FULL CONFERENCE PROGRAMME

SUNDAY, 17 FEBRUARY

10:00 - 13:00 Middle East Advisory Council (by invitation only)

14:00 - 18:00 Workshop on Emerging Markets (Pakistan, Libya, Syria, Iraq)

18:00 - 19:30 WELCOME DRINK at the InterContinental Festival City Events Center

MONDAY, 18 FEBRUARY

08:30 EXHIBITION OPENING: H.H. Sheikh Maktoum Bin Mohammed Bin Rashid Al Maktoum, Dubai, UAE

09:30 - 10:00 KEYNOTE: Amin H. Nasser, Senior Vice President, Upstream, Saudi Aramco, Saudi Arabia

10:00 - 10:30 COFFEE BREAK

Session 1
10:30 - 11:20 Middle East Security Overview: A Round-up of the Region
Sam Wilkin
Middle East Analyst, Control Risks, UAE
Summary The session will cover the current geo-political climate and security overview in the Middle East, finishing with an outlook for the region.
Abstract With the Middle East experiencing such rapid change over the last two years and remaining in flux, Control Risks will set the scene for the conference with their Middle East security overview. Looking at the political backdrop, Control Risks' Middle East analyst will examine the security environment and give delegates a regional outlook, looking into the latest risk of operating in the Middle East against the prevailing political and security backdrop.
Biography Sam Wilkin sits on Control Risks' Middle East and North Africa global risk analysis desk. Sam consults clients on political and security risks in the region, with a particular focus on Iraq and the Arabian Peninsula, travelling frequently throughout the region to inform his analysis. Sam previously worked at the think tank Institut Français des Relations Internationales (IFRI) in Paris covering energy issues in Europe and the Middle East. Sam holds a first class honours degree in Arabic and Persian from the University of Edinburgh, spending time living in Yemen and travelling widely throughout the region. He speaks proficient Arabic, Farsi, French and Spanish.

Session 2
10:30 - 11:20 Cyber and Physical Threats to Industrial Control Systems
Shawn Cochran
CPP, Senior Associate, Booz Allen Hamilton, USA
Summary Understanding threats to Industrial Control Systems: Participants will review ICS/SCADA security breaches to better understand attackers and their motivations; discuss current and evolving threats, vulnerabilities, exploitations, and learn how to implement an ICS risk assessment framework.
Abstract Ominous at a minimum, critically destructive at a maximum, threats to Industrial Control Systems are increasing in frequency and sophistication. Whether these attacks are motivated by financial gain, theft, espionage, or a political agenda is immaterial. The issue at hand is that Industrial Control Systems are among an organization's most critical digital assets and must remain secure and available at all times. Traditionally, Industrial Control Systems manufacturers have prioritized functionality and availability over security; however, the evolving nature of the threat, and the criticality of these systems requires a fundamental change in how we approach security to ensure these threats do not go undetected and are addressed before any damage becomes irreparable. These assets merit a primary security investment because they are critical to business operations continuity, service reputation and revenue stream preservation. Recent initiatives reflect an increased awareness of security concerns, but more remains to be done.
Biography Shawn Cochran has 23 years of leadership experience spanning careers in the communications industry and the United States military. He is a management professional with global experience in coordinating, developing and implementing anti-terrorism, emergency preparedness, crisis management, and disaster recovery programs in dynamic and rapidly changing environments around the world. He has led vulnerability assessment teams in support of the public and private sectors, and has keen insights into corporate issues, standards and challenges. He brings subject matter expertise in areas encompassing: physical and cyber security, data and communications networks; technical analysis of telecommunications infrastructures; international coordination; civil emergency preparedness; Continuity of Operations Planning; Continuity of Government; and, information sharing between critical infrastructure/key resource owners and operators in the Federal Government and the private sector.

Session 3
10:30 - 11:20 Safer Cities through Improved Situational Awareness
Lee Wagstaffe
PSP, Technical Account Manager, CNL Software, UAE
Summary We review the technology which enables cities such as Washington DC, Atlanta GA, Manchester and London (UK) to deter crime through improved situational awareness. The integration of disparate physical security systems leads to a more proactive approach to event monitoring and response.
Abstract Governments inherently have an obligation to protect their citizens as well as provide a safe environment for visitors. Successful "Safe City" projects can serve as a model for Middle Eastern governments as a way to improve the safety and security of people, property, assets and reputation. New technologies such as PSIM allow governments to improve their situational awareness and help them detect, deter and defend against threats. In the current economic situation it is necessary to have a security environment that maximizes performance, increases efficiency and allows better use of existing investment in security infrastructure while reducing the cost of management and improving the ability to adapt to future requirements. Through case studies we will be sharing some of the key considerations involved when implementing the citywide safety and surveillance program, taking tips from major deployments in Washington, DC, Atlanta, GA and Manchester, UK, each securing millions of residents and visitors from violence, crime and acts of terror.
Biography Lee began his career in security in 2003 when he transitioned to the Security Industry from the IT industry. Involved in implementing some of the first IP CCTV systems for public space surveillance for towns and cities in the UK. Rising through the ranks and relocating to the Middle East in 2008 Lee has been responsible for the design and implementation of several large scale infrastructure projects across the region. Lee Achieved PSP accreditation in 2010. "Joining the ASIS International Dubai Chapter was a real plus for me" he says "It allows me to broaden my network connections as well as increasing my knowledge in areas which I do not come into daily contact with through my employment". Currently Lee is employed by CNL Software where his primary role is managing the design and deployment of large scale command and control systems for the Security, Police and defence sectors. Lee will be presenting a talk on "Safe Cities" based on our many years of experience working with Manchester Police as well as more cent experience in the cities of Washington, DC and Atlanta, Georgia (USA).

Session 4
11:25 - 12:15 Top Vulnerabilities Affecting GCC Banks
Tarek Naja
Security Consultant, Verizon Business, UAE
Summary In the past few years our threat and vulnerability team has done numerous assessments against banking applications of some of the biggest banks in the GCC. The assessments uncovered nearly 200 hundred vulnerabilities. The talk discusses some of the top vulnerabilities and their effect.
Abstract GCC banks operate similar if not identical banking platforms that Verizon Business; throughout working with these banks, has identified numerous flaws in. Flaws would range from executing fraudulent transactions to compromising entire databases. A number of the biggest banks in the GCC have requested that Verizon Business conduct a security assessment of their banking platforms. Verizon Business deployed the highly skilled Threat and Vulnerability penetration testing team that extensively tested applications such as: Internet Banking, Retail Banking, Corporate Banking, CMS, Brokerage, Trading Platforms, Wealth Management Platforms etc. Over two hundred vulnerabilities where identified in the space of 6 month. The talk will discuss the top five of these vulnerabilities; some of which are relatively easy to find and exploit resulting in serious impact on the business. Real world examples will be shown to emphasise the impact of such vulnerabilities. Following that, a number of recommendations will be provided on how to identify and remediate such issues.
Biography Tarek is a security consultant with an MSc in Information Security and specializing in penetration testing. Working alongside diverse and highly skilled teams Tarek have been involved in countless comprehensive security audits for global applications platforms, and have experience in the telecommunications, financial and media business sectors. Tarek is currently leading the Verizon Business Threat and Vulnerability team in the Middle and Africa.

