



## **SECURITY MANAGEMENT – STAGE 1**

Amwaj Rotana – Jumeirah Beach Residence, Dubai, United Arab Emirates;

25 March – 5 April 2012

### **BACKGROUND**

This very popular and comprehensive programme - *successfully completed by hundreds of security managers from many of the world's most famous and most successful companies* - is designed for security managers, coordinators and their equivalents, who wish to gain a thorough understanding of how to manage security within a corporate environment. Suited equally for existing security managers and those newly appointed from police or military or business backgrounds, the course will enable delegates to use a range of risk management and security design tools to enhance their organisation's ability to protect its assets.

The course takes the form of lectures, workshops, exercises and makes extensive use of case studies. Delegate participation is actively encouraged.

**This course may be used to earn credits towards the Middlesex University MSc Professional Practice in Corporate Security Management.**

### **WORKSHOP DETAILS**

- Duration: 10 days, 25 March – 5 April 2012, 8:00 am – 4:00 pm;
- Fees: RO 2,950 /AED 28,175/US\$ 7,675 (includes workshop materials, lunch & breaks at the venue);
- Presenter: Stephen Phelps, BSC, CPP
- Venue: Amwaj Rotana – Jumeirah Beach Residence, Dubai, U.A.E.

### **WHO SHOULD ATTEND**

- Security Managers
- Security Consultants
- Those who have to deputise for security managers.
- Military of police service personnel who are seeking to transfer to a career in commercial security

*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](mailto:precept@omantel.net.om)

Website: [www.preceptmanagement.com](http://www.preceptmanagement.com)

## METHOD OF INSTRUCTION

The course takes the form of lectures, workshops, exercises and makes extensive use of case studies. Delegate participation is actively encouraged.

## THE WORKSHOP

SESSION	LEARNING OBJECTIVES
<p><b>1 – Security Risk Management</b></p> <p><b>The aim of this session is to teach delegates the basics of Security Risk Management, Security Risk Analysis and Security Risk Treatment and to provide them with the knowledge and tools necessary to use these processes in the workplace.</b></p>	<p>Having successfully completed this session, delegates will be able to:</p> <ul style="list-style-type: none"> <li>• Explain the main stages in the security risk management process</li> <li>• Explain the positive influence of security risk analysis on organisational operations</li> <li>• Apply quantitative and qualitative security risk analysis to appropriate situations</li> <li>• State the major categories of asset</li> <li>• Describe the security risk analysis process</li> <li>• Describe two methods of assessing risk levels</li> <li>• State four factors which can negatively or positively influence risk</li> <li>• List and explain five ways of treating risk</li> <li>• Explain the difference between direct and consequential loss</li> <li>• Demonstrate the use of security risk analysis in a simulated situation</li> </ul>
<p><b>2 – Security Operations Management</b></p> <p><b>The aim of this session is to provide delegates with the tools and techniques required for the specialist elements of a security manager’s tasks.</b></p>	<p>Having successfully completed this session, delegates will be able to:</p> <ul style="list-style-type: none"> <li>• List the main roles of a security manager</li> <li>• Explain the role of a cost effective security department in contributing to the operational success of an organisation</li> <li>• List four non-security skills and four characteristics of an effective security manager</li> <li>• Explain the concept of ‘Board Driven Security’ and be able to describe the reporting chain that encompasses this concept</li> <li>• Describe four layers of policy and procedure structure</li> <li>• Explain the difference between a policy and a procedure</li> <li>• List the four characteristics of a good procedure</li> <li>• Describe the concept of ‘Proactive Security’, explain its purpose and list examples</li> <li>• Describe what makes an effective management objective and explain how this would help the security department to contribute to corporate objectives</li> </ul>

