

## INSIDE THIS ISSUE:

A special investigation	2
Congratulations	3
Recruitment Fraud	4
Convergence	5
Maritime Security	6
New Members	8
Secured Environments	9
Fraud	11
Europe	12
Oops!	13
Piracy	14

## ESSENTIAL INFORMATION

JOINT EDITOR – Helene Carlsson  
(07802 864485).  
helene.carlsson@btinternet.com

JOINT EDITOR – Mike Hurst  
(0845 644 6893)  
mike@hja.co.uk

ADVERTISING –; Graham Bassett  
(07961 123763);  
graham@gbassett.co.uk

ADMIN. MANAGER – Jude Awdry,  
ASIS UK Chapter 208, PO Box 208,  
Princes Risborough, HP27 0YR.  
Tel: 01494 488599;  
Fax: 01494 488590;  
e-mail: asis@awdry.demon.co.uk.

MEMBERSHIP ENQUIRIES –  
Nigel Flower, CPP (01276 684709 -  
email: nigelflower@msn.com)

PUBLISHERS – The 208 Newsletter is  
published by Chapter 208 of ASIS  
International.

FREQUENCY – The 208 Newsletter is  
published four times per year, Spring,  
Summer, Autumn & Winter – please contact  
the editorial team for deadlines.

IN GENERAL – The 208 Newsletter welcomes  
articles & photographs, but while every care  
is taken, cannot be held responsible for any  
loss or damage incurred while in transit or in  
our possession. Please send all material to  
the editors. The Newsletter may publish  
articles in which the views expressed by the  
author(s) are not necessarily those of ASIS.

ISSN NO – 1350-4045

## Formalising Your Competence through Certification

- **How do you carry out a security survey to identify weaknesses in your security posture?**
- **What types of security systems are available to you, and how do they work?**
- **How do you specify an electronic security system for your site?**
- **How do you discriminate between different vendor bids?**
- **What is the procedure for planning, design, installation and acceptance testing?**
- **How do you measure the performance of your security system?**
- **How do you get the best value for money out of your vendor?**

These and many more questions are answered during the PSP (Physical Security Professional) certification programme, a four-month combined distance-learning/residential study programme that begins again in January, culminating in examination in May.

Increasingly, employers and security professionals are appreciating the need for professionalisation

through internationally-recognised certification, and ASIS UK Chapter offers certifications in three areas: Security Management (CPP), Risk Analysis, Surveys, Systems Selection, Design and Integration (PSP), and Investigations (PCI).

Internationally, there is an exponential growth in security professionals undertaking ASIS certifications, which are offered at examination centers in over 150 countries, and regionally across the UK. Take this opportunity now to become a member of the fastest-growing body of certified security professionals in the world by contacting [davidcresswell@arc-tc.com](mailto:davidcresswell@arc-tc.com).

### Special PSP Offer

ARC's PSP Review Course has been completely rewritten for 2009/10. So confident is ARC that you will pass the examination based on this course that in the unlikely event that you should fail the examination, having completed all course elements successfully, ARC will pay for you to resit!

"Both the PSP and CPP credentials have afforded me an international status amongst an elite team of safety and security professionals, and the knowledge gained from these certifications is extremely tangible in



continued on page 3

# A Special Investigation

Let me set the scene. It was 18th September in the year 2009, the eve of the ASIS Autumn Seminar.

The mild evening still held a chill in the air as a group of plucky individuals from ASIS Chapter 208, some accompanied by partners decided to brave the dangers of Whitechapel on a Thursday evening in search of clues to reveal the identity of "Jack the Ripper"!!! They had travelled from all corners of the Empire, Wales, Scotland, Liverpool, Norway!

Able to buy one of Her Majesty's Yeoman Warders (in civilian garb), this daring group, as yet unfortified by alcohol, set forth on their gallant quest.

Using the keen eyes, rapier-like intelligence and forensic skills you

would expect of an ASIS member the team analysed the facts and inspected the crime scenes.

Despite the events taking place in 1888, the group, a combination of Sherlock Holmes, Hercule Poirot, and Inspector Clouseau, managed to find new meaning from the subtlest of clues, putting themselves in the place of the Victorian gentry of the time. "Save fallen women!" one shouted, "Save one for me!" shouted another.

Finally all agreed that there

was just one element missing... beer!

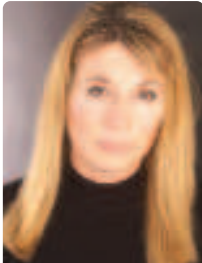
Retiring to a local hostelry for sustenance, the drinking, I mean the deliberation started and after serious thought this ASIS think tank were unanimous in their decision.

The murderer of those five unfortunate women was identified. All will be revealed (or not) in the next thrilling edition of...

THE ASIS NEWSLETTER!!!



## Editorial Team



Helene

### Helene Carlsson – Joint Editor

Helene is working as a security consultant at Atkins, a multinational engineering and design consultancy.

After over 20 years as a corporate security professional (Sweden, UK and internationally) she left the corporate world to work as an independent security consultant. She has worked with many different clients, specializing in most aspects of non-IT Security, Business Continuity and Crisis Management.

Helene has been a member of ASIS since 1989 and on the ASIS 208 committee for many years (too many perhaps). She has been working actively on the Media sub-committee for the same amount of time.

helene.carlsson@btinternet.com



Mike

### Mike Hurst – Joint Editor

After several years in "The City", Mike Hurst entered the fire and security industry in 1989 and worked initially in Sales & General Management positions.

In 1992 he joined HJA Fire and Security, Recruitment Consultants where he is a Director. He recruits at all levels across a range of security disciplines.

He is a Fellow of the Recruitment and Employment Confederation (FREC), and sits on the Verification Board of The Security Institute (MSyI) and has contributed numerous articles to security publications. Mike is Joint Editor of the Newsletter, Webmaster and set up and administers the ASIS 208 Blog.

mike@hja.co.uk



Graham

### Graham Bassett – Advertising and Seminar Exhibitors

Graham is Commercial Director for Momentum Security Recruitment and has worked in the security recruitment sector for some 19 years.

He was also the founder Chairman of the BSIA Recruitment Code of Ethics and also sits on the REC Association of Executive Recruitment Committee (AER), responsible for standards, members benefits and marketing.

Like Mike he is also a Member of the Recruitment and Employment Confederation (MREC).

He is well traveled and his working career has taken him to various interesting spots around the globe to include a three-year assignment in Saudi Arabia.

Graham is an avid supporter of taking ASIS forward within the commercial world of security and is pleased to see such an increase in exhibitors and advertisers supporting the chapter.

graham@gbassett.co.uk

continued from page 1

connection to my daily operations".  
 Drew Donovan, Deputy Chief, Safety and Security  
 Coordination Service, World Intellectual Property Organization.