Session 5
11:25 - 12:15 Clouds Computing: A Study in Practice
Khaled Alamri
CEO, EBTCO, Saudi Arabia
Summary The session will cover information protection, remote computing information security, how to secure access to corporate information for remote workers and challenges for clouds computing.
Abstract Today the need for advance technologies in clouds computing requires demand for better security. Giving access to the corporate infrastructure at the domain level or at the least access point requires attention to security measures governing the secure clouds model. As demand increases for online computing such as eLearning, emarking, outsourcing and offshore extensibility and availability, we see huge gap in security measures and setups for controlling and securing access to the corporate information. The online experience

promises a lot to business owners. It offers ease of access to the workspace, lower investment by companies, less requirements for space and furniture and much more. Therefore, the tendency for secure cloud models gives corporates, governments and other sectors a jump over advance computing and technologies through implementing security measures to protect the corporate data via online computing. Furthermore, business owners require enhanced tools leveraging today's available utmost technologies in current infrastructure to monitor and measure the online performance through clouds computing. In fact, there are smart metrics that we can use to ensure proper use of office hours for those who connect over the clouds. It is an interesting experience with intelligent tools to unlock the online experience for securing access to organization's network, data and physical nodes.

Biography Khaled Alamri has over 10 years of vast experience in IT sector with knowledge and expertise in areas of information security, biometrics, VoIP, RFID, software engineering, management, sales and marketing. Featured twice in "up-to-date" TV show Saudi channel 2 discussing Automated FingerPrint Identification System (AFIS) and Biometrics in general such as Iris, Facial, Vein and other technologies. Wrote several articles in major newspapers and magazines such as Alriyadh Newspaper, Alwatan and others. Interviewed by Dar Al Hayat on security business growth in the region. Designed, developed and implemented complete high-end solutions to fortune 100 companies in the Middle East to solve critical business applications and enhance productivity.

Session 6
11:25 - 12:15 Antalya Airport Private Security Outsourcing Experience
Dirk Schusdziara
General Manager, Antalya Airport, Turkey

Murat Kösereisoğlu
General Manager, Securitas, Turkey

Summary Antalya Airport Terminals are operated by private Operators IC-Fraport. The Operator has decided to outsource its inhouse security. The presentation will show experience of outsourcing 1200 guards.

Abstract In Turkey Antalya Airport Terminals are operated by private Operators IC-Fraport. The Airport serves 14M passengers/year. The Operator has decided to outsource its inhouse security. This is the story of an "experience of outsourcing" 1200 private security guards. Before and after an outsourcing experience. The nature of a seasonal Airport, the fulfilment of International and National Aviation Security standards as well as matching optimization in manpower planning. Two sides of the coin, the Operator's view and the Contractor's view. The challenges the parties have faced the joined organized effort they have put together. The key performance factors for a successful outsourcing. The outcome and the future plans. The Operator's General Manager Alexander Laukenmann together with the Private Security Contractor Securitas General Manager Murat Kosereisoglu presents their perspectives of the experience.

12.15 - 13:30 LUNCH BREAK

Session 7
13:30 - 14:20 Session to be confirmed

Session 8
13:30 - 14:20 Corporate Manslaughter. Get prepared.
Roger Warwick
CPP, Senior Partner, Temi Group Pyramid International, Italy

Summary Governments around the world are introducing corporate criminal liability laws for Corporate Manslaughter. They have already imposed enormous fines on international corporations and long prison sentences on management, including security management. Security Management needs to find out now what is happening and get prepared.

Abstract Do you know how corporate manslaughter could affect you and your corporation? A thorough understanding of this potential legal minefield will be provided in this session. Through examples from international jurisdictions and case studies, this presentation will help you understand the problem and turn it into an opportunity for security management by establishing across-the-board relationships. Learn how to develop country risk assessments to identify problems that employees could face from both a political as well as a legal perspective. Learn how to influence and interact with your legal, human resources, health, and safety department heads to set up and implement adequate global security procedures.

Biography Roger is the MD of Pyramid International, a Security & Investigations Company based in Italy, a Senior Partner of Temi Group, an International S&I consultancy, a certified ISO 27001 and 28000 Lead Auditor and Security Management Systems Skill Examiner. He has pioneered the involvement of ASIS in International Security Standards and received the ASIS Presidential Award of Merit for the provision of information to

leadership and the encouragement of member involvement in the development of International Security Standards. He is a consultant to ISO, CEN, UNI and the European Commission on security matters.

Session 9
13:30 - 14:20 Critical Infrastructure Protection Energy Sector
Dr. Cyril Widdershoven
Business Development Manager, TNO, The Netherlands
Summary Security threats to oil and gas/energy infrastructure is underestimated. Low-intensity warfare (terrorism, political unrest), in combination with Cybercrime, is potentially a lethal threat to ongoing and future energy projects worldwide. An integrated approach (security - oil/gas) is needed to counter these threats in full.
Abstract The increased political insecurity in oil and gas producing regions, in combination with interconnectivity and dependency of the global market, make it a playground for new security threats. Ongoing research has shown that current security applications put in place at upstream, midstream and downstream projects does not take into account the fact that real parties pose an existential and operational threat. TNO's ongoing research and collaboration, based on its long technology development and consultancy to the global defense industry (NATO ao.) in combination with its ongoing consultancy and development projects in the energy sectors worldwide, has brought several new insights to the surface. MENA energy operations and developments are currently not capable of resisting the future threats, linked to IT Security, Integrated Operations and Physical Threats. TNO's independent and integrated approach brings new ideas and technologies to the market which can be used by operators, service companies and governments alike.
Biography Dr. Cyril Widdershoven has been a long-time observer of the Middle East-North African region and of the global energy market. He is currently BD Manager MENA Oil & Gas at Dutch applied science and technology institute TNO in Delft. In his former positions, he was Senior Manager at Deloitte Financial Advisory Services, focusing on M&A, Due Dilligence and other aspects of the international oil and gas sectors. Before Deloitte, he was Principal Consultant on energy, utilities and chemicals issues at global consulting and advisory firm Capgemini, providing thought leadership to customers.

Session 10
14:25 - 15:15 Today's Role of Effective Global Security and Crisis Response in Business Continuity and Resiliency
Daniel Richards
CEO, Global Rescue, USA
Summary Today's global organizations face unprecedented risks. Poor preparation and inadequate systems threaten international operations. Review your plans and systems to identify potential threats and proactively mitigate gaps and omissions.
Abstract The world has changed. Whether due to natural disaster, political instability, terrorism, or cultural conflict, international business operations are more vulnerable today than ever. Traditional systems and levels of preparedness have proven inadequate. Corporate security, risk management, and business continuity professionals must have reliable comprehensive crisis response solutions to operationalize during emergencies and protect human capital. Provoking topics included: 1) The importance of enterprise-wide emergency action planning, and strategies to review and test plans; 2) Effective situational awareness strategies; 3)The pros and cons of leveraging technology as an enabler of effective emergency communication; 4) Lessons learned from recent medical and security emergency events with both optimal and sub-optimal outcomes; 5) Best practices for organizations based upon size and geographical footprint.
Biography Mr. Richards has served as the CEO of Global Rescue since he founded the company in 2004. He has planned and led crisis response services for hundreds of organizations, including extractions from many Middle Eastern, North African, and Central Asian countries. He is frequent speaker regarding crisis response, resiliency, entrepreneurship and insurance topics.