<p><b>3 - Principles of Security Design</b></p> <p><b>The aim of this session is to provide delegates with the tools and criteria necessary for designing and checking of security-related protective measures.</b></p>	<p>Having successfully completed this session, delegates will be able to:</p> <ul style="list-style-type: none"> <li>• List and describe the four components of a security system</li> <li>• Describe, by giving examples, the main principles of security design</li> <li>• List and give examples of the four components of the proactive security environment</li> <li>• Explain how each component of an integrated security system interacts with the others</li> <li>• Explain the concept of layered security and describe in the context of at least two different environments</li> <li>• Identify methods for the successful integration of security into the business</li> <li>• “Sell” security plans to management</li> <li>• Select from a range of security measures to achieve deterrence and crime prevention</li> <li>• Demonstrate the use of international security design best practice in a security design exercise</li> </ul>
<p><b>4 - Perimeter Security</b></p> <p><b>The aim of this session is to provide delegates with the guidelines and information to allow them to plan, design and evaluate the protective measures that apply to the protection of the perimeter of a site or building.</b></p>	<p>Having successfully completed this session, delegates will be able to:</p> <ul style="list-style-type: none"> <li>• Explain, with examples, the five D’s of an effective perimeter</li> <li>• Explain the equation <math>T_p &gt; (T_d + T_i)</math> with regard to the optimisation of perimeter protection</li> <li>• Identify an appropriate perimeter zone so as to give the best investment option</li> <li>• List the main types of perimeter barrier</li> <li>• Design an appropriate perimeter barrier system in a simulated situation</li> <li>• List four types of perimeter intruder detection system and explain the operating principles and advantages/drawbacks of each and the environments to which each is best suited</li> <li>• Design an appropriate, cost effective perimeter intrusion detection installation in a simulated situation</li> <li>• Describe how intrusion detection systems are monitored and how, if necessary, this can take place off site</li> <li>• List three types of lighting source and state the advantages and disadvantages of each</li> </ul>
<p><b>5 - Buildings Security</b></p> <p><b>The aim of this session is to provide delegates with the guidelines and information to allow them to plan, design and evaluate the protective measures that apply to the protection of buildings.</b></p>	<p>Having successfully completed this session, delegates will be able to:</p> <ul style="list-style-type: none"> <li>• Describe five methods of illicit entry into buildings</li> <li>• Describe the differences between preventing illegal access during working and during non-working hours and give three examples of best practice in preventing this from occurring</li> <li>• List three main criteria for designing building shell protection</li> <li>• List and describe four methods of securing external doors</li> <li>• List and describe four methods of protecting and alarming windows</li> <li>• Explain the differences in the problems of protection of older, low risk buildings and newer, high risk buildings</li> <li>• Explain the difference between shell, space and point alarm systems</li> <li>• Describe the principles of operation of three types of building intrusion detection system sensor</li> <li>• Design a cost effective system for protecting building facilities and operations in a simulated situation</li> </ul>

<p><b>6- Workplace Crime Prevention</b></p> <p><b>The aim of this session is to evaluate, through discussion, the extent of employee crime in delegates' businesses and to study a number of crime prevention strategies that can be applied to a workplace scenario in order to reduce crime.</b></p>	<p>Having successfully completed this session, delegates will be able to:</p> <ul style="list-style-type: none"> <li>• Compare the extent of employee crime in their respective businesses against internationally accepted norms</li> <li>• List at least ten factors which might motivate an employee to commit a crime against his or her employer</li> <li>• Identify some common traits of an employee-thief</li> <li>• Explain Felson and Cohen's "Routine Activity Theory"</li> <li>• State which elements of a crime prevention programme are within the remit of the security manager</li> <li>• Differentiate between, and explain, situational crime prevention and social crime prevention and explain how the former can be used in a workplace environment</li> <li>• Explain the key elements of a corporate crime prevention programme</li> <li>• Explain, using examples, the concept of Crime Prevention through Environmental Design (CPTED)</li> </ul>
<p><b>7 - Protection against Explosive Devices</b></p> <p><b>The aim of this session is to provide delegates with an awareness of the functions and characteristics of the main types of improvised explosive devices, and the countermeasures necessary to confront each.</b></p>	<p>Having successfully completed this session, delegates will be able to:</p> <ul style="list-style-type: none"> <li>• Illustrate, by example, the prevalence of the improvised explosive device (IED) as the terrorist weapon of first choice</li> <li>• Identify the six key components common to most IEDs</li> <li>• List and describe the main types of improvised explosive device</li> <li>• Explain the different between low and high explosives</li> <li>• Explain the behaviour of blast in relation to nearby structures</li> <li>• Describe the main means of activating an IED</li> <li>• Implement the key countermeasures with regard to a postal IED</li> <li>• Implement the key countermeasures with regard to a hand-delivered IED</li> <li>• Implement the key countermeasures with regard to a large vehicle IED</li> <li>• State the minimum evacuation distances for a variety of different IED scenarios</li> <li>• Select and manage the safe evacuation to an appropriate assembly point</li> <li>• Identify measures to mitigate against suicide vehicle attacks</li> </ul>
<p><b>8 - Access Management</b></p> <p><b>The aim of this session is to enable delegates to design and implement appropriate access management systems and to manage their operation.</b></p>	<p>Having successfully completed this session, delegates will be able to:</p> <ul style="list-style-type: none"> <li>• Explain the four aims of access management</li> <li>• Describe four methods of preventing unauthorised access</li> <li>• Describe four methods of preventing unauthorised removal of property</li> <li>• List and describe three methods of preventing the unauthorised introduction of prohibited articles into the protected area</li> <li>• Describe the design requirements of an access control system for employees, contractors and visitors</li> <li>• List and explain five considerations when designing and implementing a visual access control system</li> <li>• Briefly describe the functioning of an electronic access control system</li> <li>• Describe the basic principles of operation of three types of biometric identity verification device</li> <li>• List three reasons for carrying out searches of people entering and leaving protected premises</li> <li>• Design an access management system in a simulated environment</li> <li>• Describe a typical key control system</li> <li>• Design a search system in a simulated environment</li> </ul>

