ASIS International

208 News

THE UK CHAPTER ASIS INTERNATIONAL

OCTOBER 2007

INSIDE THIS ISSUE:

CHAPTER CHAIRMAN TOLD TO GET ON HIS BIKE

Despite the fact that the first flush of youth having passed them by about the time Mafeking was relieved, Chapter Chairman Derek Webster accompanied by trusty sidekick Chris Brogan, left Twickenham for Paris on September 11th. Nothing surprising there except they were cycling in support of the charity Scope.

Their departure was delayed due to a compulsory stop at the Scrum Bar. They arrived safe and sound at 16:50 on 13th well in time to see England's match (if you can call it a match) against South Africa. They have raised almost £5,000—Well Done! Rumours they are cycling to Beijing for The Olympics have not been denied.

New CPP Programme

The demand for CPP Certification on the UK is increasing dramatically and the issue of trying to coach and examine these numbers is presenting a problem. However there is a solution! Following this week's committee meeting, the following has been agreed. ARC Training, who manage the CPP training programme on a 'non profit making basis' on behalf of the UK Chapter of ASIS International is delighted to announce that beginning 2008 it will be conducting 2 CPP certification examinations p.a. – *cont page 3*

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@momentumesecurity.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

Chairman's notes will return next month

Editorial Team

Helene

Helene Carlsson – Joint Editor
After over 20 years as a security professional in the corporate world (Sweden, UK and Internationally) Helene thought the time was right to explore the consultancy business.

In 2003 she started up her own business and has been working with Greymans Ltd, a Business Risk Specialist company. She is also working as an independent Security Consultant specializing in most aspects 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 and 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 Member of the Recruitment and Employment Confederation (MREC), and sits on the Verification Board of The Security Institute (MSyl) and has contributed numerous articles to security publications. Mike is Joint Editor of the Newsletter, Webmaster (the new web site is under construction) 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@momentumsecurity.co.uk

New CPP Programme

The examinations will be on May 3, 2008 and November 1, 2008. Each examination will be preceded directly by a one-week condensed "crammer"-type course, for which a distance learning preparation programme will be available four months earlier.

Precise dates are as follows:

EXAMINATION 1/2008

Distance study begins: End January
Preparation programme: 28 April – 2 May
Examination: 3 May

EXAMINATION 2/2008

Distance study begins: End July
Preparation programme: 27 – 31 October
Examination: 1 November

Package cost (including accommodation)
£1225 + VAT for Region 25 ASIS members (Applicants outside Region 25 should contact Janet Ward).

For details on how to register, contact the Professional Certification Representative, David Cresswell. Upon registration and receipt of payment you will be sent a copy of the CPP Study Guide.

Please note that there is no change to the PSP certification schedule:

Distance study begins: End July
Preparation programme: 27 – 31 October
Examination: 1 November

Women in Security – Breakfast Seminar

In addition to the regional Seminars (initially Manchester and Bristol) and the forthcoming CCTV Seminar, Chapter 208 is running a
WOMEN IN SECURITY – BREAKFAST SEMINAR

Thursday, 25 October 2007

Prudential plc, Laurence Pountney Hill, London EC4R 0HH


Jacqueline Walker


Lynne Davies


Sharon Williams

THE PROGRAMME IS AS FOLLOWS

08:00 Coffee and breakfast

08:45 Welcome and Introduction
Derek Webster – Chairman of ASIS UK Chapter

Barriers to Success
Alison Miller

Cameo Talks from Successful Women in Security
Lynne Davies – BP
Sharon Williams – American School in London
Jacqueline Walker – Prudential
Jane McKenna – Chubb

Questions & Answers

Seminar Closing
Lynne Davies

Coffee and networking

10:30 Seminar closed

Maximising the potential of Integrated Systems

In this article Peter Goodenough takes the opportunity to express his views on how business and organisations can maximise on the benefits of an integrated approach to security.

The electronic security industry has certainly made substantial progress towards delivering true system integration over the last few years. You may however have heard it referred to under a variety of names e.g. amalgamation, convergence, fusion, unification - all of these words are currently being used to describe the process of delivering some form of an integrated security solution. By doing so they offer clients the potential of maximising on the benefits from their investment in security systems by way of ensuring that those systems interact and provide security personnel and management with what could be mission critical information.

Long gone are the days when teams of integration experts were unable to produce anything more than a mimic panel with LEDs that flashed if and when an intruder or fire alarm system was activated.

The evolution from analogue to digital equipment, the increasingly acceptance of IP and the introduction of sophisticated software, made possible by the recent dramatic increase in computer processing power are some of the factors that have brought us into an era where true system integration is possible.

Are Global Integrated Systems Effective?

Integrated systems offer the potential of efficiency, flexibility, simplicity and economy. There is the danger however that in reality, integrated systems will often prove to be inefficient, inflexible, complex and expensive. The consequence of this being disappointment among clients whose expectations of the system are far higher that what is actually delivered.

