SECURITY MANAGEMENT – STAGE 2

Millenium Hotel, Doha, Qatar, 26th September– 7th October 2010

BACKGROUND

This university-accredited programme is designed to enhance your ability to implement security risk management and loss prevention programmes that will make a quantifiable contribution to organisational loss reduction goals. The course focuses on developments in security risk management and addresses some of the more complex issues of corporate security management.

The workshop is accredited by Skills for Security (The UK Skills and Standards setting body for the security business sector) and Middlesex University and constitutes the second of six modules that make up the Middlesex University MSc Work-Based Learning Studies (Corporate Security Management).

WORKSHOP DETAILS

- Duration 10 days, 26th September– 7th October 2010, 8:00am - 4:00pm;
- Fees: RO 2,950 (includes workshop materials, lunch & breaks at the venue);
- Accommodation: *Hotel rates can be provided upon request;*
- Presenter: Barry Vincent, MA, MSc
- Venue: Millennium Hotel, Doha, Qatar

WHO SHOULD ATTEND

- Experienced Security Managers who have undergone basic training in security management
- Experienced Security Consultants

METHOD OF INSTRUCTION

Instruction will be participatory, requiring a high level of interaction on the part of the delegates. Workshop materials will be supported by videos, exercises and case studies. Instruction will be in English.

Please contact us for further information or click here to register

Precept Management Consultancy, P.O. Box 255, P.C. 112, Sultanate of Oman
Tel: +968 24497123, Fax: +968 24497222, E-mail: precept@omantel.net.om
Website: www.preceptmanagement.com

Security Management Stage 2
May 2010

Week 1

Time	Sun	Mon	Tues	Wed	Thu
0800-0930	Introductions and Administration	Business Integrated Security Management	Fraud Risk Management	Integrating Security Technology	Digilife Risk Analysis Presentations PW
0945-1145	Developing Security Risk Management	Business Integrated Security Management	Transport and Distribution Security	Specifying Security Technology	Investigations Management and Forensics PW
Lunch and Prayers 1145-1245					
1245-1415	Developing Security Risk Management	Exercise Digilife Introduction	Developments in CCTV	Exercise Digilife	Information Security Management
1430-1600	Developing Security Risk Management	Business Integrated Security Management	Security Convergence	Selecting a Guarding Contractor	Digilife IT Security Management

Security Management Stage 1
May 2010

Week 2

Time	Sun	Mon	Tues	Wed	Thu
0800-0930	Business Travel Security Management	Business Continuity Management	Corporate Response to Terrorism	Crisis Management Exercise	Exercise Digilife Tiger Final Presentations
0945-1145	Business Travel Security Management	Business Continuity Management	Corporate Response to Terrorism	Crisis Management Exercise	Exercise Digilife Tiger Final Presentations
Lunch and Prayers 1145-1245					
1245-1415	Business Travel Security Management	Business Continuity Management	Corporate Response to Terrorism (CBRN)	Crisis Management Exercise	Examination
1430-1600	Business Travel Security Management	Business Continuity Management	Business Finance	Crisis Management Exercise	Delegate Action Plans

SESSION	LEARNING OBJECTIVES
1 – Developing Security Risk Management *The aim of this session is to create an awareness and understanding of a range of approaches to risk management and to engender an appreciation of its value and relevance to security management.*	**Learning Objectives:** Having successfully completed this session, delegates will be able to: • State how risk management has evolved as a business management tool • Appreciate a range of risk measurement methodologies and their application to specific risk management scenarios • Differentiate between quantitative and qualitative risk measurement and explain the contexts in which each is used • State eight stages which make up a security risk management process • Identify a range of factors which can negatively or positively influence impact of potential loss • Calculate annual loss expectancies, demonstrating a realistic appreciation of consequential loss • Use the "decimalization" method to calculate exposure
2 – Business Integrated Security Operations Management *The aim of this session is to enable delegates to develop detailed security programmes which are integrated with corporate aims, objectives and operations.*	**Learning Objectives:** Having successfully completed this session, delegates will be able to: • Demonstrate an ability to locate appropriate information on security-related issues and problems using all available sources • Identify key cost implications associated with security, based on procedural manpower and hardware solutions • Demonstrate an understanding of the interaction between corporate goals and security programmes and the importance of ensuring that these programmes contribute to corporate achievement • Present a case for the reduction of risk in a cost-commensurate way • Demonstrate the application of a range of techniques for selling security

	solutions to senior management and raising their awareness of security issues • Describe appropriate methods for the cost-effective deployment of manpower under given situations • Explain various methods of implementing and maintaining loss-recording systems and their use • Make recommendations for the structuring of a corporate security awareness programme
3 - Integrating and Specifying Security Technology *The aim of this workshop is to enable delegates to more effective specify and use security technology in an integrated way, in order to deliver greater return on investment.*	**Learning Objectives** Having successfully completed this session, delegates will be able to: • Appreciate the main developments in security technology • Select security technology developments that will make a cost-effective contribution to security risk reduction • Specify integrated security technology that operates on an integrated (IT) platform • Use a standard internationally recognised format for technology procurement • Differentiate between technical specifications and performance specifications and know when to use each • Evaluate between different technology providers • Explain the difference between consultants, integrators and installers and know when best to use each • Use cross functional user teams and project management teams appropriately in the selection and implementation of new technology • Plan lifespan for new technology and implement a programme of proactive maintenance • Implement an acceptance and testing programme for new technology

