

FULL PROGRAM

1. The Rise of the Jihadists - the Second Stage of the Arab Spring

Monday, February 16, 2015: 10:30 -11:20

Breakout 1

We will address what is now a distinct second stage of the Arab Spring and assess the impact jihadists will have as they exploit the new realities of the region.

The Islamic State of Iraq and the Levant (ISIL) has swept across western Iraq after securing a foothold in eastern Syria. It has declared a new caliphate in the region and is directly challenging al-Qaeda for leadership of the global jihadist movement. Jihadists are fighting one another in Syria and this competition is already spreading to other countries. Meanwhile, jihadist activity is increasing in Egypt in response to the return of an Army-backed regime while Libya is slipping into rising tribal, Islamist and jihadist violence. To what extent will this wave of violence change the face of the region?

Presenting Speakers:

Tim Williams, *Managing Director, Stirling Assynt, United Kingdom*

Mazen Saadah, *Managing Director, Stirling Assynt, United Kingdom*



After joining Stirling Assynt in 2009, Tim Williams became Director, Political & Security Risk in March 2011. While responsible for the Assynt Report and bespoke political and security risk projects, he presided over a significant growth in the business. On acquisition by Falanx Group Ltd in May 2013, Tim was appointed Managing Director of Stirling Assynt and is responsible for profit and loss across all the company's business lines. Tim previously worked at the Society of British Aerospace Companies, the Royal United Services Institute (RUSI) and in a defence policy role for the Conservative Party. He has lectured widely on security issues, including at RSMF, the NATO School and Wilton Park, and remains an Associate Fellow of

RUSI.

Mazen Saadah is Director, Middle East and North Africa, and Islamic Affairs Adviser at Stirling Assynt. His principal expertise concerns political and security risks in MENA and Islamist-related issues. His deep knowledge of Islamic and cultural issues and of the jihadist philosophy enables him to understand jihadist groups' ideology and hence their strategy. He has played a significant role in developing the Assynt Report through enhancing analytical quality of reporting. His advice and expertise have enabled business and government to increase profits, mitigate risks and protect them from threats emanating from jihadists. In addition to his advisory work, he regularly speaks at conferences and public forums. He received intensive religious studies in Saudi Arabia.

3. New Operations - Entry and Exit Strategies

Monday, February 16, 2015: 10:30 -11:20

Breakout 3

New operations entry and exit strategies Incorporating lessons into planning, tactics, and training. Mode of entry understanding and overcoming difficult operational challenges. Improve capabilities across the spectrum of joint operations.

Discussing the security risk management process for starting up an operation in a new high-risk country. Focusing on security support to marketing, contracting, operations, enterprise risk amongst others. Looking at an example of an oilrig start up.

Presenting Speaker:

Ben Murrell, Security Manager, Asia-Middle East-Africa (AMA), Transocean Services AMA JLT, UAE



Mr. Murrell is a Company Security Manager in the Offshore Drilling Industry and has over 32 years international experience in the Military and Security Management and as a Senior Security Risk Consultant for Fortune 500 companies and governments. Ben wrote the company's Corporate Security and Emergency Management Manual and is the author of 'Installation Physical Security Guidelines', which is being used as a benchmark for the physical protection of the companies offshore drilling installations operating

in high risk environments worldwide. Mr. Murrell is Board Certified as a Certified Protection Professional (CPP), and Certified as Company Security Officer (CSO) and an active member on the Chief Security Officer Roundtable Advisory Board of ASIS International as well as a Member of the Security Institute (MSyl) and the Overseas Security Advisory Council.

4. Security By Design in Abu Dhabi

Monday, February 16, 2015: 11:25 -12:15

Breakout 1

The SSPM, the first of its kind in the Middle East, establishes a system for approaching crime prevention and counter terrorism during planning and design that has practical worldwide applications.

In November, 2013 the Abu Dhabi Urban Planning Council launched their newest planning policy document: the Safety and Security Planning Manual (SSPM). The SSPM, the first of its kind in the Middle East, establishes a new system for approaching crime prevention and counter terrorism in the earliest stages of a project's life: during planning and design. The session is designed to introduce important aspects of the new system, including common opportunities and constraints faced by local planners and designers. An emphasis is placed on demonstrating the breadth of the SSPM's practical application, regardless of location, in two separate case studies.

Presenting Speaker:

Hunter Burkall, Associate Director of Security, WSP Global, United Arab Emirates



Hunter R. Burkall, PSP, is a Physical Security Professional and CPTED Specialist with 14 years' experience in physical security planning, design and operations. Hunter recently served as a Security Advisor to the Abu Dhabi Urban Planning Council (UPC) and helped lead an Executive Council project, which established new regulation for how crime prevention and protective security is approached across the Emirate. He is a Security Advisor to the Qatari government on major master

planning projects taking place in Doha. Hunter is also responsible for managing and delivering security works for a number of iconic projects across the region. He is a member of ASIS International and sits on the ASIS Security Architecture and Engineering Council and the ASIS Supply Chain and Transportation Security Council.

5. Counterterrorism Rewards Programs: Government and Private Sector Information Sharing to Counter Growing Threats

Monday, February 16, 2015: 11:25 - 12:15

Breakout 2

The session discusses current terrorism threats in the region, and how information sharing, including the use of rewards programs, can counter these threats.