<p><b>9 - Security Surveying</b></p> <p>The aim of this session is to provide delegates with the guidelines and information necessary for them to plan and carry out a security survey and report on the findings.</p>	<p>Having successfully completed this session, delegates will be able to:</p> <ul style="list-style-type: none"> <li>• Describe the difference between a survey, a review and an audit</li> <li>• Describe the purpose of a security survey</li> <li>• Select the most suitable and cost-effective option for conducting a survey</li> <li>• Explain the benefits of “peer surveys”</li> <li>• List the main stages of a security survey</li> <li>• Explain the key pre-survey tasks</li> <li>• Carry out a security survey in a simulated situation</li> <li>• Sequence a survey report</li> <li>• Produce a Board-level presentation of survey results in a simulated situation</li> </ul>
<p><b>10 - Protection of at-Risk Personnel</b></p> <p>The aim of this session is to enable delegates to manage the personal protection of key staff, including travelling staff, expatriates and their families.</p>	<p>Having successfully completed this session, delegates will be able to:</p> <ul style="list-style-type: none"> <li>• Identify the key human assets at risk in their organisations</li> <li>• List the circumstances in which the risk to staff is increased</li> <li>• Identify the main threats to key personnel</li> <li>• Identify and mitigate the factors that predispose a person to increased risk</li> <li>• Research in-country risks for all countries in which their staff operate</li> <li>• Select from a range of personnel protection options</li> <li>• Produce and deliver country security risk briefings</li> <li>• State the key elements of a corporate travel risks policy</li> </ul>
<p><b>11 - Protection of Sensitive Information</b></p> <p>The aim of this session is to provide delegates with the knowledge and skills necessary to play a lead role in the formulation and execution of a corporate information security programme.</p>	<p>Having successfully completed this session, delegates will be able to:</p> <ul style="list-style-type: none"> <li>• Differentiate between information security and IT security</li> <li>• Define what is meant by the term <i>business espionage</i></li> <li>• Use a range of criteria to determine the value of specific information</li> <li>• Identify the main types of information</li> <li>• Identify the key threats and threat sources to information</li> <li>• Describe the activities of information brokers</li> <li>• Classify and protect sensitive information in accordance with information security best principles</li> <li>• Differentiate between the terms trade secret, proprietary information, intellectual property, copyright, registered trademark and patent</li> <li>• Evaluate a range of options to deal with a suspected information thief</li> </ul>
<p><b>12 - Technical Surveillance Countermeasures</b></p> <p>The aim of this session is to provide delegates with the knowledge and skills necessary to reduce the risk of technical eavesdropping in both a general environment and on special occasions.</p>	<p>Having successfully completed this session, delegates will be able to:</p> <ul style="list-style-type: none"> <li>• Describe how telephone calls, fax transmissions and emails can be intercepted by state and non-state entities</li> <li>• Describe six methods used by spies to collect audio data from within a room</li> <li>• Identify simple devices that are used to carry out eavesdropping</li> <li>• Estimate the extent of the use of eavesdropping equipment in the corporate environment</li> <li>• Explain how to sweep an environment for listening and recording devices</li> <li>• Explain how to scan an environment for listening devices</li> <li>• Select between in-house and external TSCM resources</li> <li>• Produce a TSCM security plan for a specific event</li> </ul>