4 - Developments in CCTV *The aim of this session is to enable delegates to evaluate and differentiate between the many and varied CCTV products on the market, to make sound cost- and risk- commensurate decisions, and to establish and manage an effective CCTV monitoring operation.*	**Learning Objectives** Having successfully completed this session, delegates will be able to: • Describe and explain the key elements of a CCTV installation • Prepare a CCTV operational requirement • Explain how digital CCTV systems work, including the stages of image acquisition, compression, transmission, storage, retrieval and event activation • Appreciate the relationship between focal length, field of view, depth of field and lens size • Determine, in co-ordination with technical staff, the most appropriate and cost effective means of image transmission • Select appropriate cameras for given situations and circumstances • Determine storage needs based on differing parameters, with a basic understanding of image compression • Select from a range of storage options, including digital video recorders and network video storage solutions • Select from a range of CCTV options for monitoring in darkness • Determine how best to use video motion detection • Describe and employ intelligent video systems for specific circumstances • Select from a range of recording frame rates for differing circumstances • Describe the characteristics of a basic CCTV control room

5 - Fraud Risk Management and Ethics *The aim of this session is to enable delegates to make a greater contribution to the prevention and detection of workplace fraud, a crime the cost of which, according to the Association of Certified Fraud Examiners, is equivalent in many businesses to that of their net profits.*	**Learning Objectives** Having successfully completed this session, delegates will be able to: • List the key elements of a corporate fraud and ethics policy • Give examples of typical unethical behaviour and measures to counter it • Describe the factors that motivate an employee to commit fraud against his/her employer • Describe the characteristics of a typical fraudster-employee using real examples in support • Explain at least ten different types of fraud typical in a corporate environment • Identify fraud risk-prone activities and areas in a business • List and explain the key elements of a fraud response plan • Implement a range of measures to reduce an organisation's exposure to fraud • Explain the sensitivities and basic requirements for conducting an investigation into a suspected corporate fraud
6 - Investigations Management and Forensics *The aim of this session is to develop the ability of delegates to successfully manage an internal investigation into a workplace crime, and to make use of available forensic science.*	**Learning Objectives** Having successfully completed this session, delegates will be able to: • Plan and sequence a corporate investigation • Identify all interested parties for a range of investigation scenarios • Present an economic justification for investigating • Provide advice to senior managers on when and how to involve outside resources including specialist services and law enforcement agencies • Select an appropriate investigator based on a range of criteria • Recommend in consultation with business managers appropriate

	investigations strategies, routes and outcomes for a range of crimes • State the steps to be taken when seizing a PC or laptop as evidence • Produce a range of documentation, files and forms to be used in investigations • Select from a range of appropriate surveillance tools, including electronic monitoring, agents and informants • List the main forensic techniques available to the corporate security manager and explain where they would be applied • Demonstrate the procedures required for the preservation of forensic evidence • Explain the process for identifying and selecting appropriate forensic science services • State the special requirements when initiating an investigation into suspected theft or unauthorised disclosure of information
7 - Transport and Distribution Security *The aim of this session is to enable delegates to be able to design and implement protective systems for use in transport and distribution operations.*	**Learning Objectives:** Having successfully completed this session, delegates will be able to: • Draw and explain a typical manufacturer-to-customer transport system • List and describe typical protective strategies for distribution and transport systems • Recommend technological solutions for goods and vehicle tracking and recovery • Explain a typical flow of documentation within a transport system and identify points at which it could be exploited for criminal purposes • Construct a typical security system for use in a distribution warehousing environment • List typical procedures used to counter internal theft in a warehousing environment

8 - The Corporate Response to Terrorism *The aim of this session is to raise delegates' ability to identify and utilise a range of mitigative measures which are designed to increase organisational resilience to terrorist attack, particularly attacks using improvised explosive devices.*	**Learning Objectives:** Having successfully completed this session, delegates will be able to: • Explain the rationale behind the increased shift towards terrorists' targeting of businesses • Appreciate both the short-term and long-term impact of terrorist attacks on business • Differentiate between government and corporate responsibilities in response to terrorism • Use standard risk analysis methodologies to provide the basis for terrorism risk mitigation • Select from a range of intelligence sources which provide background information on terrorist groups, modus operandi and targeting • Conduct a counter-terrorism vulnerability assessment • Produce an overall corporate protective strategy • Select from a range of physical protective measure including stand-off, blast walls and anti-suicide vehicle attack momentum-retarding measures • State the minimum requirements for an internal refuge area • Explain the characteristics of an explosion, particularly the blast wave, and identify ways to create physical resilience in buildings • Recommend and produce a graded system of alert states and measures • List the key requirements for creating operational resilience and business continuity through a terrorist bomb attack • Identify the main risks from, and mitigative strategies against, non-conventional weapons (CBRN).