Countering the regional and global threat of terrorism is critical to the safety of your organization and your employees. To be successful, private industry and government professionals must seek information from staff members, and they must share this information. While governments can take direct action to stop terrorists, private businesses have more access to timely information. The use of coordinated rewards programs can provide a great path for employees to keep themselves and their organization safe. Learn about current threats, rewards program success stories, and how to coordinate counterterrorism efforts.

Presenting Speakers:

Brian Wood, Diplomatic Security Service, U.S. Department of State, USA

6. Does Fraud Matter?

Monday, February 16, 2015: 11:25 -12:15

Breakout 3

Organizations perceived to lack the willingness or capability to fight fraud

run the risk of damaging their reputation. Zurich Insurance deploys a comprehensive framework that addresses fraud and crime pro-actively.

Uncoordinated and fragmented attempts to combat fraud are inefficient and ineffective. The deployment of an overall framework for managing activities that address fraud is essential to provide a holistic approach to enterprise risk management. The intention is to show the approach Zurich Insurance has chosen to protect itself and to share with the audience a comprehensive arsenal of fraud fighting tools. The audience will get an understanding of fraud risks a multinational organization faces and how these are being mitigated. They can then reflect on how components of Zurich's anti-fraud framework may help enhance their organization's fraud control environment.

Presenting Speaker:

Torsten Wolf, Head of Group Security Operations, Zurich Insurance Company Ltd., Switzerland



Torsten Wolf is the Head of Group Security Operations for Zurich Insurance. In his role he leads the Group's efforts to deploy security standards worldwide and to oversee the prevention, detection and response to non-claims related crime and fraud directed against Zurich. Torsten looks back on more than twenty years in the insurance industry where he worked across personal lines and large corporate business. Torsten is a Certified Protection Professional as well as a Certified Internal Auditor and holds a Degree in Business Studies and Economics as well as a Master Degree in Business Administration. He is a regular presenter on topics of security, crime and fraud at international conferences.

**7. Enhancing Threat Analysis through Community Engagement.
Leveraging Local Knowledge to Secure Operations in East Africa**

Monday, February 16, 2015: 13:30 -14:20

Breakout 1

In East African countries community engagement during threat analysis is of particular benefit to the eventual design of risk controls by detailing the beliefs and motivations of human threat sources.

The complexities of societies and communities in countries across East

Africa stem from the multiple layers of tribal, ethnic, religious and linguistic differences and identities set against a backdrop of economic inequalities, evolving governance structures and continuous human development challenges. Threat analysis informed by community engagement can help to identify local, cultural and tribal attitudes to security threats which can help highlight key gaps in a western security approach. Simply identifying the same 50 security risks without analysing them specific to the local area leads to risks which are incorrectly assessed and as importantly sees opportunities which are under-exploited.

Presenting Speaker:

Tim Jones, *Head of Advisory Services, Edinburgh International, United Arab Emirates*

Tim Jones is the Head of Advisory Services at Edinburgh International (EI). He runs a team of analysts and consultants who analyse and distribute political and security risk reporting and deliver consultancy services across the Middle East and Africa. He has a Masters in International Development and is a member of ASIS. He has worked as a security professional in Nigeria, Tanzania and Kenya as well as across the Middle East and Central Asia. Prior to joining EI he served for eight years in the British Infantry completing two tours of Afghanistan and a tour of Iraq during which he worked as an intelligence liaison and targeting officer to a Task Force within the US Special Operations Command. He is based in London but travels regularly in the Middle East and Africa.

9. 2013 API 780 Risk Assessment Methodology: Rationale for Use, Best Practices, Implementation and Benefits

Monday, February 16, 2015: 13:30 - 14:20

Breakout 3

The purpose of this panel is to discuss the applications of the new API methodology in a diverse industrial environment.

The Ministry of Interior of KSA has made the use of the API methodology mandatory to assess the security risks facing major industrial facilities. The updated version (API 780- 2013) differs in many ways from its predecessor. The panel of experts is engaged daily with this updated version. For many security managers, there is confusion whether to continue with the old methodology or require the updated version from the security consultants they

intend to select for a project. The panel will answer their most important questions: What has changed? Is the old version obsolete? Which one should one choose?

Presenting Speakers:

Jean Perois, CPP, PSP, PCI, Senior Vice President, Risk & Co, Bahrain

Jeff Lee, ASIS ARVP Region 3, Saudi Aramco, KSA

Scott Chapel

David Moore



Jean Perois, CPP, PCI, PSP is a seasoned professional with a varied experience in the GCC where he has been operating in professional and managerial capacities for the last ten years. ASIS International Certification Representative for the ME, he has led numerous CPP and PSP review courses in the region, and led the 2 days CPP review course in Dubai at the last ASIS Middle East conference in 2013 and 2014.