Is this a result of a misunderstanding between the client and the system integrator as to what can be achieved or perhaps the combination of a poor design and planning? Is it a case of the hardware and/or software not being fit for purpose? It could be any or all of these but if the component parts of the integrated system have been sourced from reputable manufacturers and a competent system installer has been chosen to implement the integration, the cause of the disappointment might be down to more mundane but still very important issues such as:

- ***The absence of operational procedures***
- ***Inadequate training***
- ***Incorrect or incomplete data entry***
- ***No naming conventions***

Peter Goodenough is Sales and Marketing Director for Frontline Security Solutions. Peter has worked within the electronic security industry for over 15 years and is a keen and active member of ASIS

- ***No process in place for feedback or the tracking of corrective measures***

When these issues arise they are normally symptomatic of the fact that within the client's organisation there is not singe person "ownership". They may therefore be ignored until problems arise with responsibility for falling between the security and IT functions of a business.

Taking Control

In reality it is the lack of post installation controls and procedures that hinder clients from

getting the maximum out of their integrated system. It may be time consuming, it may be a hard slog but there is no way around putting procedures in place to ensure continuity and consistency in the way systems are managed across all the client's sites which may even be in different countries. This is the quite often the **missing link** that prevents the effective delivery of information from **'security system'** to the **'operator'**.

Coordination

System integrators have an obligation to their clients to make sure they fully understand that the small investment needed to put proper procedures in place will save them money in the long term and deliver immediate results. The clients may however not have any person on board who has the required level of expertise and even if they do, that person may not have the time to take on the responsibility of driving though the implementation of the procedures.

This human resource does not however have to be part of the client's headcount. A number of system integrators have recognised the requirement and have built a team of people who have the necessary operational experience as well as technical expertise in both hardware and software disciplines. These true integration experts, who we call Operation Coordinators, can be imbedded into clients' businesses for a period of what will typically be a two to three months. The objective would be to fine tune the system to meet the clients' specific operational needs and in parallel produce procedures as well as fully train anyone who needs to interact with the system.

The benefits are obvious and immediate in that the system delivered very soon matches the system specified. Clients therefore get a fully functional system and among the operators, the system has far more credibility as a result of everyone understanding how to get the best out of it.

Perhaps the time has come for the role of the Operation Coordinators to be included in specifications for major projects. This will ensure that everybody involved in a system integration project i.e. consultant, client, system integrator and manufacturers place a greater emphasis on planning for the post-installation operation of the system.

How criminal is criminal crime?

By definition, computer crime is a criminal activity involving information technology. Examples of this are unlawful access to computer systems, unlawful interception or interference of telecommunication, systems and data, misuse of devices and software, forgery and electronic fraud.

But how useful is this definition in terms of understanding computer crime for the purpose of prevention and investigation? It is easy to assume that it's all about technology but in fact, computer crime is committed by people and psychological research is critical in the understanding of computer crime.

The US Department of Justice distinguishes between 3 categories of computer crime. The first category is computer assisted crime, where the computer is used as a tool to commit traditional crime online. Examples are fraud, gambling, child pornography, piracy, and harassment. The second category defines the computer as incidental to the crime where the computer can be seen as an accomplice. The computer is incidental in as far as it is used for filing, personal information and emails. The third category is computer targeted crime and is the most commonly reported in the media. Here the computer is used to attack a victim's system in terms of its confidentiality, integrity and availability of data or systems. Examples are denial of service attacks, viruses, theft of services, and theft of information such as trade secrets.

Coincidently the majority of resources are allocated to creating technical barriers to prevent computer targeted crimes. However, computer crime does not necessarily fit into just one of the above categories. Criminals will use a combination of non targeted methods to achieve their objectives. They utilise the huge gaps in non technical security and exploit the weakest links which are employees, management and organisation's often insufficient security procedures. This is achieved through the infiltration of the victim organisation or social engineering in order to obtain physical access to data and systems via other employees. Therefore, psychological aspects of both offender and victim behaviour need to be considered in order to maximise security and minimise computer crime risk.

It is critical to understand the psychological and particularly psycho-social aspects of computer crime in order to implement effective security strategies and raise security awareness that goes beyond technology, procedures and policies. Moreover, an understanding of fundamental principles of human behaviour and the nature of fast changing social contexts provide great opportunities for psychology to make a difference in the fight against crime. Often crime is understood with the benefit of hindsight but by looking at how people form beliefs and attitudes and construct their own realities, it is not surprising to find that security strategies mismatch the mental model of how people actually perceive computer crime. For a more detailed discussion of the psycho-social factors in the implementation of information security policy, see Mich Kabay's article in The Risks Digest, 1993.

