

# SECURITY MANAGEMENT STAGE 3

11-22 May 2009  
17-18 September 2009

Location: Thames Valley, UK

**This programme is designed to enhance security managers' ability to formulate security policy and manage security programmes at a regional or corporate level. Great emphasis is placed on broadening delegates' contribution to your organisation's security risk management strategy.**

**The course will culminate in a strategic security management simulation exercise, which is designed to provide a realistic context in which delegates, working in syndicates, can exercise the skills learned on the course. The exercise will be based around a series of security events which befall a notional company and will test delegates' ability to address the needs of company stakeholders in a balanced manner whilst simultaneously ensuring that corporate interests remain paramount.**

**It is assumed participants have already attended Security Management Stage 2 (or equivalent).**

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

## CONTENT

### **Corporate Risk Management**

An overview of, and relationships between, security risk, strategic risk, political and legislative risk, financial risk, enterprise risk, operation risk, insurance risk and safety risk; security risk management and relevant legislation; corporate governance; managing risk perception; emerging risk issues; risk, corporate responsibility and ethics; turning risk into advantage; risk mapping; the interaction of risk and business strategy

### **Corporate Social Responsibility**

The business case for corporate social responsibility; the elements of corporate social responsibility; social responsibility, ethics and security leadership; stakeholder communication; liaison with government and non-government organisations; codes of business conduct and business best principles; dealing with unethical behaviour

### **Adding Strategic Value to Security Management**

Analysis of the latest research in scoping the developing role of security management; aligning security with corporate objectives; the message from the boardroom; broadening the contribution of the security management function to add strategic value; the concept of the Chief Security Officer

### **Setting a Vision for Corporate Security**

Integrating security into business plans and projects; marketing the security function to business and to the Board with the use of analytical and presentation tools; strategic planning; strategy fundamentals; the strategic vision; mission and the role of the Chief Security Officer in implementing strategies

### **Kidnap Risk Reduction and Response**

Kidnap types, perpetrators and outcomes; kidnap hotspots and current trends; information sources; the corporate duty of care; where kidnapping occurs; travel security protocols; risk reduction measures; use of executive protection specialists; countering pre-kidnap surveillance; kidnap sequence of events; immediate response to a disappearance; the immediate corporate response to a claim; proof of life; liaison with law enforcement agencies; K&R insurance and third parties; technology and victim tracking; conduct after capture

### **Security Project Management**

Project management defined; project design; when to use project management; project purposes and lifecycles; project team selections; planning and sequencing a project; preparing a project scope document; project estimations; procurement and contractor bids; work breakdown structures and Gantt charting; implementation and operation of the project; training, testing and warranty; maintenance and replacement issues

### **IT Security – Managing Strategic Risks**

The future of IT threats; developing an IT security strategy; liaison with IT professionals; SCADA overview and vulnerabilities; identity theft; social engineering; peer-to-peer risks; data back-up and risks; developments in peripheral storage devices and future strategies to counter information siphoning; data risk management and offshore outsourcing; data management and internal negligence; encryption; alternatives to passwords

### **Investigation of Information Leaks**

The main threats to sensitive corporate information; the corporate espionage process; where and how information leaks occur; the risk from permanent, contracted and temporary staff; surreptitious technical methods used by

information thieves; legal implications and sensitivities when investigating suspected information loss; managing an investigation into information loss; use of outside agencies; the role of specialised forensic assistance in investigating suspected information loss

### **Terrorism – Future Trends and Responses**

Current and future threats to business; Al-Qaeda and affiliates threat assessment; sectors and operations most susceptible to terrorist targeting; risk management strategies for high-impact terrorist threats, including vehicle improvised explosive devices, suicide attacks, chemical attacks, radiological dispersal devices, bioterrorism and cyberterrorism; conducting a counterterrorism vulnerability assessment of a key point; the main requirements of a corporate counterterrorism strategy; the key elements of a facility counterterrorism plan; the main requirement when creating resilience, response and recovery

### **Illicit Trade and Counterfeiting**

Counterfeiting, the “grey market” and contraband; the global nature of counterfeiting; the effects of counterfeiting on stakeholders; identifying counterfeit risk-prone areas of company operations; counterfeiting risk reduction strategies and methodologies; conducting transnational brand enforcement operations

### **Product Tampering and Extortion**

The effects of malicious product tampering; factors giving rise to incidents of malicious product contamination; identifying malicious tampering risk-prone areas of company operations and product flow; crisis management and product recall procedures; reducing the risk of deliberate product contamination

### **External Liaison and Stakeholder Engagement**

Liaison with government and non-government agencies and organisations; identifying and engaging stakeholders and partners; implementing mutual aid arrangements; critical national infrastructure and interdependencies; ensuring corporate compliance with regulation; regulatory bodies

### **Business Expansion - Security Considerations**

Determining risk backgrounds of potential new operating environments; risk issues surrounding merger, acquisition and partnerships in new countries; political risk assessment methodologies; internal and external political risk drivers; due diligence of potential partners, suppliers and distributors; ethics and reputation management; specific-to-sector risks; stakeholder influence and expansion decisions; legal considerations in overseas expansion; managing reputational risk and local community considerations; report writing

### **Security Intelligence**

The nature of security intelligence; sources of security intelligence and security intelligence agencies; information and intelligence collection, analysis and dissemination; business security intelligence collection and best practice; corporate applications of security intelligence and information

### **Dealing with Protest Activity**

Protest movement overview; environmentalist groups; anti-capitalist groups; single issue groups; determining whether a group is militant; the threat from protest activity; networked threats; targets for protest activity; methods of attack (physical and cyber attack); mitigation methods; protecting key managers from protest attack; protest activity and event security; open information sources; covert intelligence sources; protection of reputation; external support in dealing with protest groups; engaging protest groups to reduce risk

### **Strategic Security Management Exercise**

This project, based around a multinational food and drinks company, requires delegates, working in groups, to design an overall security system and plan to cover a range of operations including managing the security of raw materials production across a number of countries, manufacturing at regional hubs, distribution of finished product to point of sale. The project comprises both a security strategy development phase and an exercise phase. During the exercise phase delegates will have to appropriately and proportionally respond to a range of simulated strategic business, crisis and security issues that threaten business continuity, reputation and security of supply. Some of the event will be multi-site in impact. This will require the formation and operation of structures to respond to a range of notional events and to produce and present a post-exercise review, showing critical analysis of the situation and the delegates’ performance, together with recommendations for future action.

**£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](mailto:precept@omantel.net.om)

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



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