Jeff Lee, ASIS ARVP Region 3, Saudi Aramco, KSA

Scott Chapel

David Moore, President & CEO, AcuTech Consulting Group, USA

David Moore is the President & CEO of the AcuTech Consulting Group. Mr. Moore has over 35 years of experience and is as a leading security and process safety management consultant to global corporations. AcuTech was the lead author of the ANSI/API Standard 780 "Security Risk Assessment Methodology for the Petroleum and Petrochemical Industries" and the CCPS® "Guidelines for Security Vulnerability Analysis for Fixed Chemical Facilities". He is a recognized expert in and frequent speaker on risk assessment for security. He also was the project manager for the initial development of the Chemical Facility Anti-terrorism Standards (CFATS) as a prime contractor to DHS.

**10. The Three Pillars Approach: Effective Staff Travel Safety
Systems for Today's International Business**

Monday, February 16, 2015: 14:25 - 15:15

Breakout 1

A competitive global economy means staff are traveling to riskier locations. Ensure the integrity of your organization's travel security systems by applying the Three Pillars Approach.

A competitive global economy means businesses are pushed to explore new endeavours – which can mean staff traveling to riskier locations. As they do, the business turns to the organization's security management to ensure staff safety. In this session, you'll learn the Three Pillars approach to travel security. Taught by two security professionals with extensive expertise working in at risk locales, this session will cover: 1. Pre Trip Briefings – how to equip staff with timely, relevant safety information 2. Travel Tracking – ensure you know staff whereabouts 3. Contingency Planning– be prepared to respond to an international security incident.

Presenting Speakers:

Scott Ruddick, *Global Security Advisor, MEDA, Canada*

Steve Ritchie, *Global Security Advisor, MEDA, Canada*



Scott Ruddick is Director, Security Services with MEDA (www.meda.org), a Canadian based international aid organization. An interdisciplinary risk management and security professional who specializes in humanitarian aid, he brings 15 years of security experience in conflict and at-risk zones, across five continents. Scott is an engaging presenter, who has taught courses and seminars on international issues for a number of universities.

Steve Ritchie is the founder of Risk Visibility, (www.risk-visibility.com), a consulting firm that provides security management services to organizations working in at risk zones. A former member of the British Armed Forces, Steve has worked in many of the world's 'hot spots', assisting international organizations with establishing effective security management systems and managing the risks inherent in working in volatile environments. Steve is a sought after presenter on risk and security issues.

11. What's the Difference Between Crisis Management and Emergency Response?

Monday, February 16, 2015: 14:25 - 15:15

Breakout 2

This presentation explains what constitutes an emergency versus a crisis, and provides best practice guidance on how each can be prepared for and responded to.

There is often confused language when it comes to crisis management – emergency response, crisis communication, incident management, event management. All of these operational response processes are vital in a crisis; but in our view crisis management sits above them at the highest strategic level of the organization. Effective crisis management therefore goes beyond the initial cause of the crisis focusing not only on what happened but what is at stake for a company: reputation, financial bottom line, license to operate, ability to continue operating with consumer and employee confidence, and in some cases its own survival.

Presenting Speaker:

Stephan Engel, *Managing Director, Register Larkin Middle East. UAE*

Mike is an international authority, author and lecturer on reputation, issues and crisis management. A French speaker, his pioneering work in the field of crisis communications began with the Gulf Oil Corporation in 1979, where he dealt with one of the oil industry's worst disasters – the tanker explosion at Bantry Bay in Ireland. He went on to initiate many of the best practice systems, procedures and training programs designed to enable companies to handle effectively the communication aspects of crisis situations. Mike now regularly trains senior executives on how to effectively manage their response to a crisis and provides strategic advice to executive teams when incidents occur. In addition to many papers on reputation management and crisis communications, he is the author of *Crisis Management*, published by Century Hutchinson, and *Risk Issues and Crisis Management* co-written with Judy Larkin.

12. The Sinking of an Oil Platform - a Crisis Management Event

Monday, February 16, 2015: 14:25 -15:15

Breakout 3

Events followed in rapid succession, escalating and complicating the problems

as situation became increasingly perilous. In the few minutes all of us began to comprehend the full scope of the crisis. Once we understood it, we realized that the event become one of survival. The fog of communications & responsibilities occurs in any crisis, what happens when key personnel are injured from Command & Control? Testimony from a survivor onboard when the oil platform sunk and how these lessons learn will apply to any corporations.

Presenting Speaker:

Shawn Winter, *HSSE Consultant, Independent, Italy*

Shawn Winter has many years of progressive Operational and Directorship in formatting policies within the Private Sector and US Government. Since 2005, he has been in the private sector working for Major Energy, Maritime and Aviation Corporations throughout Eurasia, Africa & Middle East. Additionally, involved in three separate hostage negotiations in Somalia and Syria. Before entering the private sector, he was the Anti-Terrorism & Force Protection Director for Europe & Africa at Military Sealift Command for 5 years. Upon accepting this position, he retired from the US Navy after 30 years with his last assignment was with the NATO Strike Force - Special Operations Command, Allied Forces Southern European Command in Naples, Italy.

14. Re-Thinking All Hazards Risk Assessments

Monday, February 16, 2015: 15:45 - 16:35

Breakout 2

An all-hazard approach to risk assessments and preventive measures seems efficient but it may lead to inaccurate risk prioritization's because of a lack of emphasis on rigorously analyzing security threats.