To that extent it is important to understand how the general public perceives computer crime as those beliefs and attitudes play a fundamental role in their day to day working behaviour and security consciousness, regardless of how much direct responsibility they carry for security at the workplace. A perceived absence of violence in computer crime makes it more challenging to think of computer crime as criminal. It is easy to understand the aspects of a violent crime and empathise with the victims. With regards to computer crime it can

Simone Zimmerman is a Forensic IT Consultant with Grant Thornton's Forensic and Investigation Services Practice in London and is currently seconded to the Digital Forensic Unit at the Serious Fraud

Pre-Seminar Dinners a Success

The pre-seminar dinner initiative is proving to be a big success.

Held the evening before the seminars, the informal dinners, normally sandwiched in between a swift drink in the bar give members, speakers and guests an opportunity to chat and network.

Since most seminars are in London, they also give attendees and additional reason to come in to town. The last two dinners have attracted over 30 and 50 guests respectively.

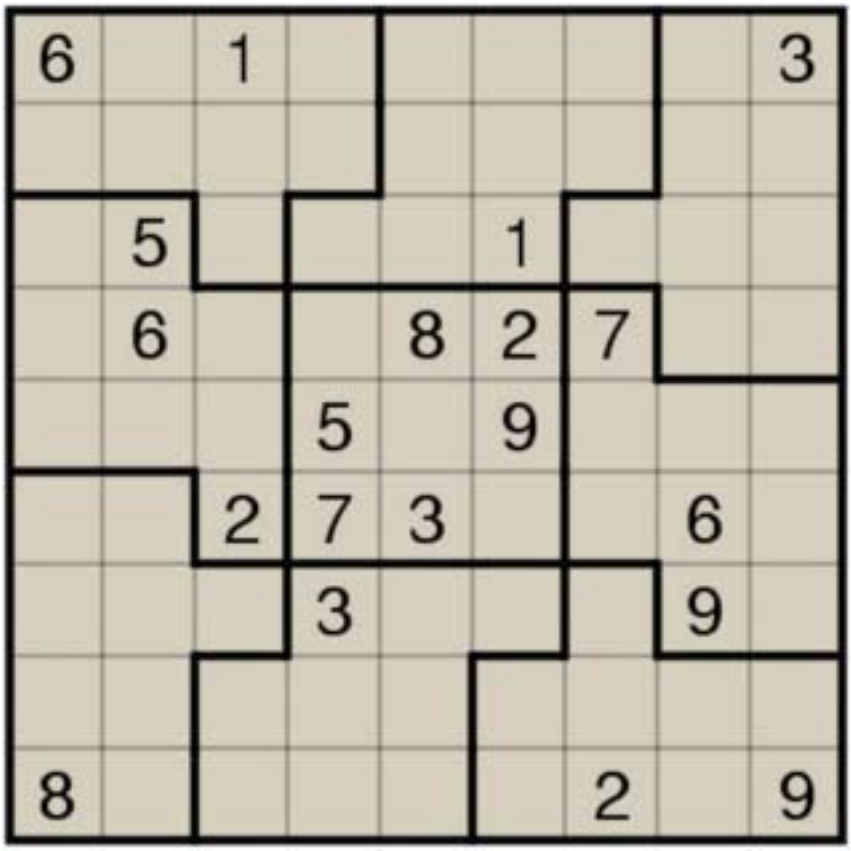
See you in November !

be the contrary. In some cases, the criminal assumes a Robin Hood mentality to the extent that the crime is seen as victimless. For example, Thomas Gawith (New Zealand) extracted $13,700 from six bank accounts and diverted these funds to the financially needy. In another incident, an anonymous hacker changed software programs used by an online casino for the duration of two hours. The winnings totalled $1.9m and the casino had little choice but to pay out the winnings as it would have been impossible to determine who genuinely won during the time period.

But it does not mean that computer crime is a non violent crime. On the contrary, it can cause stress and trauma as a result of financial losses. In more extreme cases, technology facilitates and opens more opportunities for far more serious crimes such as paedophilia where children are groomed inside internet chat rooms.

Computer crime can provide new opportunities for criminals to overcome any feelings of guilt. Through the use of technology, the offender is even further removed from the victim and it becomes easier for offenders to negate feelings of responsibility through the construction of excuses, for example, 'everybody does it', 'no harm done' or 'they deserve it'. The offender is in a far better position to deindividualise, dehumanise and depersonalise potential victims.

Fundamentally computer crime is highly criminal and it is in everybody's interest to raise the awareness of how it can affect individuals and social groups. In the workplace, management carries the responsibility for implementing workable security strategies. Key to this success is the development of a security conscious workforce. This needs to go far beyond the acknowledgement and signing of computer use policies and working procedures but requires a more people focused approach that educates and advises on how to be aware of and react to potential security risks. Findings from psychological research on computer crime, and other areas such as social psychology, enable management to adopt a more holistic approach to security strategies.