**Education General**

Worldwide, ASIS International is offering an educational feast in the coming months. Aside from the International Seminar and Exhibits later this month in Anaheim, California, ASIS will be holding its first Middle East Regional Security Conference in Dubai, 6-8 December, with an impressive line-up of over 30 international speakers covering security issues of global concern. UK Chapter members are most welcome to register. And during 25-26 January 2010, the UK Chapter will be hosting the ASIS European Information Assets Protection Conference in London.

The IAP Conference, which will be opened by Alum Michael MP, will address the risks to company-held proprietary information and personal data, and will look at best practice in protecting information against external malevolent threats, employee misuse, and inadvertent disclose.

*David Cresswell MSc CPP PSP MSyI is the ASIS committee member responsible for Education and Certification.*



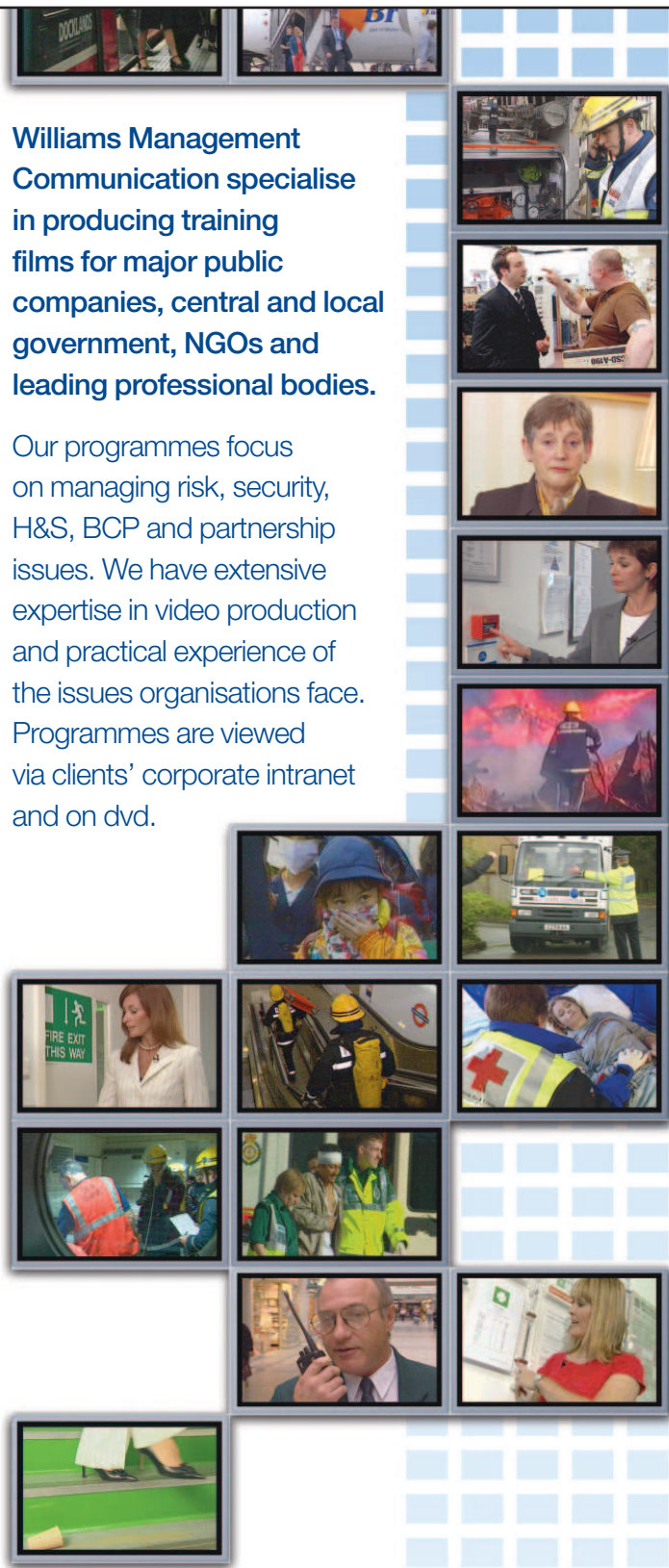
# Congratulations

*Congratulations to the following who passed the PSP Certification examination on Saturday, 12 September with excellent scores:*

- Gavin Wilson, BHP Billiton
- Dan Belai, ATC Systems (Romania)
- Chris Aldous, Buro-Happold
- Spencer Wakelam, Aviva

**Williams Management Communication specialise in producing training films for major public companies, central and local government, NGOs and leading professional bodies.**

Our programmes focus on managing risk, security, H&S, BCP and partnership issues. We have extensive expertise in video production and practical experience of the issues organisations face. Programmes are viewed via clients' corporate intranet and on dvd.



**WILLIAMS  
 MANAGEMENT  
 COMMUNICATION**  
 SPECIALIST VIDEO PRODUCTION

Kingfisher House, 21-23 Elmfield Road  
 Bromley, Kent BR1 1LT

Telephone: +44 (0) 208 315 6700  
 Fax: +44 (0) 208 315 6721  
 email: admin@williamscommunication.co.uk



[www.williamscommunication.co.uk](http://www.williamscommunication.co.uk)

# Recruitment Fraud – Mike Hurst

A quick internet search for “recruitment fraud” produces a surprisingly high number of results showing pages on official company websites explaining that their organisations have been the victims of recruitment fraudsters. In two or three minutes, I found pages explaining this fraud on the sites of many major corporations including Shell, BP, Emirates, Schlumberger, Balfour Beatty and Arsenal FC .

This is a variation on the ‘419’ advance fee fraud. Individuals are approached by people passing themselves off as the recruitment team of a large corporation or as a company acting on their behalf. They will tell ‘candidates’ that they have a position open that they are suitable for, but that they need a sum of money in advance to cover some sort of administration cost. As with the normal 419 scams, these emails are often badly written, in poor English and from unlikely email addresses: however others are more

sophisticated and less obvious.

At a time of recession, with relatively high unemployment, these scams can appear more attractive than they would normally. I would say that this scam or variations of it has been around for many years, but the internet just offers individuals and organised groups another forum for their activities.

No major company or reputable recruitment company will ever ask for money up front and there will always be a formal recruitment process to go through. Be warned.

The other scam that is prevalent at the moment is the ‘CV Writing Scam’. A fraudster puts up a professional looking 3 or 4 page website purporting to be a recruitment company. He then lists a few high-level jobs on the site (e.g. European CEO - £120,000) and posts these on to some of the large job boards, paying by credit card. These attract a good response from applicants interested in the role.