The increasingly common "all hazards" approach to the development of a risk assessment is flawed due to the different methodologies used to assess threats and hazards. Due to the different components involved in assessing natural hazards and accidents as opposed to threats, a common methodology, while seemingly efficient, may potentially lead to inaccurate results. However, with some additional analytical work, the "all hazards" may be effective where an Enterprise Risk approach is adopted that comprehensively addresses all risks that may be pertinent to the assessed entity, whether it is a government, company, building, or any other entity.

Presenting Speaker:

Michael Edgerton, *Principal, Good Harbour International Consulting, USA*



Michael Edgerton, CPP, is an international security consultant whose work focuses on maritime security, security risk management, critical infrastructure protection, crisis management, and security sector reform. He has worked in numerous countries in North America, Asia, Africa, and the Middle East. Prior to entering the private sector, he served in the United States military as a commissioned officer for 20 years where he spent much of his career specialized in security and intelligence. Mike has an undergraduate degree from Bucknell University, a Master's Degree from the National Intelligence University and is a graduate of the

U.S. Naval War College. He is the author of the book, "A Practitioner's Guide to Effective Maritime and Port Security".

15. Security without Borders

Monday, February 16, 2015: 15:45 -16:35

Breakout 3

Discuss new technology that an organization can employ to maintain a secure but open environment extending to its mobile workforce and allowing critical communication during and after an event.

Historically security has been associated with borders. Today an enterprise's most valuable assets, a combination of people, ideas and information, are neither protected nor contained by traditional borders. Recognizing this, many core concepts of security need to be re-examined: What is the value of protecting a facility when much of the workforce operates from somewhere else? How do we assess the status of an organization when significant parts of it are not only remote, but mobile? How do we provide for the safety of lone workers or small work groups outside the reach of organizational response capabilities? These questions are leading to the development of a new class of security solutions and services to meet the needs of the dynamic, distributed, mobile organization.

Presenting Speaker:

Kevin Daly, Chief Executive Officer, Maxxess-Systems, USA



Dr. Kevin Daly is CEO of Maxxess Systems, a U.S.-based leading provider of proven software and hardware for a wide range of integrated, security system configurations. He has more than 30 years of technical and management experience in organizations providing high technology solutions for system control, data protection and electronic security. During his career he has brought several companies from start-up through market acceptance and fiscal stability through both the IPO and the M&A processes. Dr. Daly earned his BSEE at University of Notre Dame and holds a MS, MA and PhD in engineering from Princeton

University. He serves as Chairman of the Board for STEC, Inc., and as a Director at Iteris, Inc., both publically held companies based in the U.S. He is a board member of Project Tomorrow and serves on the Dean's Leadership Council, Bren School for Information and Computer Science at University of California, Irvine.

16. Soft Target Hardening: Protecting People from Attack

Monday, February 16, 2015: 16:40 - 17:30

Breakout 1

Provides a critical examination of vulnerabilities to soft target attack, the perpetrators and their targets. Presents hardening tactics and deterrence/mitigation methodology and activities.

Terrorist attacks occur daily at civilian-centric venues worldwide, and approximately ninety percent of fatalities in modern day wars are now non-combatants. The battlefield lines have clearly been redrawn, with innocent men, women and children caught in the crossfire. The purposeful targeting of civilians and associated breach of moral boundaries is shocking and causes a ripple effect of fear - two primary goals of terrorism fueled by radical religious and political ideology. Despite escalating violence against places of worship, study and leisure around the world, there is a universal psychological "blind

eye" to the threat; as such, we hesitate to explore susceptibility to soft target terrorist attacks and discuss deterrence and mitigation tactics. This presentation serves to enlighten and arm those who secure, own, and operate soft target facilities.

Presenting Speaker:

Jennifer Hesterman, *Academic Author, Taylor & Francis Group, Qatar*



Dr. Jennifer Hesterman, Colonel, U.S. Air Force (retired) is a counterterrorism expert, author and professor. While in the military, she served three Pentagon tours, commanded multiple field units, and was Vice Commander, Andrews Air Force Base, home of Air Force One, where she led base security and escorted the President. She has a doctoral degree from Benedictine University, and Master of Science degrees from Johns Hopkins University and Air University. Dr. Hesterman was a fellow at the Center for Strategic and International Studies and the Harvard Senior Executive Fellows program. She is a member of the ASIS Crime and Loss Prevention Council, contributing editor for

The Counter Terrorist magazine and author of *The Terrorist-Criminal Nexus* (CRC Press, 2013) and *Soft Target Hardening* (CRC Press, 2014).

17. In Harm's Way: Building Successfully Integrated Travel Risk Management, Crisis Response and Evacuation Capabilities

Monday, February 16, 2015: 16:40 - 17:30

Breakout 2

Drawn from real-life case studies, these best practices demonstrate how to successfully implement travel risk management, crisis response and evacuation capabilities.

This session will focus on best practices employed by leading organizations that have successfully implemented travel risk management, crisis response and evacuation capabilities. Topics to be addressed include: (i) successful preplanning – how to build a successful plan that is both functional and usable, (ii) situational awareness – how to manage organizationally relevant information in an era of information overload, (iii) evacuations in action – how to do it right.

The presentation will include numerous case studies drawn from over a decade of experience and the thousands of operations run by Global Rescue for its clients.

