



Precept
management consultancy

SPECIFYING SECURITY TECHNOLOGY **Grand Hyatt Dubai, UAE; 31st May – 4th June 2009**

BACKGROUND

Rapid advances in technology and rising manpower costs are two of many reasons why technology is playing an ever greater role in security. It cannot be taken for granted, however, that the installation of one technological system or another will necessarily reduce risk. Furthermore, integration and convergence are driving security technology not only to perform multiple security functions – for example a CCTV camera can be used as an access control instrument – but also to be able to create dynamic return on investment across the business as traditional stand-alone proprietary security technologies merge with IP systems to provide enterprise-wide benefits.

This unique new programme is intended for security managers and specifiers who are required to specify, select and operate technical security systems. The course will focus on developments in technology, including convergence, and the migration of traditional discrete security systems to common IT-based based platforms. It is designed to help the security professional to reach rational and cost-effective decisions about the employment of new technology.

WORKSHOP DETAILS

- Duration: 5 days, 31st May – 4th June 2009, 8:00am - 4:00pm;
- Fees: RO 1,375/US\$ 3,575 (*including workshop materials, lunch & breaks at the venue*);
- Venue: Grand Hyatt Dubai, UAE;
- Presenter: Phillip Wood, MBE, CPP, MSyI.

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

WHO SHOULD ATTEND

- Security managers;
- Those responsible in an organisation for the selection and procurement of new technology;
- Security focal points;
- Security consultants;
- IT staff who liaise with security staff regarding the installation of new technologies.

METHOD OF INSTRUCTION

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

THE WORKSHOP

Day 1

Convergence

Convergence defined; the drivers of convergence; the distinction between information and IT security; merging technologies; convergence of physical and logical security systems; the single card initiative; an overview of IP/TCP control systems in physical security; cross-functioning security systems; convergence of security systems and other business systems to create dynamic return on investment; responding to blended threats; the Alliance for Enterprise Security Risk Management; working with IT staff on convergence issues; new protective technologies blurring traditional functional boundaries; facilitating convergence; overcoming obstacles to convergence; some potential pitfalls of convergence.

Physical Security over IP

The growth of IP/TCP control systems in physical security; convergence of formerly discrete security systems to create dynamic security; understanding and specifying power of Ethernet (PoE 802.3af/802.3at); understanding and specifying IP CCTV overview; bandwidth considerations and data storage options; VoIP and applicability in the business organisation; making the case for physical security over IP; the vulnerabilities of physical security over IP.

IT Network and Network Security

Emerging threats; IT network infrastructure overview; LANs, WANs, the Internet and the worldwide web; the basics of data processing, storage and transmission; IT network security overview; firewall; virtual networks for the management of physical security systems; ensuring restricted access to security systems; role-based access control; encryption and intrusion control; SCADA and security implications; remote access and control; how VPNs work; wireless networks and wireless peripherals security; home access and secure access tokens.

Day 2

Systems Specification, Project Management and Testing

Conducting a vulnerability study to identify physical security needs; creating the preliminary system design; technical specifications – general points; performance specifications – general points; preparing a specification; establishing cross-functional user groups; producing the requirements document; presenting the solutions; security systems project management; cost estimates; security systems costs breakdown; life-cycle costs; procurement approaches; evaluation criteria; vendor selection and contract award; system installation; factory acceptance testing; site acceptance testing; after-implementation testing; using installers, integrators and consultants; fifty points to consider when specifying CCTV; fifty points to consider when specifying intrusion detection systems; fifty points to consider when specifying automated access control systems; fifty points to consider when specifying intrusion detection systems; maintenance agreements and warranty.

Day 3

Electronic Access Control Systems

Specifying hardware; card technologies – pros and cons; the benefits of smartcards; dual-factor authentication; developments in biometrics and system disadvantages; points for consideration in a systems specification; the Single Card Initiative (FIPS 201); access control over IP; wireless access control systems; magnetic locks and magnetic strikes – the differences and pros and cons; how to specify and oversee the installation of an electronic access control system; proximity door readers – pros and cons; considerations when configuring door access control points; preventing passback and detecting tailgating; using proximity tokens at car park entrances; integrating automated access control systems with building intrusion detection systems and CCTV; the information stored on cards and personal security.

Electronic Asset Management

Electronic article surveillance (EAS); Radio frequency identification (RFID); GPS; GSM; satellite communications in asset tracking; linking asset tracking to personnel access management; other alarm systems; logistics and stock management processes and implications; RFID and its increasing role in retail security and personal profiling.

Day 4

Digital CCTV Specification

The fundamental principles of CCTV; CCTV operational requirement; switching to digital CCTV – the benefits; convergence and CCTV; types and applications of cameras; selecting and specifying lenses; selecting and specifying cameras; understanding manufacturer specifications; the relationship between TVL and megapixels; understanding focal length, apertures, depth of field and fields of view; IP cameras; high megapixel cameras; selecting between progressive scanning or standard interlace cameras; virtual PTZ cameras; motion detection; camera chip sizes debunked; selecting between CCD and CMOS chips; cameras and illumination levels; using infrared; thermal imaging cameras; CCTV image transmission; CCTV over Ethernet; bandwidth and compression considerations; power over Ethernet; wireless CCTV; telemetry; video analytics; CCTV for access control and recognition; image compression standards; selecting a DVR; network video recording; storage area networks; recording at the edge; choosing the correct RAID configuration.

Day 5

Perimeter Intrusion Detection Systems

Considerations when specifying a perimeter intrusion detection system; how to specify performance expectations; installation configurations; considerations when using more than one technology; environmental factors that could influence sensitivity; typical nuisance alarm scenarios; determining and specifying nuisance/false alarm rates (NAR/FAR); determining and specifying probability of detection rate (PD); fence-mounted, buried and post-mounted systems; line-of-site systems and volumetric systems; passive and active technology systems; taut wire; vibration sensors; electrostatic disturbance; electrified fence; magnetic field disturbance; ported co-ax; acoustic; fibre optics (fence-mounted and buried); seismic; passive infrared; active infrared beams; microwave; video motion detection; radar; dual technology systems.

Building Intrusion Detection Systems

Considerations when specifying a perimeter intrusion detection system; how to specify performance expectations; installation configurations; considerations when using more than one technology; environmental factors that could influence sensitivity; typical nuisance alarm scenarios; determining and specifying nuisance/false alarm rates (NAR/FAR); determining and specifying probability of detection rate (PD); building shell (boundary) sensors; building space (volumetric) sensors; special considerations when protecting windows, walls, ceilings, skylights, doors; magnetic reed sensors; glass break sensors; capacitance sensors; infrasonic sensors; ultrasonic sensors; passive infrared sensors; monostatic microwave sensors; active infrared beams; dual technology sensors; using CCTV and VMD to detect intrusion; fibre optic cable sensors; pressure sensors; integrating building intrusion detection systems.

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 of 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

Phillip Wood MBE CPP MSyI

Phillip Wood MBE is the Deputy Director Corporate Risk and Security Training. As a former RAF Regiment Squadron Leader he has first hand experience of managing operations in adverse circumstances and is the lead trainer in crisis management and business continuity management on ARC Training's university-accredited security management courses.

Phillip is a member of ASIS International, and has achieved the organisation's most senior designation, the CPP. He is also a member of the Security Institute and is Deputy Chairman of that organisation's Working Group on the Corporate Response to Terrorism.

Phillip is a member of the Institute of Management and Leadership and an affiliate member of the Business Continuity Institute.

In 1999 Queen Elizabeth II presented Phillip with the award of the MBE, one of the country's highest honours, in special recognition of his work in a specialized area of contingency planning.