuire
Keith Mulcahy
Members:
Joette Faherty
Jessica Hagstrom
Mary O'Rourke
Ken McGuire

Security Director Magazine & Media Relations
Editor:
Erica Harrison

Website Management
Chair:
Rich Patti

Seminar Program
Chair:
Erica Harrison

Show Coordination
Co-Chairs:
Larry Seltzer
Charlie Scholl
Members:
Mark Markett
Ingrid Balady

Chapter Booth
Chair:
Tom Detzel
Members:
Don Aviv
Thomas Puleo

CALENDAR OF EVENTS 2012

May 18
Military/Law Enforcement Career Transition Program
at John Jay College

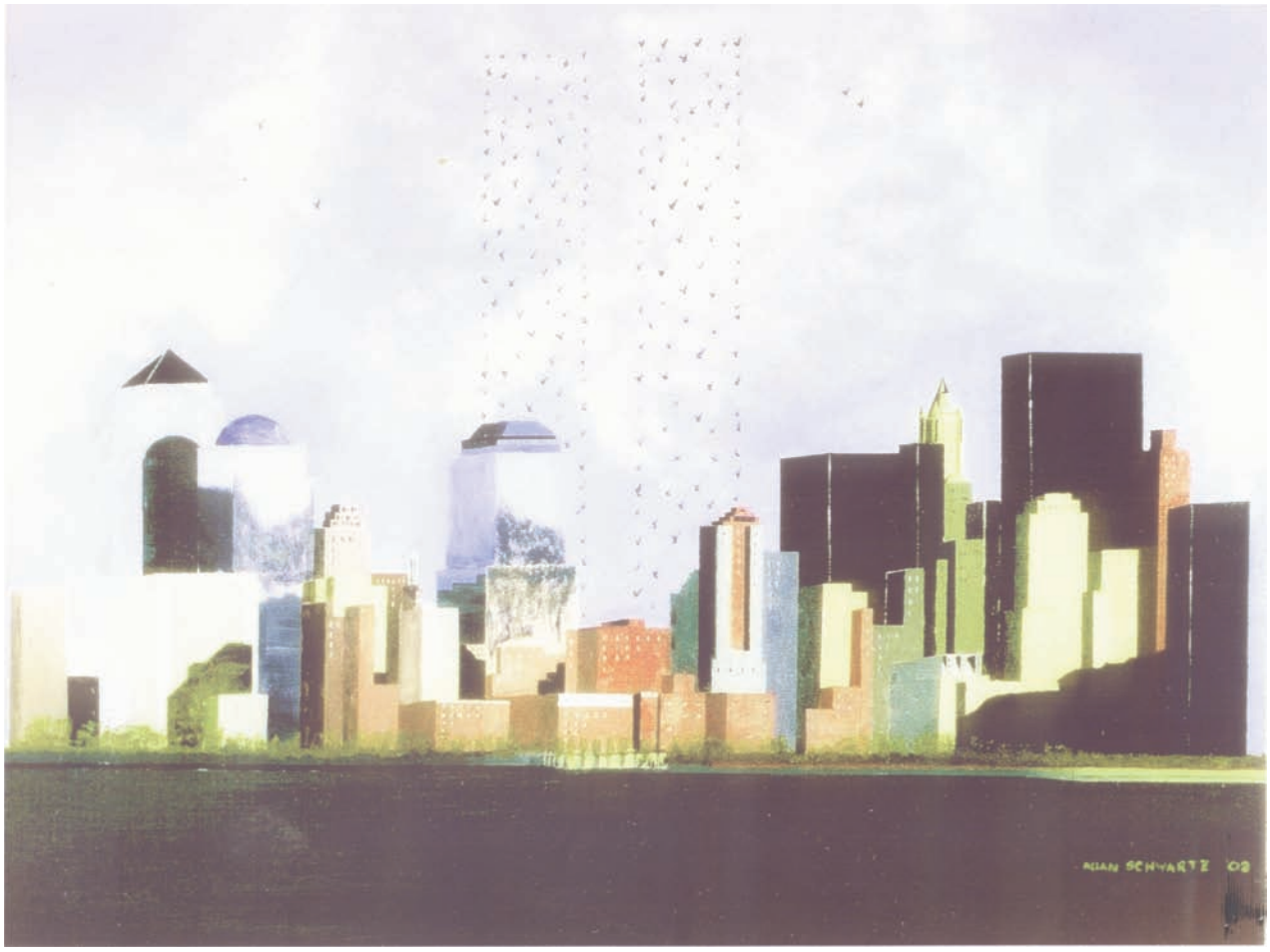
June 11
2012 ASIS NYC Golf Outing
The Village Club at Sands Point

