

SECURITY MANAGEMENT

STAGE 1

23 March – 3 April 2009

3 – 14 August 2009

16 – 27 November 2009

Location: Thames Valley, UK

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 active encouraged.

This course may be used to earn credits towards the Middlesex University MSc Work-Based Learning Studies (Corporate Security Management).

CONTENT

Security Risk Management

Risk management as a cross-functional business tool; security risk analysis; identifying assets; asset systems and asset contexts; determining probability based on quantitative and qualitative scales; measuring direct and consequential impact; risk mitigation

Security Operations Management

The main roles of the security manager; operating a cost-effective security department; creating a return on investment; effective management skills for the security manager; creating proactive security programmes; security reporting chains; service level agreements to manage contracted services

Security Policies and Procedures

Alignment of security to business processes; creating board-driven security management; devising, drafting and implementing security policies and procedures

Security Design

The components of a security system; the 18 principles of security design; the security environment; creating

risk-commensurate security; balancing risk and protection; integrating security into the business environment; selling security to management; creating crime prevention through good security design

Physical and Electronic Security

Creating a perimeter to deny, detect, deter, deflect and demark; balancing delay, detection and response to perimeter intrusions; creating layered security, perimeter fencing options, costs, drawbacks and benefits; perimeter intrusion detection systems (PIDS); off-site and on-site monitoring of PIDS; CCTV as a perimeter protection means; perimeter lighting; perimeter patrolling; the key requirements of a high-risk site perimeter; security buildings against internal and external crimes; methods of illicit entry into buildings; the key requirements of working hours protection; the key requirements of quiet hours protection; protecting the building shell using physical and electronic means; protecting the building interior using physical and electronic means; internal patrolling; building intrusion detection systems (BIDS); point alarm systems and electronic article surveillance; internal CCTV

Access Management

The key aims of access control; access management systems design and application; preventing unauthorised access; preventing unauthorised removal of property; badging and identification systems; biometric access management systems; key control systems and best practice; entry and exit searching policies and practice; applying the need-to-go principle; access management compartmentalisation

Workplace Crime Prevention

The factors which might motivate an employee to commit and internal crime; the common traits of an employee thief; application of Felson's Routine Activity Theory; the application of situational crime prevention; social crime prevention overview; crime prevention through environmental design; reducing exposure to burglary; developing a corporate crime prevention programme

Introduction to Security Surveying

Security surveys, reviews and audits; sequencing a security survey; security surveying options; peer surveys; pre- and post- survey tasks; survey report writing; presenting survey results to the Board

Manpower Selection and Deployment

Manpower selection, deployment and span of control; lines of responsibility and reporting; personnel specifications and job descriptions; background screening; dealing with disciplinary infractions

Leadership and Motivation

The principles of effective leadership; common behavioural and skill characteristics inherent in successful business leaders; application of recognised successful business leadership and motivational techniques; motivating the security team; leading meetings; delivering management presentations

Introduction to Investigations

Evidence, information and intelligence; collecting, classifying, preserving and using evidence; basic scene of crime processing; investigation strategies, routes and outcomes; investigations management and sequencing of tasks; case management; using outside agencies and services; investigation resourcing and budgeting; investigation reporting; interviewing; questioning strategies; use of agents and informants

Protection against Explosive Devices

Terrorism overview and modus operandi of groups; trends, targets and weapons; the improvised explosive device (IED) overview; IED components and construction; the characteristics of, and countermeasures for, postal IEDs hand-delivered IEDs, under-vehicle IEDs, remotely-controlled IEDs, large vehicle IEDs, suicide pedestrian and vehicular IEDs, blast and blast mitigation; telephone bomb threats; search; evacuation and assembly; CBRN threat overview and mitigation

Information Security

The value of information; identifying information at risk; identifying information security vulnerabilities; threats posed to information by staff; the activities of information brokers; the extent of business espionage; national-level threats to business information; methods of classification and secure storage; securing information while mobile; dealing with suspected information thieves; social engineering; secure disposal of office waste; office information security best practice

Technical Surveillance Countermeasures

Telephone and fax intercept countermeasures; methods of covert bugging and recording; hard-wired devices; wireless devices; recording devices; hybrid systems; creating a secure environment for a confidential meeting; using “sweeping” equipment and services; using frequency scanning equipment and services

IT Security

The contribution of the security manager to IT security; the main threats to confidentiality of information, its availability and integrity; business interruption potential of a major IT security incident; the main threats to corporate IT systems; viruses and other pathogens; hacking; denial of service attacks; phishing; inadvertent disclosure through social engineering; laptop security; managing the threat from peripheral devices; IT systems

protection overview; the key points of an IT security policy; special considerations for the security of laptops; data encryption and other methods to restrict unauthorised access to information stored on IT systems

Protection of At-Risk Personnel

The key human assets at risk; the risk and threat spectrum; circumstances which increase risk; countermeasures which decrease risk; identifying risk environments and high-risk countries; delivering country risk briefings; travel security protocols; the risk of kidnap and ransom; the fundamentals of personnel protection; use of close-protection specialists; counter-surveillance

Crisis Management

The security risk management/crisis management relationship; crisis management in relation to business continuity planning; crisis management and emergency management – the difference; the contribution of a security manager to crisis management planning and coordination; creating a crisis management response; typical crisis management team roles and responsibilities; equipping and managing a crisis management centre; crisis audiences and communications

Change Management

The external and internal drivers for change; planning for change; use of change management models; effective strategies for communicating change; identifying and responding to resistance to change

Course Project

The project, which runs throughout the course, will require delegates to work in groups to draw up a blueprint security plan for a notional multi-site production facility located in an area of elevated risk. Upon completion, delegates will be asked to deliver their solutions by means of a management –level presentation.

£4795 (plus Value Added Tax, currently 17.5%)

Includes 12 nights full board accommodation from Sunday evening

For more information, or to make a booking:

Telephone: +968 24497123

Fax: +968 24497222

E-mail: precept@omantel.net.om

www.preceptmanagement.com



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