Session 11
14:25 - 15:15 Managing the Risk of Economic Crime
Torsten Wolf
Group Head of Crime and Fraud Prevention, Zurich Insurance Group, Switzerland
Summary Using an overall framework for managing crime and fraud risk in an insurance organization is essential to provide a holistic approach to enterprise risk management. Addressing criminal and fraudulent activities pro-actively will help to protect the organizations assets and reputation.
Abstract The session will focus on the execution of an anti-crime framework in a multinational insurance organization. The purpose of this presentation is to provide the audience with an insight into the criminal and fraudulent activities an insurance carrier is exposed to; the focus will be on the less visible and publicized crime perpetrated by own staff and third parties and explicitly excludes the area of claims fraud. To address these risks a comprehensive arsenal of tools is required to be developed and deployed. The intention is to share the approach Zurich has chosen to protect itself from crime and fraud.
Biography Torsten Wolf is the Group Head of Crime and Fraud Prevention for Zurich Financial Services. In his role he leads the Group's efforts to prevent, detect and respond to non-claims related crime and fraud that is 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 Internal Auditor and holds a Degree in Business Studies and Economics as well as a Master Degree in Business Administration.

Session 12
14:25 - 15:15 ATMs - Regional Threats, Scams and Trends
John Cowling
Senior Consultant, Control Risks, UAE
Summary Overview with case studies examining regional threats, trends and scams relating to Automatic Teller Machines (ATMs) and how you could mitigate the risks.
Abstract Drawing on his experiences in the banking and cash-in-transit sectors, John will provide an overview of the threats facing the operations of ATMs in the Middle East region as well as some of the measures that be applied to mitigate these threats. Purpose: To educate participants in how physical and operational security measures may be applied to enhance the protection of ATMs, in particular those installed out of banking branches (i.e. off-site) in areas that are considered public locations including shopping malls, petrol stations, etc.
Biography John has extensive experience over 20 years working with ATMs, commencing with employment with an Australian leading bank, followed by two major cash-in-transit security companies as well as whilst working in a government maximum security prison well as having interviewed numerous offenders who attacked ATMs and security guards. This unique insight has provided John with numerous consulting engagements related mitigating risks associated with operating ATMs in both Australia and the Middle East region. John qualifications include two diplomas, a range of security industry accreditations as well as business certifications including Audit, Project Management and Training.

15:15 - 15:45 COFFEE BREAK

Session 13
15:45 - 16:35 Sectarianism, Communalism and Jihadism in the Middle East
Hugh McLeod
Director, Stirling Assynt International Group, UK
Summary The regional consequences of Syria's civil war are only now being felt. It still has a long time to run, with increasing effect in the region.
Abstract Commentary on Syria's civil war is often misleading, with talk of tipping-points and a regime on the point of collapse. This is wishful thinking since it will become increasingly inter-communal. Lebanon faces similar issues but key actors are committed to avoiding civil war there. Turkey will see security challenges, and tensions in Iraq will increase, as will sectarian instability more widely. The conflict will intensify tensions with Iran. Most regional powers are doing little to stop militants from travelling to fight in Syria, but their eventual return home may ultimately present a threat to those countries.
Biography Hugh McLeod is a founding member and Director of Stirling Assynt, a leading provider of Country Risk reporting and Business Intelligence. His company Assynt Associates joined the newly-formed group in 2008. This continues the work that Hugh had started in 2003, providing briefing and analysis to large companies and governments. From 2006-7 Hugh was Head of Security Intelligence in HSBC. Before that, he spent 18 years in HM Diplomatic Service, with postings to Islamabad, Accra, Nicosia - where he served as Political Counsellor - and Kosovo. He worked on all of the issues on which Stirling Assynt provides analysis – the FSU, counter-terrorism, Iran and the politics and security of the Muslim world. Earlier he served as an infantry officer for 14 years. His final appointment was to the Military Mission to the Soviet Forces in East Germany, where he was awarded the MBE. He read Russian at Nottingham University.

Session 14
15:45 - 16:35 The Protection of Offshore Oil and Gas Installations
Kenneth R . Lukins
President & CEO, Lukins & Associates LLC, USA

Summary Protection of offshore installations can be difficult and costly, but one critical to ensuring safe and secure operations and protection of your personnel. Exceptional new tactics and technologies are available.
Abstract The threat to offshore installations continues to grow in various parts of the world where piracy and terrorism are expanding their reach. Daily, new policies, tactics, procedures and discussions take place around the globe with the goal of eliminating the threat; but the reality is that the threat can only be reduced, never eliminated, especially in an age where terrorists, pirates, and extremists are well-funded and equipped. While dealing with the threat is the task of governments, addressing the risks and vulnerabilities of assets remains the responsibility of the shareholder. While there is no single approach to asset protection, there are several tactics and technologies now available to aid corporations in their endeavor to ensure that the safety and security of their personnel and installations are properly addressed. We will discuss a brief history, current risks to offshore installations, and new tactics and technologies.
Biography Chief Ken Lukins, U.S. Coast Guard (Retired) has 35 years experience in Facility and Installation Security and Safety, Crisis Management, Anti-Terrorism, Anti-Piracy, Maritime Safety and Security, Environmental and Emergency Response to include Oil Spills, Chemical Releases, Natural Disaster Response,

Law Enforcement/Drug Enforcement, Customs, and Immigration Operations.

Ken has provided First Responder services in Crisis Management, Security and Safety, and related Training, Drills and Support Services for the Energy, Chemical and Transportation Industries, and various governments. Ken has lead team efforts in assessing and developing security operations for numerous ports to include Algeria, Liberia, various Caribbean governments and the United States. He has been responsible for developing and leading all levels of training, drills and exercises focusing on First Responders, Facility Security and Safety, Crisis Management, Anti-Terrorism/Anti-Piracy, Maritime Security and Safety, Spill Management and Chemical Response (Including HAZWOPER - Hazardous Waste Operations and Emergency Response), Equipment Deployment and Health & Safety.

Session 15
15:45 - 16:35 Maritime Security and Organized Crime in Ports
Johan Ohlsson
CPP, PSP Knowledge Manager, Securitas Maritime & Logistic Services, Denmark
Summary Ports and port facilities are very important not just because of terrorism but also because of the fact that most trade passes through a port on it´s way for import and export. Unfortunately Organised crime is present in many ports to earn as much money as possible.
Abstract The content in the presentation is to give an overview to the vulnerabilities of the Global trade lane and the importance of Supply Chain security. Focus will be put on ports and harbours, where transnational crime works to get as much money as possible as fast as possible. Unfortunately transnational crime operates in ports all over the world using any means to reach their goals. What are the risks? How do they work? What mechanisms drive this kind of crime? Some examples will be given how they work with infiltration, corruption and bribe and how they misuse the shift of norms and values.
Biography Johan holds the position as Knowledge Manager in Securitas Competence Centre Maritime & Logistic. Johan has 12 years experience from working with Maritime security within Securitas. He is present in Cooperation of European Security Services (CoEss),Working Comitte Maritime Security and also CoEss representative in SagMas. EU Stakeholder Advisory Group of Maritime Security. In a CEN projekt Johan works with standardisation of private Maritime Security Services in Europe.