<p><b>13 - Crisis Management</b></p> <p><b>The aim of this session is to enable delegates to contribute effectively to their respective corporate crisis management mechanisms.</b></p>	<p>Having successfully completed this session, delegates will be able to:</p> <ul style="list-style-type: none"> <li>• Explain the relationship between risk management and crisis management</li> <li>• Explain the function of the security manager in relation to crisis management</li> <li>• List four main guidelines for crisis management</li> <li>• Differentiate between crisis and emergency management</li> <li>• Describe the process required to introduce a crisis management system into an organisation</li> <li>• Describe the structure of a crisis management team</li> <li>• Describe the requirements of a crisis management centre</li> <li>• Describe the process and main requirements for good business continuity planning</li> <li>• Explain the importance of good internal and external communications during a crisis</li> <li>• Explain the processes involved in dealing with the media during a crisis</li> <li>• Demonstrate the processes involved in crisis management in a simulated situation</li> </ul>
<p><b>14 - Investigations and Evidence</b></p> <p><b>The aim of this session is to enable delegates to carry out basic investigations in accordance with business best practice.</b></p>	<p>Having successfully completed this session, delegates will be able to:</p> <ul style="list-style-type: none"> <li>• Define, classify and describe different types of evidence in accordance with standard international best practice terminology</li> <li>• Differentiate between evidence, information and intelligence</li> <li>• Process a basic scene of crime and protect and preserve evidence in accordance with international best practice</li> <li>• Recommend, in consultation with business managers, appropriate investigations strategies, routes and outcomes for a range of crimes</li> <li>• Provide advice to senior managers on when and how to involve outside agencies, including specialist services and law enforcement agencies</li> <li>• Sequence and manage a basic internal investigation, including budgeting, staffing, inquiry parameters and summary reporting</li> <li>• Conduct a witness and suspect interview in a manner and style appropriate to a business environment using a range of standard questioning styles</li> <li>• State the main ways of recording interviews and the basic requirements for statement taking</li> <li>• Explain the main considerations and respective basic requirements when using agents and informants</li> <li>• Prepare a case for a presentation to an external authority or to internal management</li> </ul>
<p><b>15 – Manpower Selection and Deployment</b></p>	<ul style="list-style-type: none"> <li>• List the main component elements of a personnel specifications and job description</li> <li>• Understand span of control, lines of responsibility and reporting</li> <li>• Describe the process of background screening</li> <li>• Define discipline and best practice for dealing with disciplinary infractions</li> <li>• Calculate the manpower requirements for a security department</li> </ul>

<p><b>16 – Syndicated Course Project Exercise “Sumatran Tiger”</b></p> <p><b>The aim of this syndicated project, which runs throughout the course, is to provide a forum for tutors to formally assess and measure delegates’ ability to use both their existing knowledge and the knowledge and skills acquired during the course to design a complete security programme appropriate for the protection of a notional high-risk oil refinery facility in South East Asia. At the end of the project delegates will be required to produce and deliver a management-level solution.</b></p>	<p>Having successfully completed this session, delegates will be able to:</p> <ul style="list-style-type: none"><li>• Analyse threats and determine risks from a range of information provided in different formats</li><li>• Produce a complete risk analysis for the notional facility</li><li>• Devise a security plan utilising all necessary measures in a risk-commensurate and cost effective way</li><li>• Working as a team, produce a presentation, the quality and content of which should be appropriate for delivery to a senior management team</li><li>• Demonstrate the ability to use a range of presentation tools and management models, including financial analysis and forecasting</li><li>• Deliver the solution to a simulated senior management team and respond to critical analysis and questioning</li></ul>
--	--

## 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 all five leading UK and US multinational 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

### STEPHEN PHELPS, BSc, CPP

Stephen Phelps BSc CPP is a regular contributor to the university-accredited security management range of courses. He specialises in security intelligence, and has developed a specific training course in this subject.

His intelligence experience spans 30 years in both the government and private sectors, with a current focus on Africa, maritime security and oil and gas. He has direct operational experience in managing intelligence in a range of challenging security environments in 14 countries spanning 4 continents.

*This course is accredited by Skills for Security, the UK skills and standards setting body for the Security Business Sector*