The fraudster then telephones all the applicants, saying that he feels they have a good chance of an interview with his client if only their CV was professionally written. “Can you recommend anyone?” the eager applicant asks. Surprisingly enough the fraudster does know someone and for ‘only’ £350 this person will provide a high quality CV. Apparently some of the CVs produced really are very good, but this is not the point. After a few days, the web site will be taken down and a new one put up and the whole process starts again.

This scam is earning fraudsters hundreds of thousands of pounds, so be aware of any such sites, particularly those that have no land line number or mailing address.

**For more information, please visit [www.safer-jobs.com](http://www.safer-jobs.com) which has been set up by the Metropolitan Police in conjunction with some of the major job boards.**



## HARPER CHALICE GROUP LIMITED

# SECURITY STARTS AT THE PERIMETER

The PulseSecure™ and FenceSecure™ electronic perimeter systems are designed for full integration with CCTV, alarm and security systems, to ensure maximum deterrent to intruders and give maximum warning to the user

PulseSecure™ perimeter security systems Detect, Deter, Deny and Defend against unauthorised access and have an exceptional track record in stopping crime and losses.

Alarm and zone outputs are provided for interfacing with CCTV and other site monitoring systems.



FenceSecure intrusion detection system



PulseSecure deters, defends & detects

For a free site survey and consultation on how PulseSecure™ perimeter security systems can help reduce your security costs and losses contact [sales@harperchalice.co.uk](mailto:sales@harperchalice.co.uk)

HARPER CHALICE GROUP LIMITED, 8 Binns Close, Coventry, CV4 9TB

Tel: +44(0)24 7642 1300 Fax: +44(0)24 7642 1309 [www.harperchalice.co.uk](http://www.harperchalice.co.uk)

# Convergence: our response to the converged threat

– James Willison

As those of you who consider attending conferences will know, Convergence is appearing more frequently and gaining considerable interest from a variety of parties. Why is this? Perhaps as Dr David King, Chair of the Information Security Awareness Forum, recently stated. “Convergence is important because those that pose a threat to our people and organisations are cooperating on a greater number of levels. This includes operating common and complimentary processes. To protect our people, our businesses and our assets we need to keep ahead of the competition.”

It is in response to the increasing awareness of the converged threat to our people, businesses and assets that the ISAF and the SASIG have united to hold a Convergence workshop on September 24th. At the time of writing this is at the advanced planning stages and we are very much looking forward to hearing the views and experiences of representatives from the leading UK Fraud, Physical security, IT/Information Security and Business Continuity organisations. The objective of the day will be to hear from these leaders and then to have two workshops which will involve all the delegates. This will enable everyone to contribute and gain understanding from a wide range of experts in this matter. The final session will focus on important issues raised during the day that can be taken further. We also aim to document current best practise which others will be able to benefit from. It promises to be a most rewarding and important event.

I will report on our findings in the next newsletter.

Some of the topics that we will all consider are: What types of converged attacks are we experiencing? How can we best assess and respond to them? Are most of us still assessing risks in separate silos/functions? Who has experience of converged risk assessments? Are they more effective? Are security leaders increasingly working on physical and IT security projects together, including disaster recovery and BCP? Would convergence reduce the opportunity for employees to commit fraud and cybercrime? Can convergence be applied to our national and international security, fraud prevention, legislative and enforcement agencies? Where do we go from here? Should we urge our organisations to converge more? Or just do little bits of convergence where we can? Of course many other issues will come to the fore and I hope to share these with you in the months ahead.

The European ASIS Education committee are planning an Information Assets protection conference at Nomura’s London HQ from the 25th - 26th January 2010. We are looking forward to the active participation and leadership of various sessions from those in the Physical security and Information security communities. This promises to be a conference which will be relevant to security professionals who are seeking to understand how to protect our information assets from a managerial perspective. This concerns both functions and it is significant that leaders from the Corporate and Digital arena will share the teaching and discussions.

James Willison, Chapter Convergence Lead.



# Maritime Security

## – An Overview – Duncan Macdonald

In support of the recent Autumn Seminar on the topic of Maritime Security, the Newsletter this month contains articles from two of the speakers.

The topic for the Winter Seminar / AGM is Hotel and Travel Security.

On 1st July 2004, the International Ship and Port Facility Security Code (ISPS Code), an International Maritime Organisation (IMO) initiative on the review of measures and procedures to prevent acts of terrorism which threatened the security of passengers and crews and safety of ships, came into effect and was adopted unilaterally by all signatories to the International Convention for the Safety of Life at Sea 1974 (SOLAS). (This incidentally also included a few States which were landlocked with no access to the sea.)

Although some individual States, including the United Kingdom and United States of America, had already addressed the threat from terrorism, as opposed to piracy, and taken the lead to apply preventative security measures, for some classes of vessel and selected ports, to mitigate against both domestic and international terrorism prior to the introduction of the ISPS Code, a large number of maritime States did not have any form of effective security regime in place.

The principle objectives of the ISPS Code were set out as follows to be interpreted and set into a formal practice by respective Contracting Governments. They included:

The establishment of an international framework of procedures and practical measures, between Contracting Governments (the signatories) and their respective Government agencies, local administrations and the maritime industry (ships and port facilities).

Defining the roles and responsibilities of Contracting Governments.

Identifying the risk to maritime operations and setting commensurate Security Levels to meet that risk. (It should be noted that these Security Levels are part of a risk management process which are set by the Contracting Government or a Designated Authority and are separate from national Threat Levels identified by Government security agencies.)

The collection and exchange of security information between respective Contracting Governments, Government agencies and the maritime industry.

Setting protocols for the conduct of Ship Security Assessments (SSA) and Port Facility Security Assessments (PFSA) by Contracting Governments.

Engendering confidence building by the application of security measures.

As part of a co-ordinated response, the ISPS Code also set out a range of mandatory requirements on ports and port facilities, through the management of Port Facility Security Officers (PFSO) to:

Prevent and deter unauthorised access to the vessel or port facility from both the land and water approaches.

Prevent the introduction of weapons or explosive devices into a port or its environs.

Make provision for raising and responding to alarms.

Define protocols to be adopted for the submission of Port Facility Security Plans (PFSP). Similar protocols were set out to be adopted by individual vessels for the submission of Ships Security Plans (SSP).

Identify and implement a regime for regular security training, drills and exercises for all staff to be conducted within specific time frames.

Similar requirements were defined for Company Security Officers (CSO) and Ship Security Officers (SSO) to implement for fleets and individual vessels.

The ISPS Code specifically applies to cargo vessels over 500 gross tonnes and all passenger ships engaged on international voyages and the port facilities serving those vessels. This also included ferry and cargo services between the United Kingdom and the Republic of Ireland, although some provision has since been made to exempt vessels engaged on regular scheduled services from all the requirements, providing they do not deviate from their normal route.