9 - Business Travel Security Management *The aim of this session is to introduce to delegates a set of security measures and protocols which will enable their businesses to discharge their moral, and often legal, obligation to ensure the personal safety of travelling staff, especially those travelling overseas to unfamiliar or high-risk areas.*	**Learning Objectives:** Having successfully completed this session, delegates will be able to: • Use standard risk analysis methodologies to identify and mitigate against the risks to business travellers • Identify the key business travel risk mitigative strategies • Describe the travel planning process • Establish a system of visitor receiving protocols for their respective locations • Establish a system of overseas security travel protocols for business travellers departing their respective locations • Produce a handout of personal security best practices for high-risk countries • Select from a range of 3rd party services which provide intelligence and other business travel support services • List the key threats to business travellers and the main mitigative strategies for each • Identify which countries are currently assessed as high risk to business travellers and why • Explain the extent of kidnap for ransom (K&R) and produce K&R policies and protocols • Deliver pre-travel security briefings for staff travelling overseas • Produce a range of tools and templates to improve the security of business travellers, including handbooks and pre-arrival visitors' packs • Establish an expatriate security programme

10 - Information Security Management *The aim of this session is to increase delegates' appreciation of the dynamic value of, and the threats to, sensitive corporate information and to provide them with the knowledge, tools and templates to devise a comprehensive corporate strategy aimed at enhancing the protection of information in all of its forms.*	**Learning Objectives:** Having successfully completed this session, delegates will be able to: • Explain the key difficulties in protecting information in a contemporary IT-connected workplace in which the rapid exchange of information is critical to maintaining competitive advantage • Describe, with the aid of a graph, the effect of information leakage on a forecasted product life cycle • Allocate responsibilities for protecting information throughout the business • Recommend a wide range of measures to better protect sensitive information stored on laptops, including unauthorised hacking when attached to a public wireless and hotel guest network • Recommend a range of measures to reduce the risk of electronic eavesdropping of telephone and fax calls • Implement a system for the secure destruction of sensitive waste • List and explain the effects of most recent and prevalent threats to IT systems • Describe the components and functioning of a multi-element IT security system • List the main tools available for the protection of an IT security system and explain how they interact • Apply IT security to a simulated business environment
11 - Convergence of Physical and IT Security *The aim of this workshop is to provide delegates with an understanding of the growth of converged threats and how physical and IT security functions are converging to meet these threats.*	**Learning Objectives:** Having successfully completed this session, delegates will be able to: • Define and describe the concept of convergence • Explain security technology convergence

	• Give examples of security threat convergence (blended threats) • State the main advantages of converged programmes such as the Single Card Initiative • Identify ways to gain maximum return on security investment through convergence • Appreciate the potential pitfalls of convergence
12 - Selecting a Guarding Contractor *The aim of this session is to enable delegates to make good decisions when engaging contracted manned guarding services.*	**Learning Objectives:** Having successfully completed this session, delegates will be able to: • Determine a procedure for the pre-selection of guarding contractors • Identify the key differentiating factors that indicate the quality of a contractor • List the main elements of a service level agreement suitable for a guarding contract • Establish a procedure for liaison with guarding contractor management and the rapid resolution of problems • Raise and maintain the standard of contract guarding to a level commensurate with the image of the company
13 - Business Finance and Budgeting *The aim of this session is to give delegates an overview and understanding of the various financial components of corporate finance and, using this understanding, ensure that their function is operated in line with good management practice.*	**Learning Objectives:** **Having successfully completed this session, delegates will be able to:** • Provide a basic overview of business financial management • Explain the use of balance sheets and profit and loss accounts and, using basic models of each, identify and interpret the various data contained therein • Describe how to calculate the key financial ratios used in measuring

	business performance • Describe how a cost centre works with regard to allocation of overheads • List and explain the main types of budget
14 - Business Continuity Management *The aim of this session is to provide delegates with a range of tools and techniques which will allow them to coordinate and contribute to the business continuity management system.*	**Learning Objectives:** Having successfully completed this session, delegates will be able to: • Explain the relationship between crisis management and business continuity management • Describe the various roles fulfilled by a corporate business continuity planning coordinator • List the "deliverables" of a Business Continuity Plan • Describe various standard business continuity models • Explain the business continuity planning processes • List the steps involved in business impact analysis • Explain the importance of planning, exercising, maintaining and auditing business continuity plans • Develop a range of appropriate responses • Carry out a business continuity risk analysis, gap analysis and recommend risk treatments • Describe typical business continuity planning structures • Recommend a range of appropriate recovery solutions