Presenting Speaker:

Scott Hume, Associate Director, Global Rescue, USA



Scott Hume is associate director of security operations at Global Rescue. Prior to Global Rescue, Hume spent a career in the U.S. Army as an infantry officer, culminating in promotion to the rank of Lieutenant Colonel. He served globally and in nearly all types of infantry units, including service in the 75th Ranger Regiment. Additionally, Hume earned a B.S. in Computer Science Engineering from Norwich University, an MMAS from the U.S. Army's School of Advanced Military Studies, and an MBA from the University of New Hampshire's Whittemore School of Business and Economics.

**18. A Balancing Act: Building a Robust Aviation Security Solution
Whilst Maintaining a Seamless Passenger Journey**

Monday, February 16, 2015: 16:40 - 17:30

Breakout 3

The future of the aviation industry ultimately requires a balancing act: Building a robust security solution whilst maintaining a seamless passenger journey. Attend this session to learn how.

Whilst today's airports aim to be bigger, faster and friendlier than ever, the threat to airport security becomes increasingly more sophisticated and varied. With the Middle East at the epicenter of the phenomenal growth, how will the region address the need to build systems, meet legislation, revise procedures and train employees to meet that threat, whilst appearing serene, seamless and service-oriented to the travelling customer? Using research into behavior and expectations during the passenger journey, this session will provide insight on how technology and people solutions will help future-proof the aviation security industry during this unprecedented growth phase.

Presenting Speaker:

Waqar Mohamed, Regional Aviation Manager, G4S, United Arab Emirates



Having graduated from the University of Wolverhampton (UK) in Business Studies & Finance, I commenced my career with British Airways in 1990, working in Terminal Operations, Duty Manager and Customer Services Manager roles. In 2007, I became Station Manager for Swissport UK, and after a brief spell at Aberdeen Airport, joined G4S as Station Manager at East Midlands Airport in 2010. With responsibility for over 300 staff employed in all aspects of airport security, I managed to increase operational and compliance performance by over 25% each, and won two awards from ASQ Europe as “Best in Class”. I was Aviation lead for G4S Australia in 2012, before being appointed General Manager (G4S Aviation UK), looking after 14 operational sites. I moved into my new role as Regional Aviation Manager (Middle East) in October 2013, and provide operational and commercial support for all aviation business.

19. Education - the Forgotten Protective Security Measure for Critical National Infrastructure

Tuesday, February 17, 2015: 10:30 - 11:20

Breakout 1

Security education (SyEd) programs work by increasing security whilst reducing risks! This presentation will demonstrate that SyEd is underused in protecting organizational assets against loss, harm or damage events.

Millions of dollars are spent on security technology in protecting organizational assets; especially critical infrastructure. The same organizations budget for security education programs is a fraction of this, if represented at all. This presentation will demonstrate that a proactive security education program will support and enhance the levels of organizational security applications, reduce organizational and personal risks and has the potential to create the biggest ‘bang for the buck’ security benefit used by an organization. The presentation will show that SyEd programs can be used by any organization and represents great value for money, in financially difficult times.

Presenting Speaker:

Andy (Frank) Davis, *Managing Director, Trident Manor, United Kingdom*



Over the last 30 years Andy has worked for various British governmental organizations including overseas assignments in Uganda, Colombia, Venezuela, Saudi Arabia and Pakistan where he was responsible for the security of British governmental assets and operations.

Andy was the Head of Security for a UAE based developer before establishing Trident Manor (Limited) a security, risk and crisis management consultancy based in the UK but with an international reach.

Andy holds a MSc. in Security and Risk Management, is a Chartered Security Professional (CSyP), a Fellow of the Security Institute (FSyI) and holds CPP status. Andy is an active member of ASIS and the CSO Roundtable, sitting on the CSO Leadership Development Committee and other technical and working groups in support of security advancement.

21. Inside Information - Terrorist Use of Intelligence

Tuesday, February 17, 2015: 10:30 - 11:20

Breakout 3

This presentation details some of the methods employed by terrorist groups to collect and use Intelligence in their attack planning. It also explains the Intelligence cycle model in detail.

Terrorist groups routinely collect Intelligence using similar methods to those employed by Law Enforcement, Intelligence and Security agencies. The collected Intelligence is used by terrorist groups for their attack planning, ensuring a higher degree of mission success, resulting in greater casualties and generating wider publicity for their cause. This presentation begins with an overview of the Intelligence cycle, then using a case study of a previous attack, moves on to provide delegates with an understanding of some of the techniques and methods used by such groups to collect, analyse and use Intelligence, and to highlight some of their capabilities.

Presenting Speaker:

Paul Burke, National Security Leader, Middle East & Africa, IBM, United Arab Emirates



Paul Burke is an Arabic-speaking professional with over 27 years' experience in strategic intelligence management. Currently IBM's National Security Leader for Middle East & Africa, he was previously employed as the UK National Intelligence Adviser, in Baghdad (2004-2006) and in Kabul (2007–2009). In Iraq, he worked in counter-terrorism and in Afghanistan he mentored the Intelligence Division of the Counter-Narcotics Police of Afghanistan (CNPA). His work has covered all aspects of Intelligence at strategic, operational and tactical levels. A Doctoral candidate, he will graduate with a PhD in Policing and Security in 2014, with his Doctoral thesis examining "A Review of The Intelligence Cycle and its Effectiveness in Counter-Terrorism since 2003". He holds an MA in Intelligence and Security Studies. Paul is the author of "Open Waters, Hidden Dangers: The Terrorist Threat to Maritime Security".