It is recognised that the ISPS Code has generally raised awareness throughout the maritime security industry and has identified a range of mandatory and recommended procedures and measures which should be followed, it does not detail, or set standards for achieving them. This has left it open to interpretation by individual States, based on their own national security standards which may or may not be acceptable to another State. It does, however, make provision for a port operating at a lower Security Level than a visiting vessel, to increase their measures, without increasing the Security Level, in order to operate at an acceptable level as the vessel.

The International Ship and Port Facility Security Code was incorporated into the European Commission (EC) Regulations as EC Regulation 725/2004 with

effect from 01 July 2004, thereby making it a legal requirement for all States within the European Union, including the United Kingdom, to comply with its provisions. EC Regulation 725/2004 was transposed, through Statutory Instruments into UK Law as the Ship and Port Facility (Security) Regulation 2004 and the Ship and Port Facility (Security) (Amendment) Regulations 2005 and forms the basis of a National Maritime Security Programme covering all commercial maritime operations. In 2005, the UK provisions were extended to cover domestic passenger vessels which were engaged on voyages more than 20 nautical miles from land, and in 2007 they were further enhanced to incorporate some domestic sea going passenger and cargo vessels over 500 gross tonnes, including tankers, engaged on all domestic voyages.

#### The United Kingdom Approach

Prior to the attacks against the USA on 11 September 2001, the United Kingdom's maritime security regime was applied by the Department for Transport (DfT) through its Transport Security and Contingencies Directorate (TRANSEC) and governed by legislation covered in the Aviation and Maritime Security Act 1990 (AMSA). However, this only applied to passenger vessels and roll on/roll off (RoRo) services and the ports that served them, either permanently or for a temporary period. Physical security standards at those ports were partially based on those applied at Passenger Airports, albeit with less emphasis on technical innovation. The maritime sector, unlike aviation, did not, at that stage, have a National Maritime Security Programme in place.

Passenger vessels included domestic ferries and cruise ships employed on international voyages, but also encompassed any vessel, including cargo ships, carrying more than 12 fare paying passengers. The latter option applied to the larger cargo vessels, including those on regular exotic voyages to the Caribbean and Americas bringing cargoes of fruit and spices. These vessels could be subject to unannounced inspections whilst in UK Ports, for compliance, by maritime Transport Security Inspectors from TRANSEC.

In early 2003, with the imminent introduction of the ISPS Code, the Department for Transport, through the Maritime Security Branch in TRANSEC, was appointed as the Designated Authority to the Contracting Government (the United Kingdom), tasked with implementing Ship and Port Facility Security Assessments on all vessels and port facilities, which fell within the scope of the ISPS Code, in the United Kingdom and Overseas Territories by 01 July 2004 and thereafter reporting compliance of those facilities to the International Maritime Organisation. Although the ISPS Code had made provision for these Assessments to be carried out by RSO acting on



Duncan Macdonald is an independent Protective Security Adviser and Transport Incident Researcher.

Joined HM Forces from school in 1968 and pursued a successful 25 year military career, including 19 years within the Intelligence Corps specialising in information gathering, protective security and counter terrorism disciplines.

behalf of a Contracting Government, it was decided that in the UK, they should be conducted by the Designated Authority (TRANSEC), both to establish a common standard of approach, and, as a Government Department, to deter any accusation of bias for commercial gain.

However, TRANSEC neither had the manpower, nor resources to conduct all these Assessments within the time frame and it was therefore decided that TRANSEC would concentrate its resources on passenger vessels and the ports and port facilities. The Maritime and Coastguard Agency (MCA), an Executive Agency of the Department for Transport, with Regional Offices around the UK, because of its wide experience in cargo handling operations, would assume responsibility for the UK cargo fleet.

A necessary consultation process was conducted with the UK maritime industry, following which, around 600 port facilities were selected and prioritised into four categories according to the risk they presented or type of cargo handled. Those categories were passenger (PAX), container-roll on/roll off (CRR), chemical oil and gas (COG) and other bulk cargo (OBC). The chemical, oil and gas industry, which had been previously regulated by the former Department for Trade and Industry (DTI) and had sufficient security measures and contingencies in place, was not subjected to the Assessment process. The OBC

ports, considered, to be least at risk from terrorist attack, were subjected to a Self-Assessment process using a template produced by TRANSEC. The remaining three categories (PAX, CRR and COG), considered to be most at risk, were subjected to a Port Facility Security Assessment (PFSA) by Transport Security Inspectors, and included recommendations to improve security. The PFSA process was completed both in the UK, her Crown Dependencies and Overseas Territories ahead of the July 2004 deadline.

Port Facility Security Assessments, conducted by TRANSEC and corresponding Ship Security Assessments, formed the basis upon which individual Company Security Officers (CSO), Ship Security Officers (SSO) and Port Facility Security Officers (PFSO) formulated their respective plans and contingencies which had to be submitted and approved by the Contracting Government prior to the issue of a Certificate of Compliance. The Port Facility Security Plan (PFSP) had to comply with a standard template and include detailed contingencies for enhancing measures for the three Security Levels in addition to detailed plans of their Restricted Areas, Temporary Restricted Areas and Controlled Buildings.

Separate exercises were conducted in TRANSEC to identify a suitable security training regime for Port Facility Security Officers (PFSO), and to identify a common set of physical security standards which could be applied by degree to each port facility. They had to be both practicable and achievable, within the capabilities of available manpower and resources of

each facility. Since the costs of security enhancements were met by the industry, this could only be achieved with their cooperation and agreement. In addition, an approval and accreditation process for Port Facility Security Officer training providers, not required by the ISPS Code, was introduced as a mandatory requirement in the UK so that training providers could both understand and deliver a standard of training to meet the DfT's requirements. The MCA conducted similar exercises in respect of Company Security Officers (CSO) and Ship Security Officers (SSO).

In addition to addressing the issue of security within ports and on board vessels, TRANSEC, in conjunction with the Maritime and Coastguard Agency, has taken a leading role in the promulgation of Marine Guidance Notice 298, which deals specifically with Measures to Counter Piracy, Armed Robbery and Other Acts of Violence against Merchant Shipping to all ship owners, companies and Masters of Vessels. It was recognised that this not only applied to UK vessels, but was also intended for UK nationals serving on board foreign flagged vessels. Whilst this document is unlikely to prevent piracy attacks, it does raise awareness and offers practical advice to reduce the risk from such attacks.