15 - **Security and Crisis Management Exercise** *The aim of this exercise is to provide a forum for tutors to formally assess and measure delegates' ability to design and manage a multi-site corporate operation and react to a range of simulated crisis and security situations. Critically, tutors will monitor and record delegates' ability to interact at "senior" management level, their ability to reach logical and cost-effective solutions through discussion and negotiation, their ability to think and reaction rationally and proportionally in the face of a range of difficult situations and their ability for critical self-analysis.*	**Learning Objectives:** Having successfully completed this session, delegates will be able to: • Design an overall security system to cover a range of operations from manufacture to point of sale • Successfully present, using a range of management and analytical tools, the above design to a senior management team and respond to critical questioning and analysis • Appropriately and proportionally respond to simulated security issues such as vehicle hijack and product diversion, fuel theft and industrial unrest • Demonstrate the ability to form and operate a crisis management structure to respond to a range of notional security and non-security events • Produce and present a post-incident review following a crisis, showing critical analysis of the situation and their performance, together with recommendations for future action • Demonstrate an ability to utilise interpersonal and leadership skills in a simulated high-pressure situation

THE COMPANY

The ARC Training International Academy for Security Management is the UK's leading provider of security management training courses and probably the best-known international security management training company in the world - since its creation in 2000, delegates from no less than 100 different countries have attended ARC Training courses in the UK and at various locations across the globe.

ARC Training clients include four out of the top five US companies and four out the top five UK companies. Delegates from almost all business sectors have studied with ARC. These include: the automobile industry, aviation and aerospace, construction, higher education institutes, the financial sector, insurance and banking sectors, government and government-associated agencies, police, leisure and hotels, logistics and transport companies, manufacturing, media, oil and gas and extractive sector companies, pharmaceutical companies, property management, retail, security companies, the service sector, telecommunications and utilities.

ARC has conducted programmes extensively throughout the Middle East and clients in the Region have included RasGas, Saudi Aramco, Saudi Arabian Monetary Agency, Saudi Petrochemical, SABIC, Saudi Electricity, Bahrain Telecommunications, ADGAS, Kuwait Oil Company, Sultan Center Kuwait, Burj Al Arab, Jumeirah International, Emirates Towers, Madinat Jumeirah, Wild Wadi Water Park, Grand Hyatt Dubai, Kempinski Hotel Mall of the Emirates, Burjuman, Emirates, Al Bustan Palace Hotel, Intercontinental Hotels (Muscat, Abu Dhabi, Amman, Cairo & Nairobi), Dubai Aluminium, Shuweihat O&M LP, Tawam Hospital, Oman LNG, Petroleum Development Oman, Oman Gas, Royal Oman Police, Oman Waste Water, SOCAT, Bank Muscat, National Bank of Oman, United Finance Company, Central Bank of Oman and Telenor Pakistan.

ARC has also conducted several open programmes in Cyprus and clients include Cyprus Petroleum Storage, Lanitis Development, Laiki Group, Hellenic Bank, Bank of Cyprus, Ministry of Justice & Public Order and the Ministry of Communication & Works (CYTA).

All ARC trainers are leading practitioners in their respective fields and bring to the training environment many years of experience, both in the UK and overseas. As a minimum qualification, the full-time members of the security management training team are all CPP-certified, ensuring not only professional competence, but also that the ARC Training International Academy for Security Management adheres to the strictest codes of conduct within the industry.

PRESENTER'S PROFILE

Barry Vincent, MA, MSc

Barry is an accomplished security professional with a unique skill set. A former senior police officer with an extensive risk and crisis management background, he is experienced in police command roles in major policing operations and strategic planning, and was seconded on international service with the United Nations International Police Task Force to Bosnia and Herzegovina to oversee policing operations and develop a democratic policing arrangements in the aftermath of the civil war.

In recent years he was responsible for the distribution and supply chain security arrangements with the leading UK retailer, and advised the heads of security in the retailer's international businesses on security in retail and supply chain operations. He was also responsible for coordinating their business continuity plans and developing crisis management arrangements and training for senior management. He has travelled extensively in S.E Asia and Europe.

In 2007 he established his own security consultancy business bringing his expertise to a range of clients. He is a non-executive director with a number of companies providing security solutions to the retail and logistics sectors, in particular, and also advises clients on business continuity management and related issues. He is an Associate trainer with ARC Training and conducts their Retail Security, Security Surveying, Crisis Management/Business Continuity and Masters-linked Security Management programmes for clients from a range of industry sectors and nationalities.