September 20
Evening Networking Event
Sequoia Restaurant

October 19
Monthly Meeting
Location TBD

November - day TBD
2nd Annual Breakfast and Learn
St. Johns University/NYC Campus

December 14
Holiday Event
Hard Rock Cafe/Times Square



"ON WINGS OF MEMORY "

By Allan Schwartz

About The Painting

"On Wings of Memory" is an original painting done in acrylics on canvas. The painting is 48"x 36". The theme begins with the lower Manhattan skyline showing all of the commercial and corporate high-rise buildings, the buildings of the World Financial Center and the residential condominium high-rise buildings that border the site of the World Trade Center.

The lower Manhattan skyline, as we see it today, is missing the mighty twin towers of the World Trade Center. The theme continues with the dedication of the memory of the towers and the memory of all who were lost in the tragedy. To maintain an eternal vigil at the site, the birds of New York, in their sorrow, have gathered at the location of the former twin towers. The birds continue to fly over the site of the former twin towers as they represent peace, freedom, tranquility, gracefulness, vigilance and dignity.

The bird formation is the shape of the twin towers for all to see and, more importantly, for all to remember.

About The Artist:

Allan Schwartz, a native New Yorker, was deeply moved by the events of "9/11" and had a strong need to convey the everlasting "presence" of the twin towers in our minds and in our hearts, in their absence.

Having worked on the 92nd floor of One World Trade Center (the North Tower) and having known several who were lost, he envisioned a concept of remembrance that he expresses in his painting. Allan never painted before.

Allan lives in Yonkers, New York.

Robert C. Gwinnell, PSP, CSPM

Physical Security Professional
ASSA ABLOY
738 Fairway Drive
Union, NJ 07083
Work: 908.688.8820
Mobile: 908.358.4848
RGwinnell@AssaAbloyISS.com

Services and Areas of Expertise:

Provides consultation and training on electrified access control solutions

Specializes in the issues security directors, system integrators and other security professionals face

Over 30 years experience as a sales consultant providing revenue control and security business solutions to banks, retailers, telecom companies, colleges/universities and commercial businesses

Industry Memberships:

ASIS International
Door and Hardware Institute (DHI)

ASSA ABLOY Integrated Solutions Specialist

ASSA ABLOY

Together, security directors and the ASSA ABLOY Integrated Solutions Specialist team can improve facility security by ensuring the right product for the right application, properly installed. With a focus on doorways, including electrified openings, ASSA ABLOY provides a full range of services, backed by the most innovative and reliable products in the industry. This allows us to meet the security and life-safety needs of any facility, while adhering to local and national codes and standards.

Contact us today for all products and services pertaining to electrified openings.
www.assaabloyiss.com

Specializing in industry-leading door and hardware brands:

ADAMS RITE | BARON | CECO DOOR | CORBIN RUSSWIN | CURRIES | GRAHAM | HES | MAIMAN | MARKAR | McKINNEY
MEDECO | NORTON | PEMKO | RIXSON | ROCKWOOD | SARGENT | SECURITRON | SMP SPECIALTY DOORS | YALE

The global leader in door opening solutions