*Finally, maritime security within the UK forms part of the UK's "CONTEST" recently approved new National Security Strategy.*

## Welcome to these new Members!

Andrew Allan		Warren Kilburn	
Naser Awad		Richard Knowlton	Vodafone
William Ayamdo	Ghana MoD	Mike LaCorte	Conflict Intl.
Alec Barclay	Gallaher Ltd	Lukman Longe CPP	Nigeria LNG
Thomas Barker	Janusian Security Management plc	Alistair Macrae	Lynceus Ltd
Stuart Bradshaw	Sussex Police	Andrew Morris	
Andrew Clancy	Met. Police	Robin Orrells	
Simon Clarke	G4S Risk Man.	Bob Owen	Metropolitan Police
Giles Clayton-Jones	Lynceus	Andy Palmer	Associated Security
Ian Currie	Shell Petroleum	Stephen Payne CPP	JT Intl
Colin Dann	Wilson James Ltd	Kelvyn Pearce	Momentum Rec.
Andrew Dean	VF Services UK	Roy Powell	Gallaher Ltd
Penny Derham	British Embassy Bangkok	Nicholas Probert	
Francis Doherty	Worldwide DCS	Rodney Rush	
Kevin Drake	Control Risks Thomas Dyson	Robert Scanlan	
Christopher Fearn		Malcolm Shearer	
Mark Fermor	NCG Media	Llywelyn Skidmore	International Atomic Energy Agency
Peter Finch	Sandwell & West Birmingham Hospital	Mark Skinner	
Peter Flockhart		James Tamblin	
Matthew Gouldby	Signet Jewellers	Tony Thornton	
Toby Harding	Pilgrims Group Ltd	Richard Trim CPP	VISA Intl
Kywanna Hopkins	SGS Group	Caroline Waddicor	
Rebecca Hoppe	Shell	Harry Watters	Diageo
Wayne Hunt		Jerry Woods	University of Bristol
Dino Ilaria		Cornelius Wussah	
Dean Jenkins			

# 'Secured Environments': a new police award for organisations that get their security management right



Katy Owen of Perpetuity discusses the new police crime prevention accreditation.

For the first time organisations that follow good security practice can be accredited by the Police as a 'Secured Environment'. Surely of all the accreditations available this is set to become la crème de la crème amongst them all. Ask yourself this, if you are good at security why would you not want a 'Secured Environment' accreditation to impress staff, customers, the Board and shareholders?

'Secured Environments' is an accreditation awarded by the police to organisations that can prove that they are adopting good security practice. It has been developed by the Association of Chief Police Officers Secured by Design (ACPO SbD) in conjunction with Perpetuity Research and Consultancy International Ltd. It is part of the 'Secured by Design' suite of crime prevention initiatives managed by ACPO SbD. Importantly Secured Environments focuses on management and processes rather than products, equipment and physical building design.

Crime prevention measures often fail because they are implemented incorrectly, poorly managed or even because they were not the correct response to a problem in the first place. Secured Environments has been developed to help rectify that. The accreditation is based on six key

principles of good security management that have been developed based on a review of best practice from around the world and honed by the experience of crime prevention experts. Organisations that can show that they have met the six principles for protecting themselves against crime are accredited as a 'Secured Environment'.

## So what are the principles?

The Secured Environments accreditation is different to other police awards, because it is not conditional on design issues, nor specific physical security requirements, rather it focuses on people, process and strategy. After all, as security professionals well know, without the support of staff at all levels supported by good plans, processes and procedures for managing security, it will inevitably be compromised.

To meet the first principle an organisation must demonstrate that its management team are committed to creating a Secure Environment. Not only does there need to be evidence of commitment from the senior leadership team, but members of staff also need to believe that the organisation is committed.

The second and third principles require the organisation to show that they understand its crime risks; analysis of data on incidents plays one part of this. Based on a good understanding of the problem organisations must have a plan in place to mitigate risks. Clearly the response needs to be appropriate and proportionate. In order to demonstrate this, managers will need to be able to describe the threats posed to their organisation and explain how these risks are recorded, monitored and analysed. They also need to be able to explain why specific security measures are in place within their organisation and how these address the problems they identified.

The management and implementation of security measures are the focus of the fourth and fifth principles. Organisations must demonstrate that they have a security plan in place with clear objectives. They also need to show that they have adopted appropriate processes to ensure that crime prevention measures are implemented effectively. In addition all employees need to be aware of their roles and responsibilities with regards to security. In many of the evaluations of crime prevention that we at Perpetuity carry out, poor implementation is often the reason for failure.

And finally, but by no means any less important, an organisation must be able to explain how their security measures are monitored and evaluated and provide examples of how these findings are fed back into their security systems and processes.

### What next?

Since its inception in 2007 a number of organisations have gone through the process and achieved the award whilst many more are currently working towards the award. The Universities of Bath and Bristol were the first to receive the accreditation and since then many more have followed. It has received excellent feedback from all of those involved,

'The Secured Environments auditing process is professionally conducted by well qualified consultant staff; the auditors probe the practices and procedures within the organisation and importantly seek out evidence to support the criteria under examination. It is comforting that the auditors looked at all levels of commitment and service from senior management to the security practitioners; in addition they sought the perceptions of our customers, the staff and students of the University.' Head of Security Services, The University of Bath

'Taking part in the Secured Environments scheme has enabled us to take stock of our existing processes and identify potential areas of vulnerability. It has proved invaluable in terms of future business development and will be regularly reviewed as the business continues to grow.' Managing Director, Media Outcomes

'It was good to get an independent audit of the school's security measures and processes; I would recommend it to all schools. We have received a lot of positive press as a result of the award, and it sends out the message to parents that their children are safe.' Headteacher, Brentside High School

Clients have cited a range of benefits including:

useful feedback on ways to improve existing

security management processes, demonstrate to staff and clients that security is taken seriously, justify security investment

Furthermore, in the current climate where competition is tough, many have also used it as a marketing tool and a point of difference. Indeed the benefits cannot be understated.

Secured Environments - operated and managed by Perpetuity on behalf of ACPO SbD - is a versatile scheme. Indeed any type of organisation - large or small - can register to become a Secured Environment including hospitals, hotels, schools, universities, businesses, shopping centres, financial institutions and night-time economy establishments.

'Secured Environments is a real heavyweight in terms of a security world, many others have not got the academic rigour and background.' Head of Estates, The University of Bristol

**For more details about Secured Environments and how you can get involved with the initiative please see the police webpage**

**[www.securedenvironments.com](http://www.securedenvironments.com) or contact Perpetuity (+44 (0) 116 222 5555; [securedenvironments@perpetuitygroup.com](mailto:securedenvironments@perpetuitygroup.com)).**



Jerry Woods – University of Bristol,  
Superintendent Geoff Spicer - Avon and Somerset Police, Katy  
Owen – Perpetuity, Brian Schofield – University of Bath



# Fraud, the credit crunch and growing temptation.

The Association of Certified Fraud Examiners 2008 Report to the Nation revealed occupational fraudsters are generally first time offenders with small businesses being especially vulnerable to costly occupational fraud. This can be found together with comprehensive new guidelines for fighting fraud at <http://www.acfe.com>.