22. Strategic Thinking about Operational Risk Management

Tuesday, February 17, 2015: 11:25 - 12:15

Breakout 1

This session will explore how intelligence-driven Operational Risk Management (ORM) will help an organization protect, monitor and respond to global and regional events.

This panel of security professionals from various industries will engage in a discussion of what Operational Risk Management means for them. From a strategic level, we will look at Travel, Information Asset Protection, Supply Chain, Fraud, Facilities and other areas of risk. You will learn about where these experts believe the responsibilities lie within an organization and what role intelligence will play in developing and running successful programs. Real-life examples will be used to illustrate how a comprehensive Operational Risk Management program can be used to assess and respond to risk-related issues before, during and after their occurrence.

Presenting Speakers:

Bruce McIndoe, *Regional Security Advisor, Qatar Petroleum, USA*

Ryan Greyling

Leon Duplooy, *Regional Security Advisor, Qatar Petroleum, USA*



Bruce McIndoe is a recognized leader in the travel, intelligence, and risk management industries. As CEO of iJET, Mr. McIndoe is a key contributor to the company's strategic vision and growth. His technical achievements and visionary approach drove Business Travel News in naming him one of the "Top 25 Most Influential People in the Travel Industry". In 2013, he

was appointed to the TSA Homeland Security Science and Technology Advisory Committee (HSSTAC) Task Force. He speaks at numerous industry events and often appears on television, radio, and in print as an authority on global travel and security issues.

24. Non-Standard Behaviour Detection: Risk from Insider

Tuesday, February 17, 2015: 11:25 - 12:15

Breakout 3

The session focuses on development of Non-standard Behaviour (NSB) Detection framework, by using existing tool and technique, to prevent classified business information from insider.

An insider, who has access to organization's information, can misuse it in a manner that can affect confidentiality of information or can result in loss of business. Such insider often displays certain Non-standard Behaviour (NSB). There are several existing data points related to insiders that can be utilized to detect NSB. However, these data points, which often reside in silos with different departments, need to be pulled together under a single framework with the help of available tools and techniques to effectively track NSB indicators. NSB framework development process involves finding answer to several

question such as, who are insiders, why and how do they steal information.

Presenting Speaker:

Pramod Bhatt, Director, Sanofi, India



Pramod is a seasoned professional with over 18 years of experience in the field of security and intelligence. Presently he is working as Director of Security and Intelligence in Sanofi. Earlier, he headed Protective Intelligence practice of Deutsche Bank in South Asia. He was intelligence advisor to regional and global head of Corporate Security and Business Continuity. Prior to this, Pramod worked as a risk management consultant and advised a number of Fortune 500 companies. Before his corporate career, Pramod commanded an intelligence unit of Indian Army. Pramod is an alumnus of Risk Leadership School London and Indian Institute of Management Ahmadabad. He

has spoken at several events such as Strategic and Competitive Intelligence Professional Conference in Philadelphia, ASIS conferences in Orlando, Macau and Kuala Lumpur, CSO Round Table and Asia Crisis & Security Group in India.

26. Detection, Delay and Response – Designing an Effective Physical Protection System

Tuesday, February 17, 2015: 13:30 - 14:20

Breakout 2

This analysis will incorporate properties of the physical protection system and capabilities of an adversary - as projected on a time chart.

Each component of the physical protection system will be broken down and explained. The relationship between each (detection, delay and response) component will be analyzed, with a few examples showing successful and unsuccessful events. The presentation will also explore solutions that can address a faulty design with specific examples. The presentation will have a visual aspect overlaying the properties of each component on charts that can easily allow for the required analysis. This analysis will incorporate properties of

the physical protection system and capabilities of an adversary - as projected on a time chart.

Presenting Speaker:

Sorin Pudroschi, *Regional Physical Protection Lead EAME, Pacific-Northwest-National-Laboratory/DOE/NNSA, USA*



Mr. Pudroschi has over 20 years of combined experience in global security management and operations, physical security implementation for high-value and high-risk infrastructure and facilities, project management, emergency and disaster response, tabletop exercises, law enforcement and successful project implementation at critical sites around the world. He directly supports the implementation of physical security upgrades, system design, and vulnerability and security assessments for the NNSA and DOE's Global Threat Reduction Initiative in Europe, Middle-East, and Africa, as well as other regions. He coordinates with DOE and foreign government officials in

complex, sensitive, internationally-critical, and technically-challenging projects within the Defense Nuclear Nonproliferation Sector. In previous roles, Mr. Pudroschi was the head of security for a number of global high-tech companies. In these positions he was responsible for all physical security operations, security implementations, investigations, executive protection program and regulatory compliance. Prior to these Mr. Pudroschi worked in a law enforcement capacity.

27. Preparing an Enterprise Security Plan Addressing Middle East Cyber Threats & Risks

Tuesday, February 17, 2015: 13:30 - 14:20

Breakout 3

Is your security plan updated to address today's threats to compromise sensitive information? Step through how to leverage ISO 27000, PCI DSS & NIST to develop an enterprise security plan.