Session 16
16:40-17:30 Case Study: Lessons Learnt from Designing and Implementing an Integrated Crisis, Risk, and Security Organisation
Robin Kroha
M.A., Head of CSM Certificate Study Programme, Frankfurt School of Management and Finance, Germany
Summary Using a real world example of a major German bank this session will present the lessons learnt in designing, implementing and continuously improving an integrated security organisation. Aimed at aligning the security function with the company's business and legal requirements the project was multifaceted.
Abstract Corporate Security can, and should, be a major contributing factor to a company's value chain. In reality, however, security functions are more often than not scattered across an organisation. This results in gaps that expose an organisation to risk, and can cause major loss. To avoid these risks, a major German bank with a turnover of approx 180 billion US$ decided to create a security organisation whose main goal was to overcome this challenge. The presentation describes and analyses key elements of this project. This will cover: 1. Establishing a Security Risk Assessment Process to establish the bank's global exposure to risk. Using this analysis to identify adequate risk mitigating measures using a GRC (Governance, Risk, and Compliance) tool. 2. Deriving organisational, technical and documental requirements from the risk analysis. Turning these requirements into business processes. Rolling out these processes across the entire organisation. 3. Establishing the organisation and managing that change. Includes highlights of methods and metrics introduced to achieve sustainable quality levels across the entire organisation. 4. Lessons learnt during the set-up of the project, the analytical and decision making phases as well as during the implementation and maintenance and improvement phases.
Biography Robin Kroha is the Head of the Certified Security Manager Study Programme at Frankfurt School of Management and Finance, Germany. He is also a lecturer of the Risk Management and Corporate Security Master of Science programme at University of Applied Sciences, FH Campus Wien, where he teaches security risk management. Professionally, Robin is Director Corporate Security Management at HiSolutions AG, Berlin, Germany. HiSolutions AG is a strategic risk oriented consulting company, and a Certified Security Provider for the German government. He is a certified ISO 27001 Lead Auditor and a consultant to the Federal Office for Information Security. In this capacity, he developed a comprehensive framework for crisis and emergency exercises for German government agencies. Robin's work experience spans 14 years in the sector of crisis and security management. Past positions include Associate Director at Control Risks and Senior Manager at KPMG. He holds an MA in political science from Bonn University.

Session 17
16:40-17:30 Dog vs. Machine

David Loney
General Manager, Impact Canine Solutions, Kingdom of Bahrain

Summary Detection tools are used in the process of identifying threats and assess the level of risk associated with those threats. Without incorporating methods of detection officers are operating in the blind and can only react to immediate dangers.

Abstract Since the 1980s, scientists have been nosing around for opportunities to put detection dogs out of business. So far they've fallen short, but they continue to try. According to recent scientific investigation they might be getting closer. The latest new device, nicknamed "Dog-on-a-Chip," can alert on as little as one-trillionth of a gram of an illegal substance. So far, the sensor has only been programmed to detect cocaine but according to some, it's only a matter of time before it can be unleashed on other substances, leading some to speculate that time may be running out for K-9s that want to keep their jobs. The American Congress have also held hearings on the best way to provide security at airports and it came down to which is better—an invasive imaging machine costing hundreds of thousands of dollars that can see through your clothes or a friendly dog who might lick your hand. Is it time to take stock and pose the questions “Dog versus machine” or should be looking at “how both assist the War against Terror”.

Biography David Loney retired from the Police Service of Northern Ireland in 2007 where he had been the Head of the Police Dog Training School for the previous 6 years and been directly involved in the Police Dog Section since 1986. He is a Home Office and ACPO accredited trainer in all police dog disciplines and has a vast knowledge and experience of various law enforcement techniques and cultures especially in the police dog and conflict management arena, police training, policing a divided society, change management and policing with the community. David was the lead in the design, creation and delivery of national police dog trainers' courses to National Police Improvement Agency standards and the re-design and implementation of all national police dog courses. These achievements were recognised by him being receiving the prestigious Chief Constables Highly Commended Award.

Session 18
16:40-17:30 Intellectual Property Rights
Nadine Naim
Lecturer in Law, University of Bradford UK

Summary The benefits of a knowledge driven economy through Intellectual property rights are the way forward for new business opportunities and as a driving force behind economic growth. We examine intellectual property protection and enforcement mechanisms.

Abstract With the accession to World Trade Organisation (WTO) membership, Trade Related Aspects of Intellectual Property Rights (TRIPS) compliance was a minimum requirement. What this resulted in was a rapid transformation of intellectual property national law from virtually non-existent or minor laws to Western style statutory regulation in the Gulf. The main areas of improvement were on length of protection and enforcement mechanisms. For example, shortly before WTO ascension, Saudi Arabia passed laws in trademarks, copyrights, design rights and patents. Similarly, Oman took steps for legislative reform from 2000, Bahrain from 2003 and Qatar from 2002. The remaining two GCC States were making changes earlier, UAE from 1992 and Kuwait from 1980 . The legislative transformation to date has been at an exponential rate. The current state of affairs stands with the GCC states displaying an unequivocal level of compliance to TRIPS standard to gain credence with their WTO status. The Gulf is no longer dominated by its trade with the Organisation for Economic Co-operation and Development (OECD) and has increased its level of trade with emerging markets, especially Asian markets. As such, with the diversification of its trading partners, the protection of all types of intellectual property rights is essential to future business success. Through intellectual property the region is opening itself up to further foreign investment that can have a positive impact on the economy. This development hinges on the level of success the GCC can demonstrate in the TRIPS plus criteria of enforcement.

Biography Nadine Naim is a UK qualified barrister and Lecturer in Law at the University of Bradford, UK. Her research examines the role of Intellectual Property Rights in the Gulf Co-operation Council (GCC) and the role of Sharia Law in improving intellectual property enforcement. The key focus of the research is to address how compliant the GCC is to its WTO membership and TRIP’s Agreement and to what extent does the EU and US influence the Intellectual Property (IP) protection regimes in the GCC. The research involves an examination of the GCC TRIPS plus pressures, meeting international IP standards and current enforcement mechanisms. Efforts to reduce intellectual property infringement since TRIPS have been met with lukewarm success and therefore the Gulf States need to do more than simply make legislative changes. Now is the optimum time for the Gulf States to form a strategy which seeks economic development in line with the internet age and knowledge based assets.

18:30 - 20:00 PRESIDENT'S RECEPTION at the Al Badia Golf Club

TUESDAY, 19 FEBRUARY
09:00 - 10:00 KEYNOTE: Emotional Intelligence
Prof. Dr. Leonard Yong, Senior Consultant, EuroMaTech Training & Management Consultancy, Malaysia

Biography Prof. Dr. Leonard Yong (PhD; MEd; B.Sc; DAPA) is Senior Euromatech Consultant. He taught for more than 20 years in University of Malaya before retiring as Professor in the Dept of Educational Psychology &

Counselling. Professor Yong has extensive cross-cultural experience in consulting and research for agencies and companies in Middle East, Japan, Australia, and the Asian region. His clients include Petronas, Maybank, Intel, Motorola, Malaysian Ministry of Health, Malaysian Ministry of Women, Family & Community Development, Saudi Arabia Government, Thai Reuters, Kuwait Petroleum Company and Oman PDO.