This month has seen another depressive drop in the economy. Retail sales are down, fewer mortgages have been granted and fuel, oil, electricity and gas have all seen sharp price increases. There are few optimistic economists around and the long term picture looks grim.

In this relatively harsh economic climate employees can find themselves with growing financial burdens, increasing debts and no long term solutions to their problem.

As the Association of Certified Fraud Examiners Manual points out when this problem is non-shareable it contributes to what has become the classic model for occupational offending; the fraud triangle?.

One side of the triangle represents a perceived non-shareable financial need, the next represents a perceived opportunity and the last is rationalisation.

The perceived non shareable financial need is important and may result from many factors, the feeling of personal failure, a business failure, physical isolation with no one with which to share their problem, a desire to improve their status or importantly in this economy, employer-employee relationship. If an employee resents his status within the organisation maybe because of perceived economic inequalities, such as low pay being overworked or unappreciated but has no choice but to continue working for the organisation his need will be non

shareable. Likewise if they have debts resulting from activities which would be frowned on by their peers (e.g. gambling) they would consider to be non-shareable.

Most trusted employees can use their general knowledge and technical skills used in the job role to create a perceived opportunity to violate their trust without being caught.

Rationalisations occur before the event; the offender will not view themselves as criminal and will justify their actions to maintain in their own mind the status of a trusted person. The justifications may take many forms but all seek to rationalise their actions they can range from "I'm only borrowing the money" to "it's a necessity to save my family from shame".

When these three elements co-exist the organisation is susceptible to employee fraud but companies can do much to prevent fraud. A sound fraud prevention programme should be adopted by all companies. This requires a combination of systematic controls, monitoring and inspection, employment practices and ethical behaviour. (See Risk of Fraud: A practical guide at [www.acfe.com](http://www.acfe.com))

The ACFE Report to the Nation 2008 cited Lack of adequate internal controls as the most common factor that allowed fraud to occur. The following are some of the most common internal control weaknesses which are, in most cases, simple to remedy. The lack of management reviews. The lack of segregation of duties, common in many small or family run businesses. The implementation of simple but strict procedures can easily remedy this weakness. The lack of physical safeguards, the lack of independent checks, the lack of proper authorisation on documents and records, allowing the overriding of

existing controls, a lack of employee fraud education and an inadequate accounting system.

Importantly companies can be proactive and look out for the "red flags" that are frequently present in many cases of employee fraud. Typically the fraudster will display symptoms of fraud which can be spotted by the alert employee, manager or auditor. The list is not definitive but it includes unusual or changes in behaviour. This may manifest itself in the employee never going sick or taking any long vacation or delegating work to others as someone else doing their work may discover discrepancies. The employee may display signs of an extravagant lifestyle with continuously new designer clothing, expensive holidays or new cars beyond the reach of those in similar employment. Other changes in their behaviour defensiveness, irritability and suspiciousness may be ways of continuing to conceal their acts. Whilst yet others might include increased drinking and or smoking.

There are two sorts of companies, those that have been affected by fraud and those that haven't...yet. The Report to the Nation states that the implementation of anti fraud controls has a measurable impact on an organisations exposure to fraud, with such stark evidence it must be the duty of every CEO to keep their fraud prevention programmes up to date and continually improved.

The Association of Certified Fraud Examiners can provide training on all aspects of fraud from preventative measures to effectively investigating frauds that have been committed.

**Tim Harvey, CFE**  
**Director of UK Operations,**  
**Associated of Certified Fraud**  
**Examiners**

# Security Sector has benefited in Europe

*From 2002 – 08. wage inflation in the EU15 has averaged 28% yet those in the security risk sector have seen salary increases of up to 60% in the same period. Peter French of SSR Personnel, believes this is due to the increasing importance corporations are placing on enterprise risk.*

The period 2002 – 08 has seen increasing government regulation and this has created a \$4bn world-wide service sector alone. Whilst the focus of the world may be about risk in the banks, corporations

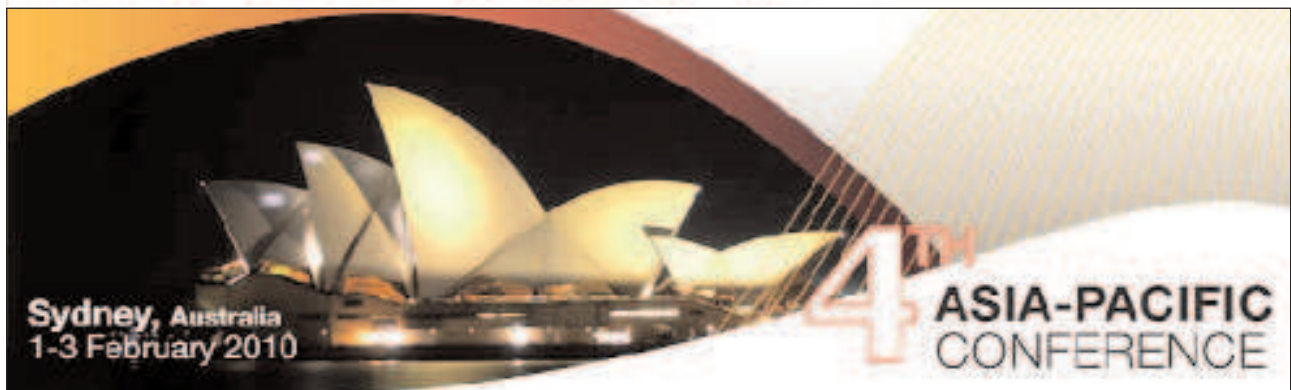
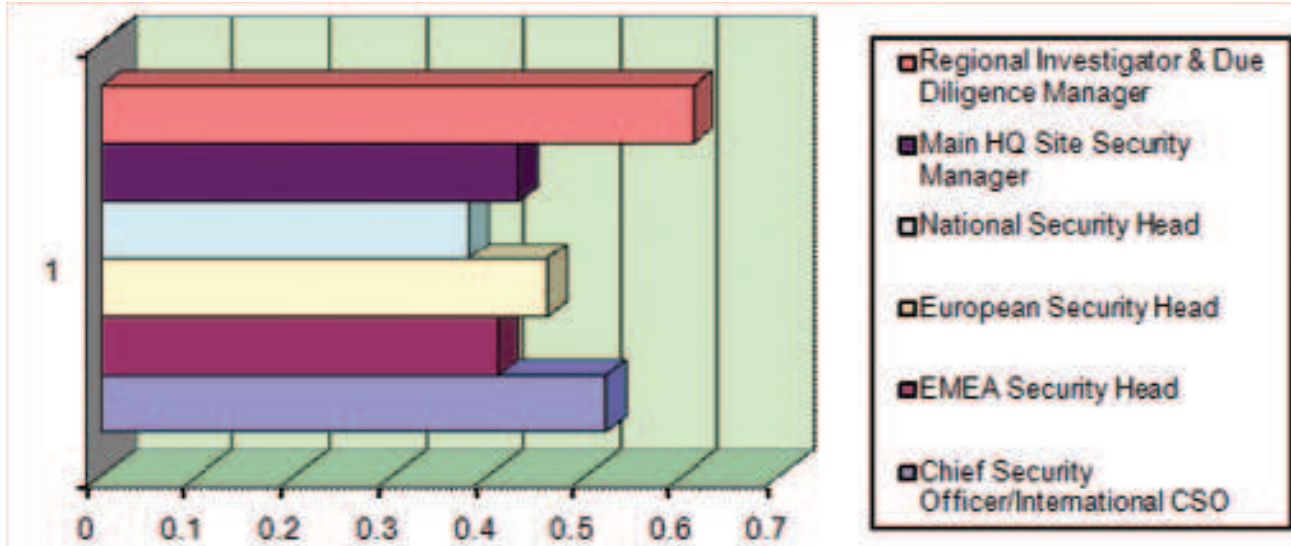
will still need to be risk takers if they wish to maximise earnings. The corporate suite has counterbalanced those risks through empowering compliance officers with a greater independence to advise the executive on how they can protect the corporate brand and reputation. Out of that process, executives have identified the need for defined security competences but with a business knowledge of their sector.” French believes that “The business security executive is being exposed to greater requirements, in many cases there are no instant security patches, but the demands of the corporation to reduce unnecessary processes can expose the C-suite to the charge by shareholders that they have been reckless.