Summer Seminar 2007

Thursday 28 June 2007 BAT, Globe House

Hosts BAT again made the Chapter very welcome for this Summer's seminar.

Dr Paul Dorey of BP (and Chair of the Institute of Information Security Professionals), spoke on the issue of convergence and how his company had tackled the issue surrounding it.

Grant Thornton Forensic IT Consultant Simone Zimmermann, (currently seconded to The Serious Fraud Office), addressed both the subject of electronic evidence and on psychological aspects of computer fraud.

We were also addressed by a representative of SOCA (Serious and Organised Crime Agency), who despite starting his presentation by telling us he could not tell us his background or what SOCA actually does, provided some useful insight into this new Agency.

The day's Sponsors were CONTINUITY2 were represented by ASIS member Charlie Maclean-Bristol.

We once again had a good crop of exhibitors: ARC TRAINING INTERNATIONAL, BELL SECURITY LTD (TRACCESS DIVISION), CONTINUITY2 LTD, ESOTERIC LTD ? HONEYWELL SECURITY UK LTD, NEDAP GREAT BRITAIN LTD and UNIVERSAL SECURITY SYSTEMS LTD.

I know we say this every time, but without the support of hosts companies , sponsors and exhibitors, we would not be able to organise such memorable seminars and attract so many attendees.

A Diary for Certification

Tim Hodges MBA PSP is Managing Director of New Pool Solutions Ltd, an independent security consultancy specialising in the technical aspects of physical security.

In June 2005 I decided to sign on for the PSP study program offered by Arc Training and after extensive email interrogation by ASIS was finally given approval to take the exam

Peter Horsburgh CPP, PSP was in charge of the distance learning, which was based on set monthly projects that provided the deadlines for agonising over issues such as which lock was better than another.

The formal study programme started in August and the four tasks were completed by October. Useful feedback was given after each project.

The reference material included the U.S. Army Physical Security Field Manual, which was initially tedious to follow due to the extensive use of US acronyms, was eventually understood.

At the end of October there was a five-day intensive Physical Security Management tutoring session at the Holiday Inn, Reading, for those on the Arc training. (I am the good-looking one on the front row far right).

Those attending were from financial services, close protection, consulting and manufacturing and the conclusion from one ex special forces person was interesting in that whatever physical protection was put in place there would always be a way round it by the committed criminal or terrorist. The only variable would be the time it took.

The exam itself was taken on the Saturday morning following the 5-day review and took some two hours. ASIS rules state that you are not allowed to disclose any of the questions but it is worth noting that it may seem simple to pick out one correct answer from a choice of four but you really do need to know the subject because of the apparently faultless logic stated by the wrong answers.

Out of the eleven who were on the 2005 ARC course eight have passed and been awarded their PSP certification.

The broader view that the certification study enabled me to have has certainly been helpful in my work as a security consultant specialising in the technical aspects.

Cost involved apart from my time was in the region of £1000. I did not stay as a resident at the Holiday Inn but would in retrospect recommend the residential option because of the useful opportunities for the informal exchange of information.

The suggestion of taking the CPP certification in 2006 was turned down due to the brain rebelling after undertaking sufficient early morning studying sessions over a 4-month period.

However after attending a certification awards dinner in March 2007 during which Bruce George MP spoke strongly in favour of qualified professionals rather than amateurs in security, I decided to see if I was eligible to take the CPP certification.

Lively e-mails followed between Ada of ASIS US and myself with penetrating questions covering my background and responsibilities. Ada finally conceded that I was sufficiently pure and secure and had enjoyed a sufficiently high level of responsible charge to take the exam.

Janet Ward of Arc was most helpful in organising reference material and again I took up their study program headed up this time by Barry Walker and the first session was held at The Swan at Streatley on Thames in June. The venue was superb in both setting and service for the 25 or so people attending. (Amazed at the capacity Janet has for red wine and yet she manages to stay so slim).

Barry and his colleagues ran through tests for the Friday afternoon, all day Saturday and the Sunday morning. The results really made you realise just how much further study would be required to meet the required level in the exam. Barry certainly deserves full credit for organising this, the first of two long weekends (which he does incidentally on a voluntary basis.)

The guidance given was that a minimum of one hour per day from June to October would be required to absorb the reference materials. This is difficult to slot in every day but an early morning start seems to provide the best solution for me.

The reference material is more broadly based than the PSP and the Protection of Assets Manual in four volumes really requires its own bookcase.

Cost involved for the CPP and the two residential study sessions is about £1900.

The study session is challenging but also enjoyable because so much is relevant to what I am doing now and where I want to be in a year's time.

Contact me at tim@new-pool.demon.co.uk if you have any questions or points you want to make which I will then raise with the Professional Development Committee.