10:00 - 10:30 COFFEE BREAK

Session 19
10:30 - 11:20 Session to be confirmed

Session 20
10:30 - 11:20 Is the Verification of Vendors Necessary in a Security Plan?
Jenny Reid
National President Security Association, South Africa
Summary Employee screening has been part of the security environment for many years yet employee fraud is still around. Vendor verification appears to be the latest requirement to try and stop fraud in the workplace.
Abstract Vendor verification has become an extension of the procurement or security function. It is believed that more and more companies are expanding their efforts to include various checks suppliers of services and products to organizations. Despite the increased awareness in fronting and fraud, organizations may still make a lot of mistakes in their procurement procedures and practices. These errors can leave companies vulnerable to the things they are engaging with security departments or companies to avoid. Here are some of the common mistakes to avoid: Error 1. Failing to establish a vendor verification policy Error 2. Failing to verify supplier documents Error 3. Failing to check employees of vendors, contractors and temporary employees Error 4. Failing to conduct reputational checks when required Error 5. Relying on a manual internal processes.
Biography Jenny Reid, currently the owner of iFacts, is a pioneer of methodologies used to ensure executives and employees are secure in their environment and companies have honest, ethical, loyal and productive employees. Jenny started in the South African security industry in 1995 and worked her way through the ranks. In 2009 Jenny bought iFacts and developed a purely screening company into an organization providing comprehensive services to ensure employees are safe and secure as well as honest.

Session 21
10:30 - 11:20 Effectively Leading a Multigenerational and Multicultural Workforce
Bonnie Michelman
CPP, Director of Police, Security, and Outside Services Massachusetts General Hospital, USA
Summary This presentation will focus on creative leadership for modern times with specific emphasis on the challenges and tools for managing/leadership a workforce made up of multigenerational and multicultural members.
Abstract We are managing in challenging times and our workforces in all industries have become very diverse. Different generations (e.g baby boomers, traditionalists, Generation X and, Millennium) all are motivated and inspired by different things. They need different approaches and people need strong leadership skills to ensure that these different generations work collaboratively and in a productive way together to achieve the best performance and outcomes. We also are now leading extensive multicultural groups who need to understand each others customs, skills, strengths and perspectives to optimize job satisfaction, performance, feelings of inclusiveness and integration. This seminar will foster thought on how to maximize the management of diverse people and groups to create a highly motivated, satisfied and high performing organization. Creative leadership tools and techniques will be discussed as well as case examples of best practices.
Biography Bonnie S. Michelman has extensive leadership and security management experience in diverse industries. She currently is the Director of Police, Security and Outside Services at Massachusetts General Hospital, Boston, Massachusetts. She also serves as the Partners Healthcare Security Consultant. She was formally District Manager at First Security Services overseeing 60 diverse operations and 1,200 people and Assistant Vice President for General Services/Operations at Newton Wellesley Hospital managing 16 departments and doing significant leadership work.

Session 22
11:25 - 12:15 Panel on Maritime Piracy
Jenny Maclean
Compliance Officer, Maritime Security, Control Risks, UAE
Summary The changing threats in Maritime Security bring unique challenges to PMSCs vessel owners and charterers. Recent piracy trends may be seen as a significant change to traditional operations but nevertheless the threat is still significant and not to be ignored. Beyond the more obvious impact of piracy, we explore in commercial terms in both cost and compliance.
Abstract Over the course of the last 24 months, the profile of piracy incidents has drastically changed and the demand for armed security services has increased. The frequency and duration of piracy attacks has led to significant changes in the risk appetite of all maritime stakeholders. Although an effective response to piracy,

maritime security comes loaded with complex compliance issues. We discuss the current methods employed to counter the latest threat and yet remain within compliance restraints and the local laws and customs around the High Risk Area. Further discussion will look at how the threat may develop or even become insignificant in the short term and dangers of complacency to any vessel owners deciding the threat has totally diminished. Control Risks will look at compliance challenges and their practical implications in the commercial world.

Biography Jenny Mclean is Compliance Officer for Control Risks' Maritime Security services, with a focus on transit operations in the IMO's High Risk Area. Based in Dubai, Jenny works with the Maritime Operations team to ensure changing requirements from port authorities, flag states and client nation states are effectively translated into daily procedures of Control Risks' maritime operations. This requires close liaison with Group Legal Counsel and Insurance Managers to ensure full legal and security.

Phil Tinsley
Operations Manager, Maritime Security, Control Risks, UAE

Biography Phil Tinsley is Control Risks' Operations Manager, managing all aspects of Control Risks' transit security operations. Prior to joining Control Risks Phil held a number of offshore project manager positions, primarily in the Seychelles and Tanzania where he was responsible for managing maritime security teams and offshore assets utilising armed RHIB patrols, host nation naval forces and guard vessels. Phil had a distinguished career in the Royal Marines retiring as Major.

Session 23
11:25 - 12:15 Security Engineering and Management
Haithem AlBalawi
Administrator, Saudi Aramco, Saudi Arabia

Summary Security Engineering and Management are two challenging tasks that hardly can meet. Professional Physical Security Engineers do their best to provide solutions to counter measure threats and risks that an enterprise or an organization can be vulnerable to. However, putting these solutions in to operation's context is the challenge for security managers. This presentation discuss this issue with proposed solutions and also share experiences and successful stories from the region.

Abstract Security Engineering and Management are two challenging tasks that hardly can meet. Professional Physical Security Engineers do their best to provide solutions to counter measure threats and risks that an enterprise or an organization can be vulnerable to. However, putting these solutions in to operation's context is the challenge for security managers. This presentation discuss this issue with proposed solutions and also share experiences and successful stories from the region. The usual practice for a threat and a vulnerability assessment process starts by a concern received or generated from an organization member, could be a corporate executive or an intel information. Then usually the consultant jobs start to assess this threat and propose counter measures. The market has a lot to offer and without the direct interference of the organization security officer, consultants ted to propose what keep them safe "Less Liable". In this topic I will cover more about putting Security in context so any solution implemented can ensure high efficiency and effectiveness. This will consider the organization environment, technology, HR and Management. Under each of these elements, the Engineering, Operation and Support (EOS) model will be applied to all solution in context and focused. The topic will also share some success stories from the region.

Biography Mr. AlBalawi is graduated from King Fahad University of Petroleum and Minerals (KFUPM) with an Electrical Engineering background and is pursuing MS in the same field. He has joined Industrial Security Operations directly after BS degree in year 2000. Mr. AlBalawi worked as a security maintenance engineer during and in 2002 headed the maintenance engineering team under the Security Systems Maintenance Division. After have moved to the Projects Group Mr. AlBalawi represented the organization in mega security projects such as the corporate Security Access Control System. Mr. AlBalawi moved the security operations field and covered as security superintendent in different security operations division kingdom wide. Mr. AlBalawi currently is the administrator for the Security Systems Maintenance Division.

Session 24
11:25 - 12:15 Panel on Hotel Security
Dr. Mohamad Z. Zineddin
Professor, Khalifa University, UAE

Biography Dr. Zineddin is the Director of joint programs and associate professor in practice in the Institute for International and Civil Security (IICS), and the department of Civil Infrastructure and Environmental Engineering (CIEE) at Khalifa University for Science, Technology and Applied Research (KUSTAR). Before joining KUSTAR he was a consultant and lead subject matter expert for Abu Dhabi government in safety and security engineering, protective structures, blast effects on modern structures, physical security, force protection, antiterrorism design and assessment. He obtained his B.Sc., M.Sc., and Ph.D. degrees in Civil Engineering from Penn State University with a specialty in structural dynamics and protective structure. Before moving to UAE, he served as a professor of civil engineering and director of research at the United States Air Force Academy (USAFA).