Sensitive client information managed by Middle-East businesses is under attack. As business information flows from mobile devices to cloud computing, how is your organization protecting assets under attack? The foundation of information security comes down to one critical document: the enterprise security plan. Step through global standards including ISO 27000, PCI DSS & U.S. NIST to understand how to craft a tailored executive security plan for your business. Examine plan components to establish security priorities for 2015. Be prepared to address cyber attacks & compliance mandates with a well-written and actionable security plan.

Presenting Speaker:

Ali Pabrai, CEO, *ecfirst*, USA



Ali Pabrai, MSEE, CISSP (ISSAP, ISSMP), Security+, is a highly sought after information security & regulatory compliance expert. He has successfully delivered tailored solutions across the United States, Middle-East, India & the Philippines. Mr. Pabrai has been a featured speaker at several conferences, including Naseba (Dubai), ISSA, HCFA, ISACA (Las Vegas), ASIS, HIPAA Summit (Washington DC. San Francisco), Microsoft Tech Forum, Internet World (India), Kingdom Summit (Saudi Arabia), DCI Expo, Comdex, Net Secure, NCPDP, HIMSS, NCSBN & idIndiaExpo (New Delhi). He is a member of the USA FBI (InfraGard).

28. Will Hotels Continue to be the Preferred Soft Target of the Future?

Tuesday, February 17, 2015: 14:25 - 15:15

Breakout 1

Insight on hotel attacks in the Middle East through case studies from presenters direct experience of what really happened and implementation of effective mitigation measures for the future.

From 2003 until 2010, there was an unprecedented escalation of terrorist bombing and armed attacks on hotels in specific regions of the world. However, in recent years this choice of soft target appears to have subsided. Why is this

or are we in a lull before a new storm of attacks. The presentation will examine and forecast future trends and potential attack hotspot locations, then provide case study examples of integrated mitigation and preventative measures such as: the OPTICS principal of total security, CARVER exercises, architectural design, standards and certification, surveillance detection, understanding insider threat, crisis management and emergency planning, intelligence lead operational security.

Presenting Speaker:

Andy Williams, Senior Partner, Temi Group, Finland



Andy Williams is based in Istanbul with the global security risk management company, Temi Group. Prior to this he was Head of Security for TDIC – a UAE government entity engaged in master development of new city builds and tourism infrastructure. This appointment was preceded by 15 years in the hospitality industry, principally with Marriott International- Ritz Carlton as a Regional Director of Loss Prevention within covering Europe Middle East and Africa. On the vocational front, Andy served as a Regional Vice President for ASIS International; is a member of The Security Institute, The Royal Society for Promotion and a former member of the European Institute of Corporate Security Management. He has also worked in liaison with: UK government NaCTSO - The EU Council and United Nations Intelligence Crime and Justice Research Unit on projects relating to counter terrorism and is also an Advisory Board Member of CSARN.

29. Blast Mitigation Measures – a Detailed Look at Products and Approaches to Protect Against Explosions

Tuesday, February 17, 2015: 14:25 - 15:15

Breakout 2

Knowledge is power. This presentation will provide the pros and cons of current blast protection products/techniques to allow attendees to effectively deploy resources to protect people and property.

The world of blast protection has been rapidly expanding and there are now numerous products and approaches to providing protection from explosive attack. Where there used to be two solutions, there may now be ten. It is critical that security and design professionals understand the strengths and limitations of the various mitigation measures, and their applicability to buildings and facilities. This presentation will look at building and site elements (such as windows, doors, exterior walls, curtain walls, columns, beams, and vehicle barriers). The presentation will discuss a) the strengths and weaknesses of these building and site elements when subjected to attack; b) the available products and techniques that can be used to mitigate these weaknesses; and c) the relative cost implications of the approaches.

Presenting Speaker:

Hollice Stone, *President, Stone Security Engineering, PC, USA*



Hollice Stone is a leader in the Security Engineering Industry with 24 years engineering, blast, antiterrorism and emergency response experience. She has devoted her career to helping protect people, buildings, campuses, and critical infrastructure from terrorism. Stone recently wrote the latest GSA Blast and Progressive Collapse guidelines and updated the US Army Corps of Engineers blast resistant door and window Guide Specifications.

30. Supply Chain Security: "from Credo to Grave"

Tuesday, February 17, 2015: 14:25 - 15:15

Breakout 3

Supply Chain Security Manufacturing Storage Transportation and Distribution
Main threats and Global trends Security Best Practices

Supply Chain Security: From Credo to Grave will take you to a journey through a supply chain, from raw material, manufacturing, storage, transportation and

distribution of goods. The journey will include main threats, global trends and some Best Practices achieving Security throughout the supply chain.

Presenting Speaker:

Carlos Velez, *Global Security Director, Johnson & Johnson, USA*



Retired LTC from the Colombian Army with over 30 years of experience working for government, international organizations and multinational corporations. Carlos has served in multiple anti-terrorist operations against drug cartels and terrorist groups. He also served in the international arena as part of the UN Blue Berets Corps during the War in former Yugoslavia. After his service, Carlos moved to private sector, occupying managerial positions in first-class corporations: Brinks, Nestle, Johnson & Johnson. Carlos is the Vice Chairman of the SC&TSC for the last two years and he is also the Lead of the Interpol Committee within the LELC, ISO 28,000 Lead

Auditor and currently the Global Supply Chain Security Director for Johnson & Johnson.