This year's crop of PSP Candidates

The Convergence of Physical and IT Security Management

The convergence of physical and IT security management is an area of growing interest for security professionals and is also proving to be an effective way of developing a sound business security strategy. It certainly has a great appeal to company directors who are looking at mitigating all forms of security risk in a unified policy. However, William Crowell, former deputy director of the National Security Agency in the U.S. indicates, in a book published this year, that the current situation is far from integrated.

"Today commercial industry is too slow to embrace security convergence in a significant way and we are less prepared than we should be. A lack of technology is not the issue in solving the problem. A collaboration of effort around the concept of establishing a "mutual defence" is required."

(Contos, 2007: xxiv)

It is this issue of a unified approach to security management which is significant and something which Dr. Paul Dorey, BP CISO, emphasized when he addressed the ASIS UK Summer seminar in June, this year. He explained how BP had recently united the Physical and IT security teams together with the Business continuity and recovery sections to form a new Enterprise Security and Compliance department. He spoke of the convergence of technologies but stressed that the success of the merger rested on the integration of the management teams themselves.

In 2004 I worked on a project with BP and nine other global organisations which involved interviewing senior Corporate and IT security leaders about the case for integration. The results of this interview process and an analysis of the available literature led to a series of eight recommendations for future security policy. They formed the basis of my Master's thesis. I submit them, together with relevant quotations from Dave Tyson's new book, "Security Convergence", to the chapter for further consideration. It has become clear that as security professionals it is now crucial to begin or further our collaboration with those in the IT security realm. The Deloitte Global Security Survey of Financial Institutions in 2006 found that relatively few companies are working at convergence (24%) but nevertheless concluded,

"As information security and the role of the CISO continue to evolve in terms of scope of responsibility and value, and as formal risk management efforts become more integrated and cross functional, it will likely become increasingly clear that the logical and physical areas of the organization can contribute more value together than apart."

(www.deloitte.com)

It is recognised that the formation of a single security department would take some time to achieve and would require the authority and support of the board of directors. The following recommendations could form the foundations of such a process.

1. A Holistic View of Security

First, the board of directors and the heads of physical and IT security need to adopt a comprehensive and holistic view of corporate security which sees it as a 'broad strategic activity' that includes all areas of security risk. At this point the business' security needs should be assessed and appropriate solutions considered. These will include physical and digital security counter measures. It is particularly important that the company's culture and vision is understood and a meaningful policy written and endorsed by senior management. This will give the security function the necessary authority to follow through on its recommendations. Dave Tyson has found, in his experience as Senior Manager, IT and Physical security for the City of Vancouver, that a comprehensive security policy 'meets all the needs of the business requirement, considers all risks for the assets, and reduces the stakeholder time (by up to 50%) necessary to evaluate the policy viability and appropriateness' (Tyson, 2007:108).

2. Co-operation on Shared Areas of Security Risk

Second, the two teams should be encouraged to communicate and co-operate more on shared areas of security risk. They should be allowed to state their views and concerns without feeling that the other side will exploit any apparent weakness. The whole point of unity is to gain from each other's expertise and enjoy mutual respect. This should strengthen the relationship between them. Dave Tyson sites the field of investigation as an example,

"Now that we see the volume of personal information stored in electronic form in our organizations increasing on an exponential scale along with the interconnected nature of attacks, it is often difficult to say whether an investigation should be handled solely by IT or Physical security. The threats have converged, and this leads us to the immutable fact that, in order to properly respond to investigations of cyber crime and crimes against people and their information, our investigation

techniques are going to have to converge as well."

(ibid. p 82)

3. The Formation of a Single Security Function.

Third, the sections should be united into one function and a Chief Security Officer appointed to lead the new department. This person could either be a physical or IT security specialist providing he or she has the full support of both groups and the confidence of the board of directors that all aspects of security will now be more effectively handled. Alternatively some companies may prefer that the new team is co-led by the CSO and the CISO.

Historically the two functions have operated independently and rarely worked together. This led to the formation of security silos and the widening of the gap between them. Some of this is probably due to the fact that most IT security specialists work in isolation from the physical security team and as a part of the IT department. The Deloitte survey indicates that there are other factors,

"This approach is due, in part, to the fact that IT security has been primarily viewed as an IT issue and that physical or corporate security has been concerned mostly with the process of keeping the "bad guys" out. Another factor in this approach has been the wide disparity between the business and IT functions in relation to competencies, compensation, inter-organizational perception and reporting structures".

If the company culture does not favour such a strategy it may be possible to establish a single reporting chain with the Chief Risk Officer or another board member as the executive who has responsibility for both areas of security. This would still be a far more unified approach than the current situation.