Simon Howse
Director of Security, Middle East and Africa Marriott International, Ritz Carlton Hotel Company L.L.C, UAE

Matthew Oyston
Security Design, Control Risks, UAE

12:15 - 13:30 LUNCH BREAK

Session 25
13:30 - 14:20 Threats to the Oil and Gas Sector and Risk Mitigation Solutions.
Pete Dordal, Jr.
Senior Vice President, GardaWorld, USA
Summary Threats to the oil and gas sector and risk mitigation solutions, with countries to be discussed Iraq, KRG, Libya, Yemen, South Sudan, Somalia and Nigeria.
Abstract There are many threats to the world supply of oil & gas, all of which are well known to the industry. Labour strikes or localized political instability delay or temporarily close production facilities. Theft of crude oil from pipelines, or transport translates to profit loss for companies, and severe weather can shut down operations on off-shore oil and gas platforms. Such threats, however, are limited in scope and relatively transient in nature. It is a part of doing business in tough and unforgiving environments - especially since the infrastructure through which crude oil, and gas is transported to refineries, storage, and the market, is by its very nature vulnerable. Pipelines stretch through isolated terrain in politically volatile regions, while refineries are too often adjacent to densely populated urban sprawl. Transport of crude or refined petroleum products via sea, rail, or road must of necessity pass through vulnerable geographic chokepoints, such as the Straits of Hormuz, in the Arabian Gulf or Bosphorus Straits in the Black Sea. These same vulnerabilities represent for today's terrorists attractive targets of opportunity. The threat of terrorism to the oil and gas sector is a real concern to the industry and to governments because its scope is not limited and its nature appears to be that of an entrenched, transnational strategy. Persistent, expanding and increasingly sophisticated attacks against oil and gas infrastructure and personnel present a sobering pattern for the industry. For example, terrorists battle-hardened in the Iraq theatre of war can and will export the experience gained from targeting Iraqi oil and gas infrastructure to other infrastructure, facilities and personnel in the Middle East region and inevitably, worldwide. A calculated strike on a key pipeline or refinery can deprive a nation of fuel and cripple its economy. A devastating attack on a tanker at sea or a fuel depot or refinery near populated areas can ravage the environment, sicken or kill many people, and afford terrorists the publicity they seek. In this presentation will review the threat in GardaWorld operating locations, provide insight into the oil field protection projects we manage in Iraq and advise the audience how to mitigate their risks in this sector.
Biography Pete Dordal Jr., is the Senior Vice President of GardaWorld, a risk management and security services company that provides services to the US, UK, and Canadian governments, international NGO's and commercial clients with primary focus on the development, defense, diplomatic, oil & gas, and infrastructure sectors.

James Grimshaw
Managing Director Iraq South, GardaWorld, UAE
Biography James Grimshaw is Managing Director Iraq South of GardaWorld, the Global Risk Management Division of Garda World Security Corporation. He joined GardaWorld in 2004 as operations manager for Vance's Kurdistan business, before taking on a commercial role to support the growth of the Kurdistan business and to develop new markets. Today, James is responsible for GardaWorld's operations in Basra. Given his extensive experience of operating in high risk and emerging markets, James also continues to work with clients to help mitigate political, economic, commercial and security risks. Before joining GardaWorld, James served as Deputy Director of a UK based not for profit organization, managing a number of projects related to post conflict reconstruction. He also managed internal security training for a leading Middle Eastern nation and was commissioned into the British Army in December 1995. James holds a Bachelor of Business Administration degree from Nottingham Business School, where he graduated with honors.

Andy Edwards
Managing Director Iraq, GardaWorld, UAE
Biography Andy Edwards is Managing Director Iraq of GardaWorld, the Global Risk Management Division of Garda World Security Corporation. Before joining GardaWorld, Andy was the Global Operations Director for Peak Group Incorporated and presided over the company's operations until 2008, when he completed the purchase of Peak. Shortly after completing the purchase, he changed the name of the company to Consilium Risk Strategies (CRS). GardaWorld acquired CRS in August 2012 and he was retained as Managing Director Iraq. After leaving the British Special Forces in 2001, Andy worked as a security consultant to a number of blue-chip companies, news networks and international development agencies around the world, including the World Bank Group, USAID, CBS news and the BBC. In 2003, he was appointed as Security Director for Orascom Telecom Iraq (Iraqna) and in this capacity managed the security operations for the rollout of the country's first GSM mobile phone network. During his time with Orascom, Andy and his team recruited, trained and managed a workforce of over 2,000 security personnel.

Session 26
13:30 - 14:20 ICAO Airport Security Requirements
Philip Johnson
Previously with Shen Milsom & Wilke, Director Dubai Office, UAE
Summary To present the guidelines for a common understanding of ICAO Annex 17 standards and recommended practices and the associated guidance for their implementation contained in the ICAO Security Manual for the Safeguarding of Civil Aviation against Acts of Unlawful Interference.
Abstract Global Environment Terrorism Understanding Annex 17 and the Security Manual Establishing the Legal Framework Establishing Coordinating Infrastructure Financial Management Development of Specific Measures to Comply with Annex 17 Including Security Measures in the Design of Infrastructures and Processes Project Management Technology and Equipment Quality Control Human Resources Management Management of Response to Major Security Emergencies International Cooperation Other Issues and Related Aspects.
Biography Philip has experience in comprehensive electrical design specializing in seaport, airport, commercial and industrial low-voltage systems. Design experience includes outside plant, structured cabling, microwave, WAN/LAN, GSM/Cellular, building management, cable management, warehouse inventory management, passenger information display, telephone, public address, CCTV and security systems. Previous project responsibilities have ranged from schematic design through construction administration for both new construction and renovation projects.

Session 27
13:30 - 14:20 Session to be confirmed .

Session 28
14:25 - 15:15 Post Bribery Act: The Competitive Edge vs. Adequate Procedures - Are They Mutually Exclusive?
Nicola Fowler
Corporate Investigations - Consultant, Control Risks, UAE
Summary 1st July 2011 saw the implementation of the "toughest anti-corruption legislation in the world". We explore how an organisation can implement an adequate anti -bribery and corruption compliance programme whilst maintaining a competitive advantage.
Abstract The presentation will establish why the Bribery Act 2010 matters and explore whether its enactment is helping or hindering commercial enterprise. In light of the same, we will consider what an organisation can do to ensure that its onerous requirements are not only met but, through the adoption of a risk based approach to due diligence, that a competitive advantage is achieved.
Biography Nicola is a Consultant in the Corporate Investigations team in the Middle East. Nicola's recent projects have included financial analysis, asset tracing and fraud risk management on behalf of local banks. Nicola is an experienced financial investigator who prior to joining Control Risks worked for the Serious Fraud Office in London where she was responsible for contributing to and managing the investigation and prosecution of serious and complex fraud, corruption and other economic crime in the UK. Nicola is a UK qualified barrister with extensive litigation experience and a strong background in commercial crime.