Over the past 10 years security has become embedded in many leading corporations with a growing emphasis on due diligence. How that is promulgated may provide a

commercial advantage. Competent individuals to lead or carry out the process are most certainly in short demand, hence basic remuneration for the period increasing by up to 60% for Regional investigators and Due Diligence Managers.

Across all relevant job families for the security sector, wage inflation is ahead of the average wage settlement. In the current year, as the SSR® Annual Survey has shown, remuneration will be with limited bonus payments. However, in the second half of 2009, we should see critical staff rewarded with significant remuneration increases, as in many organisations underlying profitability has remained strong.

Enterprise risk will be a topic for the foreseeable future requiring increasing numbers of people who have adaptable collaborative skills.



# OOPS!

## Cop arrests girl, 5 – twice

A German police chief has come under fire after arresting a five-year-old girl for playing too roughly with his son - and then charging her for giving him the finger.

Little Monika Kretzmer was in tears when the police chief - named only as Wolfgang M for legal reasons - drove her home under arrest when she upset his son at a sandpit.

But the furious cop arrested her again a few days later when she saw him in uniform and allegedly stuck a finger up at him.

The police chief despatched a team of officers to the family home in Chiemgau, Germany, to warn her parents of her actions and tell them she would be charged with anti social behaviour.

The family have filed a complaint

## Police bust scientific experiment

Dutch police swooped on what they thought was an illegal cannabis farm - only to wreck a scientific experiment.

The plants were part of a legal experiment on the use of cannabis fibres in textiles, paper and synthetic materials by the University of Wageningen.

"More than half the plants were destroyed," said Simon Vink, spokesman for the university, according to the Daily Telegraph.

"The project had been underway for years and was in its final phase, which would have allowed us to introduce these new fibres to the market.

"We will probably suffer big losses; we are busy doing the calculations."

He added the university, in the east of the country, was "busy talking to the police" about recovering costs.

Police had announced the discovery of about 47,000 cannabis plants with an estimated street value of more than £3.8m.

## Burglar left dog at crime scene

Police in Gateshead hope to catch a burglar who left an unusual clue at the scene of the crime - his pet dog.

Officers found the small white Jack Russell following a break-in at an infants' school, reports the Daily Telegraph.

Northumbria Police are now looking after the dog which they have named Bobby, although there was no name on his collar.

Officers were alerted to the burglary by a member of the public who heard banging at the school, which police have not identified at the request of the head teacher.

When they arrived, the thief had already fled empty-handed, possibly alerted by a burglar alarm going off, but the Jack Russell was still on the premises.

## A US judge ordered a defendant's mouth to be taped shut.

Judge Stephen Belden, of Canton Municipal Court in Ohio, said it was the best way to restore order after Harry Brown, 51, kept butting in, reports The Repository.

The judge ordered a court official to put duct tape over robbery suspect Brown's mouth after he kept complaining about his court-appointed lawyer.

After a warning, the judge told the bailiff to tape Brown's mouth shut.

When the tape was finally removed, Brown complained that the judge wasn't being respectful. The judge ended the hearing and sent the case to a grand jury.

	1				6			
4				3	2			5
2		5					3	
				5		9		2
	9		4		7		5	
6		3		9				
	4					1		8
9			7	1				6
			8				9	



Mark Harris left the British Army in 1994 with the rank of Major. While serving with the UN in Cambodia, in 1992, he and his team of military observers were taken hostage by the Khmer Rouge and were to be executed for being members of the UN. Since 1994, Mark has worked on numerous crises including kidnaps, hostage taking, piracy and threat related extortions. He is now Global Team Leader of the ASI Global Response Team.

**W**e have been very busy in the last eighteen months providing advice and counsel to ship owners or operators as they face the issues surrounding a hijacked vessel.

The majority of the work has focused on vessels taken in the Gulf of Aden, Horn of Africa, and the Somali Basin.

As the monsoon season comes to an end in mid-September, owners and operators of vessels that transit the Gulf of Aden, and whose vessels are considered to be “at risk”, should be reviewing the precautions they are taking and ensuring their policies and procedures are up to date and handy.

Our experience has shown that there is a very wide ranging difference between companies that are both ready and rehearsed to respond to a hijacking, to

# Piracy and armed attack against ships

– Mark Harris

those that have had their heads in the sand and hoped against hope that their vessel will not be taken. That there are vessels still transiting the Gulf of Aden without informing MSCHOA or registering with UKMTO prior to making the transit is verging on the negligent. That there are vessels doing this without any form of precaution is verging on the criminally negligent.