James Willison is a Security Convergence specialist who joined ASIS in April 2003 His focus now is to help IT and Physical security teams work together in unity to ensure effective business security. James would be pleased to hear from those who wish to work at furthering this endeavour. He can be contacted at pat.will@btopenworld.com

4. Introduction of a Smart Card Access Control System (SCACS).

Fourth, now working as a single function the security department should introduce a smart card system which aims to record accurate audit trails of personnel in physical and digital locations. This is a particularly significant way in which an organization can begin to see the benefits of convergence but it may not be appropriate for all those attempting integration to put this in place. If implemented the team will need to establish a central alarm monitoring system which enables administrators to respond to unauthorised access in real time so that vulnerable servers and files can be protected.

5. CSO to Advise Other Business Units of the Advantages of the SCACS.

Fifth, the Chief Security Officer should contact the leaders of all other business group functions to advise them of the advantages of the new smart card system and in particular show how productivity is increased following its implementation. He or she would refer to the confidence personnel can have that only those authorised to do so can access sensitive data. It could also be shown that since passwords are securely stored on the card less time will be lost from being denied access to the network and obtaining password resets. This is a significant return on investment which is worth stressing.

6. The Board of Directors to be Informed of All Major Security Incidents.

Sixth, the board of directors should be kept informed of all major security incidents which are recorded by the new department. In this respect they will be able to comply with the legislation outlined in the Data Protection Act 1998 and the Sarbanes Oxley Act 2002. The security group will be in an excellent position to conduct investigations and the reports will be accurate enough to meet the law's requirements.

7. Establish a Common Line of Reporting.

Seventh, a common line of reporting should be established. This will enable the experts from both fields to examine security vulnerabilities together and ensure all incidents receive the necessary attention they deserve. It will promote respect for those who succeed in identifying new areas of risk and specialists who provide solutions to the problems it raises. This is important as it will also ensure good levels of morale in the new department. This will have a vital impact on the relationship with senior management and the board for as Dave Tyson explains,

"Instead of reviewing two security metrics reports or having presentations by two security departments and then having to integrate the risks of both presentations, leaders can now get one report document or

presentation that provides a snapshot of all security risks across the organization" (Tyson, 2007: 18).

8. Recommend the Implementation of a Common IP Network.

Finally, the CSO should recommend to the board of directors the implementation of an identity management solution (such as those available from IBM or CISCO) which includes operating the corporate digital infrastructure on a common IP network. This will allow IP video, alarms, voice and data to be streamed through the network and strengthen the unity of the security function. It will provide greater efficiency and accuracy in responding to incidents. It will of course be necessary to have a back up system in place. Dave Tyson believes that the ability of an organization to adopt such a policy will set it apart from its rivals and so increase its competitive edge.

"The ability to integrate the traditional physical security systems (such as access control and CCTV) into the company data network allows the organization to take advantage of economies of scale, and to leverage the existing infrastructure to deliver many benefits to the organization. These benefits can include utilizing the existing transmission medium (such as the corporate data network) which reduces costs and increases reliability". (ibid. p 54)

It is perhaps only the converged security team which will actually have sufficient status with the board of directors to carry out effective security policies with their support and financial backing. The importance of the security function will be elevated and enhanced by this unity and both areas will benefit as senior management perceives the group's strategic value.

The ASIS UK chapter is at a place now where it can look to working with the members of the AESRM here in the UK and follow the lead being taken by ASIS International's board of directors.

James Willison was awarded an MA by Loughborough University in July 2005 for his work on "The case for the integration of corporate physical and IT security". He can be contacted at pat.will@btopenworld.com.

REFERENCES
Contos, B., T (2007) 'Physical and Logical Security Convergence.' Elsevier Inc.
Deloitte (2006) '2006 Global Security Survey' in www.deloitte.com.
Tyson, D (2007) 'Security Convergence: Managing Enterprise Risk.' Elsevier Inc.

Oops!!!

Thief steals cut-out cop

A thief has stolen a life-size cardboard cut-out of a policeman that was intended to deter shoplifters at a supermarket.

Police say the cardboard cut-out replica of PC Bob Molloy had been doing a great job of deterring shoplifters in Long Eaton, Derbyshire.

The cheeky thief paid for his groceries at the Co-op store and then waltzed off with the life-size PC Molloy tucked under his arm.

But Derbyshire Police may yet have the last laugh - as the theft was captured by CCTV cameras and they are confident of making an arrest.

Thefts had fallen from 36 per month to just one since PC Molloy's 2D presence was introduced two years ago, and police believe the theft may be an act of revenge.

The cut-out, which cost £100 to produce, has been rotated between stores across Belper and Long Eaton.

It shows PC Molloy in full uniform and with arms folded. It looks so life-like that some shoppers have even tried to engage the cardboard copper in conversation.

Insp Andy Picken said: "We were using the cut-out as a way of engaging more with the local community, so it is a bit disappointing.

"We are pursuing lines of inquiry and hope to have some good news soon."