Session 29
14:25 - 15:15 Assessing Supplier Risk in the Supply Chain
Brad Kingston
Security Manager - Supply Chain Management, L3 Communications - CS West, USA
Summary This session examines the basic principles of assessing security risk for your business and throughout your supply chain. Also assesses risk as pertains to counterfeit parts and violations of the US International Traffic in Arms (ITAR) regulations. Session will conduct a walk-through utilizing a supplier scorecard and utilizes the CARVER vulnerability method in assessing security risk.
Abstract The theme of this presentation is to educate the audience to conduct a supplier risk assessment. The session will conduct a walk-through utilizing a supplier scorecard and the CARVER vulnerability method in assessing security risk. The objectives are to identify threats and security risks within a supply chain, assess the needs and properly apply physical security systems in support of the supply chain security model.
Biography Brad Kingston has over 28 years experience in the security and assessments arena. Brad is the Security Manager for the Supply Chain Management Division, L3 Communications, Communications Systems West in Salt Lake City, Utah. He conducts investigations and assessments for all suppliers to Communications Systems West. Brad is a retired US Army Special Forces Sergeant Major after 26+ years with specialties in intelligence, operations and engineering. Brad has had numerous deployments to include two combat deployments to Afghanistan and Iraq. He has conducted security/vulnerability/threat assessments for facilities and firebases throughout the world. He has a Bachelor of Arts in Criminal Justice Administration and a Masters Degree in Computer Resource Management. He is an active member of ASIS International. Brad provides advice, insight and solutions for security and the entire supply chain to assess risk.

Session 30
14:25 - 15:15 The New Enterprise Security Risk Manager
Jeffrey A. Slotnick
CPP, PSP, President, Setracon Inc., USA
Summary The session addresses three core questions: Are you a Change Agent? What is Resilience and why should I care? How do I help create a resilient organization through security?
Abstract Today's Security professional touches all aspects of Security and Risk Management and all professional aspects of the Enterprise. The CEO, CFO, CIO, COO, CHRO, and CTO are just learning how to interact with the CSO! Part of the responsibility for the education of the "C" suite resides with us! But in order to be effective trainers we first have to study ourselves. This session will assist you in understanding our impact on the enterprise including internal and external relationships (critical interdependencies), the ability to identify all forms of Enterprise Risk, and having a firm grasp of core business management principles.
Biography Jeffrey A. Slotnick, CPP, PSP is a highly regarded security consultant, with more than 28 years of experience, specializing in the Homeland Security Enterprise. Jeff is peer recognized as one of the "critical architects in the homeland security enterprise" and is responsible for the some of the latest advancements in All Hazards Disaster Resilience, Organizational Resilience Management, and Standards Development. In his roles as the President of Setracon, Inc., Co-Founder & COO of OR3M, and Chairman of the ASIS Physical security Council Jeff is focused on the professional development and training of security, law enforcement, and military personnel, the provision of exceptional security services, protective services, risk, vulnerability, and threat assessments, and preparing Emergency Response Plans/ Business Continuity Plans. Jeff is a Reserve Law Enforcement Officer for the City of Centralia Washington.

15:15 - 15:45 COFFEE BREAK

Session 31
15:45 - 16:35 Update on Cyber Threats - Current Stats and Trends in Cybercrime and Espionage
Toralv Dirro
EMEA Security Strategist, McAfee, Germany
Summary Based on McAfee Labs internal data, our Quarterly Threat Reports and other resources, this presentation will give an overview of the current threat landscape, showcasing recent examples and highlight trends, for example a shift in mobile malware.
Abstract McAfee Labs, as the research organization behind most McAfee products and running our various reputation services, grouped together under "Global Threat Intelligence" (GTI) has a very good overview of what is currently happening in the worlds of malware, cybercrime and espionage.Based on our various information feeds, from GTI to customers malware submissions, analysis of malware and external intelligence, this presentation will give a solid overview of the current threat landscape and recent trends we are seeing that could change the landscape. Using concrete and current examples it will give an insight into the threats beyond just the pure numbers that make out any kind of statistics.
Biography Toralv Dirro is McAfee Labs EMEA Security Strategist at McAfee. In this role he is spokesperson for McAfee Labs and works closely with the research teams. He deals with the latest threats, their development and cybercrime as well as new security technologies like McAfee Global Threat Intelligence. He is a frequent speaker on events and conferences as well as to the media. He started his carrier with Dr. Solomon's Software in 1994 being responsible for the set-up of a research lab in Germany. After the acquisition of Dr. Solomon's through Network Associates 1998 Dirro not only worked in the field of virus research but in other aspects of IT security. Network Associsates was renamed to McAfee in 2004. He helds his current position since 2007.Toralv Dirro was born on September 21st, 1970 and studied computer science at the university of Hamburg where he also work at VTC (Virus Test Center).

Session 32
15:45 - 16:35 Assuring Business Competitive Advantage through Eavesdropping Mitigation
Werner Preining
CPP, Responsible for European Operations, Interpol Security, Austria
Summary What can be done to reduce the omni-present threat of eavesdropping on land-lines, VoIP, mobile phones and data transmission? Attendees will learn what tools and credential a serious and trustworthy expert needs to employ to minimize such threats.
Abstract Only those enterprises and institutions that keep their sensitive information secure against eavesdropping will maintain their competitive advantage for the future. But it is of equal importance for most if not all persons to keep their personal data private. The European Union for example specifies the term "sensible data" that refers to "natural persons". "Personal data" are used for Identity theft ! There is no country that did not have its recent eavesdropping scandal, involving often public servants and officials as well, abusing the public confidence. This session shows new and solid ways of prevention that can be applied with certain modification globally. Creating an increased awareness about eavesdropping and the danger / damage involved by the misuse of illegal obtained data. A considerable part of preventive work can be done with organizational measures discussed during the presentation. While after the session the attendees will not become counter-eavesdropping experts, they will be able to recognize trustworthy experts.

Biography As a former merchant-marine captain, Werner Preining works in security since 1980. Joining ASIS in 1984, he became one of the first European CPP's in 1989. Werner specialized in high-end physical-security, Emergency / Disaster Management & IT security. His specialty within the IT-field are eavesdropping measurements. As former PPS he acquired a deep knowledge of demolition, including avalanches and underwater projects. In 2001 he joined the Crisis Management & Business Continuity Council and the IT-Security Council. Since 2006 he is the chairman of the Austrian Chapter 107. In 2009 he qualified as a CMAS, 2010 as a Lead Auditor ISO-28000.

Session 33
15:45 - 16:35 Standards for Private Security Service Providers - Principles and Implementation
Dr. Marc Siegel
Commissioner, Global Standards Initiative ASIS International Belgium
Summary The ANSI/ASIS.PSC.1-2012 standard provides auditable criteria for quality of private security company operations, consistent with respect for human rights, legal obligations and good practices. The standard is now a requirement for contracting in many countries.
Abstract The new ANSI/ASIS PSC.1-2012 standard provides a risk-based approach for the provision of responsible security services in areas of the world where the rule of law has been undermined and private security is needed to protect essential relief, recovery, reconstruction, and economic development that will lead to long term stability and security. The US Defense Department requires conformance to this standard in all new contracts for private security functions. Other countries are considering its adoption as well. Learn how to use the standard to improve your business management and meet contractual requirements.
Biography Marc Siegel is Commissioner heading of the ASIS International Global Standards Initiative. He represents ASIS at the International Organization for Standardization (ISO) and at regional and national standards forums. Siegel works with ASIS International and national standards bodies on five continents to develop international and national risk management, resilience, security, preparedness, and continuity standards as well as provides training on their implementation. He is a RABQSA International Certified Security Management Systems - Business Improvement Lead Auditor as well as a certified trainer and Skills Assessor for the ISO 28000 – Security in the Supply Chain Lead Auditor Certification Program.
As an Adjunct Professor in the College of Business Administration and the Master's Program in Homeland Security at San Diego University, Dr. Siegel pioneered the concept of applying a systems approach to security and resilience management. He has worked with various countries to develop management systems standards for security and resilience in individual organizations, as well as for their supply chains.