31. Holistic Physical Security Using Risk Analysis Methods

Tuesday, February 17, 2015: 15:45 - 16:35

Breakout 1

This paper shows a method for holistic physical security risk analysis. Threat and vulnerability analysis are Integrated, using risk analysis methods such as fault trees and event trees.

For a physical security of properties, a comprehensive and integrated approach to security is important. The analysis must take into account both internal and external threats and how these can exploit a vulnerability, intentionally or accidentally. This presentation illustrates how risk analysis techniques, including fault trees, can be used for physical security risk analysis, by integrating threat and vulnerability analysis with a comprehensive and integrated approach. This risk analysis method also includes a way for prioritizing risk treatments and consequently an effective use of controls measures for physical security. This method is demonstrated

in a case study, for the storage of invaluable medieval manuscripts, for which a holistic approach to security risk analysis is necessary.

Presenting Speaker:

Bödvar Tomasson, *Division Manager, Fire, Risk @ security, Fire Protection Services, Iceland*



Bodvar Tomasson has a Masters degree in Risk and Fire Protection Engineering from Lund University, Sweden. He is a Division Manager for Fire & Risk at EFLA Consulting Engineers in Iceland, with over 15 years' experience in risk analysis, security design and fire protection. Bodvar has experience in multi-dimensional security risk analysis. Bodvar is a certified IPMA project manager and has been responsible for risk management systems according to ISO 31000 in large construction projects. He is also involved in further developing the ISO 31000 series as a member of ISO/TC262 Project Committee: Risk Management, on behalf of Iceland. As a member of the ISO/TC 223 Technical committee: Societal Security, Bodvar is involved in developing standards for the protection of society from, and in response to, incidents, emergencies and disasters, notably the ISO 22301 standard for the Business Continuity Management System.

32. Global Screening: Close Security Gaps and Reduce Risks

Tuesday, February 17, 2015: 15:45 - 16:35

Breakout 2

Global screening helps prevent employee fraud, ensure compliance, and reduce legal risks, but 85% of employers aren't conducting them. Learn critical global screening steps and how to avoid common mistakes.

Eighty-five percent of organizations have a critical security gap that leaves them open to risks for employee fraud, security issues, and legal liabilities – they are not conducting global background checks. Businesses are sourcing candidates globally for offices around the world. Understanding and verifying these candidates' employment and education experience as well as other facets of their backgrounds is critical, but screening candidates on a global scale is complex and fraught with pitfalls. The type of data available to be verified, employment laws, privacy regulations, process requirements, and cultural views of screening all vary drastically from country to country and these differences can

impact how screening is conducted. This session identifies common mistakes and how to avoid them and explores how to best navigate global requirements.

Presenting Speaker:

Dan Shoemaker, Senior Managing Director, EMEA and APAC, HireRight, USA



Dan Shoemaker is Senior Managing Director, leading HireRight's EMEA and APAC business including market strategy/development, business development, client support, and delivery of HireRight solutions based in London. Prior to HireRight, Mr. Shoemaker was with Altegrity company USIS, serving as director of the Central Business Unit. Prior experience includes serving as Assistant Secretary of Transportation for the Commonwealth of Virginia and managing government affairs for the National Air Transportation Association. Mr. Shoemaker served as the 2009-2010 Chairman of the National

Association of Professional Background Screeners (NAPBS), where he oversaw the development of chapters in Europe and Asia-Pacific, meeting the new demands of a globalizing industry. Mr. Shoemaker holds an MBA from the McDonough School of Business, Georgetown University, and a BA in Geography from Virginia Tech.

33. Private Security in High Risk Environments

Tuesday, February 17, 2015: 15:45 - 16:35

Breakout 3

Private security service providers are playing an ever increasing role in high risk environments. New contracting requirements, international standards, and liability issues are changing the playing field.

Private security service providers are playing an ever increasing role in high risk environments. New contracting requirements, international standards, and liability issues are changing the playing field. The governments of the US and UK have adopted the ANSI/ASIS.PSC.1 as a requirement for contracting, with some private companies following suit. ISO is transitioning the ANSI/ASIS standard to an ISO International Standard. How do you keep your business competitive and use the standard to improve your business management and

differentiate your company to receive contracts? What do you need to know about the new contractual realities and consequences of clients requiring certification to the PSC standards?

Presenting Speaker:

Marc Siegel, *Commissioner ASIS GSI, ASIS International Global Standards Initiative, USA*



Siegel is the Commissioner heading the ASIS International Global Standards Initiative developing international and national risk management, resilience, security, and supply chain standards as well as provides training on their implementation. He is a RABQSA International certified Business Improvement Lead Auditor, as well as a certified Trainer and Skills Assessor for both security and resilience management. Dr. Siegel pioneered the concept of applying a systems approach to security and resilience management for organizations and their supply chains. His work includes providing training and guidance on implementation of risk, resilience and security management systems, as well as risk management in regions of conflict and weakened governance for the protection of assets and human rights.