Sentry caught off guard

One of the Queen's guards is in trouble after he was caught on camera making a rude gesture outside Buckingham Palace.

His hand signal was videoed by an American sightseer and posted on YouTube, reports The Sun.

The sentry is seen moving his clenched fist up and down, apparently in a joke insult to a comrade.

Palace guards are strictly forbidden from communicating with anybody while on duty.

The guard is believed to be from Nijmegen Company, a ceremonial unit of the 1st Battalion the Grenadier Guards

Escaped convict found at police party

An escaped convict has been recaptured in Taiwan - at a barbecue party organised at the local police station.

Police in Xinzhu city invited residents to celebrate the Moon Festival with them.

But officers could not believe their eyes when they saw an escaped drug dealer called Chen, who had just been listed as one of the city's most wanted criminals, at the party.

Police officer Cai Zhengtong, who was in charge of the barbecue, said: "I saw a man dressed in an eye-catching yellow windbreaker enter the place and sit in the corner.

"He was enjoying the barbecue with the others. I really couldn't believe my eyes, since the man was just the criminal we were seeking."

Police at the party quickly arrested Chen. He told officers he thought it would have been the last place police would have thought of looking for him.

Chapter 208 welcomes 100+ new members

Jorge Albornoz	CPP
John Ansell	Secur-Ed.com Ltd
Samson Ashu	
Martin Barnett	
Stephen Batt	Schering-Plough Corporation
John Baty	
Hal Bauer	Global Implementation Group
MartynBelfield	Wyeth Pharmaceuticals
Thomas Blair	Xerox Europe
CarlBlinston	STC UK Ltd
Vaughan Bramley	
Clinton Brannigan	Red24
Andrew Broadbent	Bank of America
Steve Brooking	
Simon Browne	
Isabelle Cailler	Trigon Ltd
Peter Chegwin	Advance Security UK Limited
Simon Christian	Air Products plc
Tom Craven	Momentum Security
Christopher Cray	
William Dakin	Bank of England
Kevin Davies	
Steve Davies-Morris	
Roger Dawkins	GlaxoSmithKline
William Dewar	
Paul Dimmock	
Piers Dixon	Boots plc
John Donlon	ACPO
Frank Dunsmore	
Trevor Easley	Anubis Associates Limited
Adrian Fielding	
Keith Fleming	Wilson James Limited
Kathryn Forsyth	Pfizer
Neil Gammon	British Sky Broadcasting
Ian Gascoigne	OC & C Strategy Consultants
James Gemmell	Security Systems Dolphin Est
James Gibson	
John Gill	American Embassy London
Keith Godfrey	ConvaTec
Ron Golan	ICTS UK Ltd
Ian Goodman	
Steven Goodwin	
Dawn Green	Thames Water Utilities Ltd
Kevin Green	BurrillGreen
James Greenall	Steele Foundation
Aidan Hales	Anadarko Algeria Corp LLC
Calu Halliday	Diageo
Gez Hart	Buro Happold
Andrew Hayward	
Richard Hewetson	
Frederick Hinds	
Robin Holmwood	Buro Happold Limited
Alwyn Howie	
Phillip Huggins	
William Hunt	Threat Resolution Ltd
Dean Husselbury	
Mark Ibbotson	Asda Stores Ltd
Andrew Irlam	
Stephen Jackman	Barclays Capital
John Jacovou	Cisco Systems
Keith Johnson	
Gareth Jones	Marriott Hotels Ltd
Brian Kelly	Bold Communications Ltd
Simon Lambert	Lambert & Associates
Chas Lawrence	
Richard Leach	Hybrid Solutions
Adam Lee	
Paul Macarthur	Global World Services
Richard Mallett	VSG
Michael Marmol	
John Marriott	Noble Drilling Nigeria Ltd
Guy Mathias	HLS Limited
Adrian Maxwell	St John's Chambers
Athalie Mayo	
Richard Moore	
John Murphy	
Charles Napier	
Claudia Natanson	Diageo
John Newton	
Lee Niblett	Red24
Ifeanyi Okoh	
Aaron Olsen	Reuters Group plc
Paul Parker	
Richard Parris	Wachovia Corp
David Partridge	
Daven Patel	
Anthony Puozah	Anglogold Ashanti
Mark Purnell	Armorgroup Services Ltd
Jorge Rego	CPP
David Reid	TNT Express
Michael Rosser	Symanatec
Alexander Roth	Kuehne & Nagel Ltd
Brandt Rousseaux	BHP Billiton
Olanrewaju Saheed	
Shane Sargeant	Resilience Teams Limited
Ian Saunders	
Martin Sayer	Asda Wal Mart
Gary Simpson	The Corps
Craig Slater	Control Risks Group
Anthony Smillie	G4S plc
Kevin Smith	PricewaterhouseCoopers
Roy Smith	Chubb Security Personnel
Richard Stocks	The Babraham Institute
Charles Stuart	Hart Security UK Ltd
David Thomas	Eyefortransport
Frank Thomson	CitySync
David Tomlinson	AWE plc
Dave Unitt	
Jacquie Wathen	
Mark Webster	TPS Consult
Jason Whinfield Curl	ANC Facilities Management Ltd
Mark Williams	Pelco
Tim Wolters	
Gary Wright	VSG
Leigh Young	