16:40 - 17:30 CLOSING SESSION - KEYNOTE: Professionalising Security Professionals in the Current Environment: Global Experiences and the Way Forward.
Narayanan Srinivasan, Professor of Security and Risk , Edith Cowan University, Australia
Biography Nara Srinivasan is Professor of Security and Risk at Edith Cowan University, Perth Western Australia and Director of the Emirates-ECU Centre in Dubai. He completed his studies at the University of Malaya and Cambridge University, UK in areas of Criminology and Public Administration. Nara also completed programmes at Cornell and Harvard Universities in the areas of security management, international security and current trends in security profiling. Nara is engaged in many research projects in the area of aviation and maritime security in Australia, UK, Asia Pacific and the Middle East and works as a consultant to airlines and governments in these regions. He is credited with professionalising the security industry through education programmes globally. Nara is also part of the UN expert group on Civilian Private Security and a member of several professional groups looking at the professionalisation of security including the Australasian Council of Security Professionals.

WEDNESDAY, 20 FEBRUARY - THURSDAY, 21 FEBRUARY

Post-Conference Workshops [Held at the Gloria Hotel, Dubai]

10:00 - 15:15 Emotional Intelligence
Prof. Dr. Leonard Yong
Senior Consultant, EuroMaTech, Malaysia
Summary Emotionally intelligent management embraces and draws from numerous other branches of behavioral, emotional and communications strategies to develop more productive and successful leaders. Understanding and raising your Emotional Intelligence is essential to your success and leadership potential.
Biography Dr. Leonard Yong (PhD; MEd; B.Sc; DAPA) is Senior Euromatech Consultant. He taught for more than 20 years in University of Malaya before retiring as Professor in the Dept of Educational Psychology & Counselling. Professor Yong has extensive cross-cultural experience in consulting and research for agencies and companies in Middle East, Japan, Australia, and the Asian region.
His clients include Petronas, Maybank, Intel, Motorola, Malaysian Ministry of Health, Malaysian Ministry of Women, Family & Community Development, Saudi Arabia Government, Thai Reuters, Kuwait Petroleum Company and Oman PDO.

10:00 - 15:15 International Ship and Port Security (ISPC) Within Oil and Gas
Chris Maylor,
Senior Consultant, EuroMaTech, UAE
Summary International Ship and Port Security (ISPS) Code is one of the main regulatory practices for marine security management, ships and port facilities. ISPS within Oil and Gas programme will provide management and marine personnel responsible for Security of Corporate Marine Assets an overview of the ISPS Code, and relative terms within Oil and Gas Sector and best practice terms in the Middle East.
Biography Mr. Chris Maylor is a Senior Consultant with EuroMaTech in many aspects of security operations, particularly facilities management, covert security operations, close protection, surveillance training and Anti Terrorist Risk Assessments within hostile and non hostile environments. Chris Maylor, a former serviceman, having spent many years in the British Military, in the field of sensitive covert operations within Military Intelligence. Since leaving the UK Armed Forces he has a great deal of experience in delivering security training to the commercial sector, and training teams of people and government agencies to the standards required to undertake their security responsibilities. Additionally he has presented training courses to Governmental and Non Governmental organizations both in the UK and world wide for specialist security and related management operations. Chris has significant experience in operational management roles within the security industry and has been responsible for the operational effectiveness of teams engaged in protracted and complex covert security audits, marine and facilities security, reconnaissance, close protection teams, and technical electronic security solutions.

10:00 - 15:15 Crisis Management and Technological Security for Oil and Gas
Edward Clark,
Senior Consultant, EuroMaTech, UAE
Summary Crisis Management and Technological Security for Oil and Gas, trains individuals to incorporate best practice security management into their daily operational procedures, at a strategic, tactical and operational level. Delegates will acquire the overview knowledge, leadership skills and methods to apply Technical Security and Crisis Management practices to reduce corporate risk.
Biography Mr. Clark is a Senior Consultant with EuroMaTech for more than 10 years. He humbly offers 24 years of experience as a Special Forces Officer (Green Beret) to include combat and security assistance assignments throughout Africa and the Middle East Mr. Clark has 15 years of operational experience in combat and security assistance missions throughout the Middle East and Africa. He also brings over 25 years of formal training as an instructor, training developer and training manager to the project. After 9/11 Mr. Clark was actively recruited to serve as the Director of the Homeland Security Threats Office. It was this assignment that drove him to reverse engineer the CARVER targeting tool to conduct vulnerability assessments on Nuclear Power Plants, Food and Agriculture commodities, and other national assets to include the Ground Based Mid Range Missile Defense System. Mr. Clark has played a key role in developing National level security programs for the United States.

10:00 - 15:15 Security Investigation Techniques
Ken Corlett,
Senior Consultant, EuroMaTech, UAE
Summary Information, knowledge and intelligence are fundamental to the workings of any investigation. The ability to acquire, assess, validate and corroborate sources of information is the key to a successful investigation outcome. This training seminar looks at the techniques, methods and National Intelligence Models, and how these can be effectively deployed according to best practice.

Biography Mr. Ken Corlett is Senior Consultant at EuroMaTech for more than 10 years. He has over 24 years experience as a Senior Police Officer with the Lancashire Constabulary as a career Detective. He has extensive experience in the investigation of serious and organised crime and for building relevant investigation teams to manage related incidents. For the last decade, Ken has been working with the United Nations (UN), across Bosnia, Netherlands and Lebanon engaged in specialist investigative duties and training new and emerging police forces. Within his time at the UN, he has been specifically responsible for field investigations; war crimes cases, acts of terrorism and breaches of international humanitarian law, including all relevant legal processes and actions, for cases being heard at The Hague. Ken has recent assignments working as a Senior Consultant for the US Embassy International Narcotics and Law Enforcement (INL) in Beirut evaluating the US financed police training academy in Lebanon, and until recently Ken held the position of Chief Investigator in the Department of Internal Oversight Services for UNRWA in the Middle East, based in Amman, Jordan.

10:00 - 18:00 CPP Review Course [Held at the InterContinental Festival City, Dubai]
The Certified Protection Professional designation has been recognized around the world as security's highest professional achievement since 1977. Practitioners who have successfully passed the exam to earn the CPP are board certified in security management. The CPP increases job security because it is an individually owned credential that is portable across industry sectors and international boundaries. The CPP Review is a two-day program designed to refresh your knowledge in the major areas of security management tested on the CPP exam. Instruction is based on reference materials that are the source of exam content.

10:00 - 18:00 PSP Review Course [Held at the InterContinental Festival City, Dubai]

The Physical Security Professional (PSP) board certification is the "gold standard" for physical security practitioners - a benchmark recognized since 2003 throughout the security industry. It represents advanced training, educational accomplishment, and dedication to the physical security profession. The PSP is confirmation of your expertise and competence. Securing this prestigious designation takes experience, knowledge, and training - including the ability to pass the rigorous PSP Examination. ASIS helps you prepare with confidence through our comprehensive PSP Review Program.