

SECURITY MANAGEMENT STAGE 2

30 June – 11 July 2008
13-24 October 2008

Location: Thames Valley, UK

This programme is intended for managers who have already attended a core skills security management course such as *Security Management Stage 1*. The course is designed to enhance security managers' ability to implement security risk management programmes that will make a quantifiable contribution to organisational loss reduction goals. This course focuses on developments in security risk management and addresses a range of complex issues, and focuses on how to select and specify technology and other security services.

The course includes a security and crisis management exercise, which is designed to test delegates' ability to produce a security plan for a notional site, then to use interpersonal skills, reasoning and knowledge to respond to a range of events in a simulated high-pressure security and crisis situation.

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

CONTENT

Developing Security Risk Management

The evolution of risk management as a business tool; the eight stages of the security risk management process; risk analysis modelling and applications; risk forecasting; integrating qualitative and quantitative risk analysis; factors which exacerbate impact; impact mitigation strategies; calculating annual loss expectancies; the decimalisation method of loss calculation

Business-Integrated Security Operations Management

Budgeting and cost analysis; using information sources and security manager networks; creating security programmes that contribute to corporate achievement; developing risk- and cost-commensurate security; optimising manpower costs; developing corporate security awareness programmes; implementing an automated loss-event reporting system

Integrating and Specifying Security Technology

Developments in security technology; migration of physical security detection, control and monitoring systems to IT protocols; unifying control systems and protocols; how to specify security systems; the role of consultants and integrators; RFID; electronic article surveillance, GPS tracking; converged systems to deliver dynamic return on investment; system lifespan planning; the single card initiative; power over Ethernet; advantages and disadvantages of using leading edge technologies; security systems design; procurement and project management

Developments in CCTV

Digital CCTV system overview; selecting and specifying cameras, lenses and management systems; understanding jargon in order to make correct purchasing decisions; types of camera; the use of covert cameras; determining system needs; preparing a CCTV operational requirement; network video recording and management – what to specify; chip and resolution specification; optimising frame rates for different situations; when and how to use IR and thermal imaging; image transmission options; video motion detection; intelligent CCTV; scene requirements for identification and recognition; control room specification

Fraud Risk Management and Ethics

The key elements of a corporate fraud and ethics policy; determining and countering unethical behaviour; prevention of corruption in the procurement process; typical frauds; identifying fraud risk-prone areas and activities; factors that motivate and facilitate acts of fraud; employee fraudsters – characteristics and behaviour patterns; best practice for fraud risk reduction; incompatible responsibilities, employee rotation and segregation of duties; fraud detection and response plans

Investigations Management and Forensics

Planning and sequencing corporate investigations; advising on the use of outside specialist agencies; selecting an investigator; recommending investigation strategies, routes and outcomes; best practice for securing computer evidence; special requirements when initiating an investigation into suspected fraud; best practice when initiating an investigation into suspected business espionage; surveillance and electronic monitoring of suspects; using forensic techniques in support of a workplace investigation; preserving forensic evidence; identifying and selecting appropriate forensic science services; forensic document examination; forensic science in support of a corporate travel security programme

Business Travel Security Management

The key threats to business travellers and main mitigative strategies; the key elements of a corporate travel security policy; duty of care and individual responsibilities; the travel planning process; overseas travel protocols; planning for

travel to high-risk countries; visitor reception protocols; country risks; managing the risk of kidnap for ransom; expatriate security; traveller communications and reporting

The Corporate Response to Terrorism

Trends in terrorism – present and future; the trend towards targeting businesses; the impact of terrorist attacks on business – short and long-term; the key corporate responsibilities; liaising with government; collecting and analysing open source information; conducting a vulnerability assessment; developing a protective strategy; blast wave behaviour; mitigating the impact of shock-wave damage; protection from blast using blast walls, stand-off and building strengthening; reducing the momentum of a fast-approach vehicle suicide attack; criteria for selection of internal refuge areas; creating operational and physical resilience; the nature of the CBRN threat; CBRN and terrorism; measures to deal with the chemical, biological and radiological threat; best practice and guidelines for protection

Transport and Distribution Security

Key vulnerabilities in manufacturer to customer transport systems; developing protective strategies for distribution and transport systems; technological solutions for goods and vehicle tracking; typical documentation flows and points of vulnerability; distribution warehouse security systems; measures to control internal theft in warehouses

Managing Protection of Sensitive Information

Creating a comprehensive information security programme; threat sources and collection methods; conducting an information security vulnerability analysis; defining intellectual property; methods for classifying information; the effect of information leaks on product life cycles; allocation of information security responsibilities; identifying and countering suspected information brokering activity; using outside agencies in support of information security and information leak investigating

Convergence of Physical and IT Security

The emergence of blended threats, especially those emanating from organised criminal gangs and terrorists; the influence of technology developments; developing a converged response; the shift from physical to information-based assets; the enterprise-wide risks of having non-converged security; compliance and regulatory issues; blueprint for a converged security department; unifying systems, processes and procedures

Selecting a Guarding Contractor

Identifying guarding requirements; sources of contract guard manpower; specifying guarding contracts; preparing and evaluating bids and proposals; identifying and pre-qualifying good guarding contractors; contracts and service level agreements; selection criteria; what you should expect from a

guarding contractor; performance monitoring and measurement; key performance indicators; guard training requirements; regulation and accreditation of security guards and companies; guard powers and authority

Finance and Budgeting

Business financial management overview; interpreting balance sheets and profit and loss accounts; interpreting financial ratios; cost centres and allocation of overheads; an overview of the main types of security management budgets

Business Continuity Management

Business continuity management strategic deliverables; corporate business continuity planning coordinator – roles and responsibilities; strategic business continuity management models; strategies for survival; business continuity management planning processes; business impact analysis and objectives; preparing, exercising, maintaining and auditing business continuity plans; quality assurance; the business continuity/crisis management relationship; developing responses; business continuity management risk assessments

Security and Crisis Management Exercise

This project, based around a notional manufacturing plant, requires delegates, working in groups, to design an overall security system and plan to cover a range of operations from manufacture to point of sale. During the exercise phase of this project delegates will have to respond to a range of simulated security issues, requiring the formation and operation of a crisis management structure to respond to a range of notional events and to 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

£4700 (plus Value Added Tax, currently 17.5%)

Includes 12 nights full board accommodation from Sunday evening

For more information, or to make a booking:



P.O. Box 255, Ruwi 112 Sultanate of Oman
Tel: (968) 24497123 Fax: (968) 24497222
E-mail: precept@omantel.net.om
Website: www.preceptmanagement.com

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