The media, the general public and those one removed from the immediacy of a ship hijacking will often focus on the speculation surrounding the ransom and that negotiation. However, it is our experience that there is far more to a hijacking than just the negotiation with the pirates and the payment of a ransom. In fact, it is the negotiation with the pirates that is one of the simplest and least demanding aspects of the overall response. The hard part is identifying all of the participants and ensuring that the response to all of the participants is timely, appropriate, and consistent with all other information, passed to other participants.

So then who are the participants in a hijacking? Most immediate to the event will be the Master, officers and crew of the vessel, the pirates on board the vessel, and the management team that is responding to the issue. However, almost straight away, one of the most important group of participants has been

neglected; the families of the crew. At the start of every meeting during a case, it is important to ask how the families are, and what the company is doing for them. The pirates know how to use the families and they have demonstrated this many times. One only has to read the numerous blogs and websites that are springing up now to see how effective they are.

Numerous complaints from Russian, Estonian, or Ukrainian wives claiming their husbands, or sons are “dying of hunger”, “dehydrated and too weak to stand anymore”. These same men are able to walk strongly down the gang plank some 30 to 40 days later after saying they were dying or too weak to stand anymore, their wives victims of a pirate ruse.

These days a great number of vessels are crewed through crewing agencies. There is no doubt that the majority of these agencies are extremely competent and are able to support the owner/operator in looking after the families. However, this is not always the case and owner/operators must ensure from the very first moments of an event that they are confident the families are being looked after. If they are not 100% satisfied then they must take it on themselves, or at least strengthen the efforts to make sure the families understand the process and are briefed on what to expect.

The list of participants and stakeholders in the event extends far beyond those already mentioned.

Consideration in any response to a hijacking must be given to the commercial dynamics. Therefore the management team must liaise with cargo owners, insurers, and lawyers. They need not only to update them on what strategy has been adopted but also listen to their concerns and be able to answer them satisfactorily.

Vessels are now crewed by a number of nationalities and the management team needs to establish and maintain contact with the various diplomatic missions representing their crewmen. Not only will the pirates try to exploit the diplomatic angle, but the company will need the diplomats to assist them with passports and visas when it comes to repatriating their crew post-event as their documentation will have been stolen by the pirates.

Lastly, the management team will need to consider their liaison with international bodies and coalition naval forces.

When asked what the critical issues are when responding to a

piracy event are, I would list the following:

Setting the objective – it is imperative that the management team set their objective early in the response process as this unifies the team and other stakeholders.

Safety of the crew against threats – above all else, one must remember that the crew must be kept safe and everything reasonable must be done to keep them safe

Family management – get it started early and devote resources to sustain it throughout the event and after as well, if you look after the families you will be able to maintain your focus on getting the crew free

Media coverage – it is essential that you do your best to minimize the media coverage of your event; responding correctly and ensuring families and diplomatic missions are handled correctly will help greatly in doing this

Early planning of the end phase and recovery – as soon as your vessel has been taken you need to set up a team to start planning the end phase covering the recovery of the vessel to a safe port and the repatriation of the crew

When planning the response,

companies must ensure they have a robust management system in place to sustain the effort. All companies will have an emergency team ready to handle spills, fires on board a vessel, collisions etc. But an emergency will have a specific time period; a hijacking can last for three to four months. Therefore, there needs to be a transition between an emergency team and an on-going management team, a crisis team. In addition, the crisis team can stand on its own, it requires support, it needs functional support teams.

So, looking to the immediate future, what do companies need to be thinking about? They need to make sure their crews are prepared and that they know how to behave should they become victims. Also, companies must be sure that they have a system to look after the families in very quick time. The owner/operator must have confidence in their crewing agencies and be ready to look after the crew once the event has come to a close. Above all else, owners and operators must be able to declare that they have demonstrated a duty of care.

### **Stephen Emmins, who serves on the Chapter membership committee was granted the Freedom of the City of London at the beginning of September.**

One of the oldest surviving traditional ceremonies still in existence today is the granting of the Freedom of the City of London. It is believed that the first Freedom was presented in 1237.

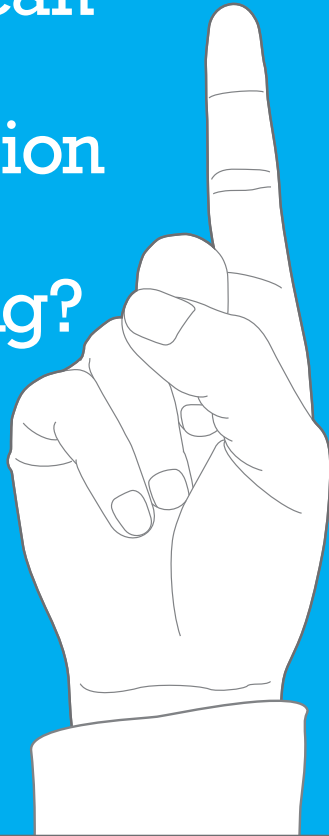
The medieval term 'freeman' meant someone who was not the property of a feudal lord, but enjoyed privileges such as the right to earn money and own land. Town dwellers who were protected by the charter of their town or city were often free - hence the term 'freedom of the City'.

All freemen receive the book of 'Rules for the Conduct of Life', written by the Lord Mayor, 1737-8. The freedom of the City is closely associated with membership of the City livery companies and Stephen is a member of the Worshipful Company of Security Professionals, successors to the ancient guilds.

*For an insight into the fascinating history and modern role of the Livery, visit [www.wcosp.org](http://www.wcosp.org)*



Who's number one  
in European  
IP alarm  
transmission  
and  
monitoring?



**iris**  
**touch**  
IP security to go

When it comes to IP in security, one company's systems are used by more major organisations, from banks to retail chains, than any other, are independently certified to the highest European standards and approved by most major insurance companies across Europe.

The name of that company is Chiron, and the name of the product is IRIS Touch, no wonder it's number one.

The IRIS Touch. Come and see the full story at...

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



Dual path



Independently certified



Back up monitoring centre capable



Remote upload/download



Alarm plus services



Connects to all alarm panels

Chiron Security Communications Ltd

Telephone: +44 (0)118 988 0228 Email: [sales@chironsc.com](mailto:sales@chironsc.com)

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



Chiron Security Communications part of Chiron Technology group of companies

# ASIS Diary

## 2009

20th Nov 2009 Winter Seminar – Canary Wharf, London

6th – 8th Dec ASIS Middle East Conference – Dubai

## 2010

25 – 26th Jan ASIS European Information Assets Protection Conference, London

1st – 3rd Feb ASIS Asia Pacific Conference – Sydney, Australia

18th Mar 2010 Spring Seminar – London

18 – 21 April European Conference, Lisbon, Portugal

17th Jun 2010 Summer Seminar – London

16th Sep 2010 Autumn Seminar – venue t.b.c.

9th Dec 2010 Winter Seminar & AGM – venue t.b.c.