Autumn Seminar 2007

Hostage taking was the subject of the Autumn Seminar this year. The seminar, organised by Mike Alexander and Mick Edgell and hosted at Barings office in Bishopsgate, had speakers coming at the issue from three different angles.

Norman Russell of Barclays gave us the view from a business standpoint and Mike Penrose of International SOS related his harrowing experience of being taken hostage. The third view was from a member of HM Forces who gave us a in sight into the Military respnse to hostage taking.

Chapter business was handled by Mike Hurst and David Creswell

updated the 80+ attendees on the changes to the CPP examination process.

Thanks to Dave Matthews and Barings, long time sponsor Peter Jones of Reliance Hi-Tech and exhibitors, ARC Training, Bell Security, Esoteric and Universal Security Systems

SRVP Report


Peter French

The quality of ASIS meetings around the world distinguishes our membership in the high regard they hold their profession. ASIS Europe's growth is now spawning new Chapters in Israel and Croatia with local members now getting ready to petition in Romania and Hungary for Chapter representation.

We ALSO have in prospect established countries beginning to spawn Chapters outside their country capitals, as membership grows throughout the professional levels. In the UK we have the beginnings of a successful regional breakfast programme which might enthuse our UK regions to establish their own Chapters.

A first in Europe will be the 208's plans to hold two examination dates in 2008 due to the number of persons enquiring about the CPP and PSP. This is in no small way due to the continued high profile endorsement 208 has for both qualifications. By 2008 full ISO recognition for ASIS will be obtained and further developments are expected to lead a major expansion of our ASIS education programmes.

Plans are well advanced for the ASIS Barcelona meeting 13th – 16th April 2008. The synopsis of presentations registered to date cover a broad depth of topics that are highly rated by their referees.

Sponsorship is well advanced and is comfortably ahead of our most successful European show held last year in Berlin.

Volunteers are a most valuable asset and I think it is timely to recognise the efforts of the European Standards Sub-Committee who have been instrumental in gaining ASIS recognition as the premier security association to which worldwide bodies can technically consult with.

We can feel justly proud that we are assisting the Standards and Guidelines Commission in identifying areas where security professionals should be represented.

As a worldwide Association we continue to lead in the areas of professional development which continues to be at the heart of our Society's growth. The appointment of Kaj Moller on to the ASIS Board of Directors provided international members with increasing representation in proportion with our global growth.

Many thanks for all your efforts in developing the ASIS brand.

ASIS Diary

25 Oct - Breakfast Briefing in Manchester

25 Oct - Women in Security - Prudential Assurance - Central London

Breakfast Workshop. Come to meet and talk through issues with other women in the Security world.

1st Nov - Breakfast Briefing in Bristol

15 Nov Pre-Seminar Dinner

16 Nov. AGM and Seminar, Reuters, London

28–30 Nov Chief Security Officer summit - Amsterdam

29 Nov - The CCTV and Electronics Workshop

A day for NON TECHIES @ Tavcom Training, Hampshire

This will be a very useful development day for gaining a better understanding of how electronic systems work and what you can get out of them. Come a see how they work, play with the kit, ask the questions you never liked to ask. Numbers will be very limited so once the invitations go out move fast, put it in your diary NOW

2008

29–31 Jan IIPSEC

11–13 Feb Asia-Pacific Regional Conference, Singapore

17 Mar - Pre Seminar Dinner

18 Mar - Spring Seminar - British Library

13–16 Apr ASIS International 7th European Security, Barcelona, Spain

May Emerging Trends in Security, Las Vegas, Nevada

May T.B.A. Golf Day and Dinner Dance

12–15 May IFSEC

15–17 Sep ASIS International Seminar 2008

Derek and Chris reach Blackpool Tower

Along with 39 others Chris and Derek reached their objective of The Eiffel Tower on schedule. There, they were met by John Inverdale and Austin Healey of the BBC and some champagne.

It was a great three days in brilliant sun, with the group suffering 3 crashes (not serious just grazed knees and cheeks) and 24 punctures, of which one was Webster's, they covered 285 km at an average speed of 12.8 km/p/h. Our members were the oldest men but they did have a 75 year old woman with them!!

Although the English rugby was rubbish, they were both still pleased to have undertaken the ride, but glad they hadn't swam the channel as well.

Between them Chris and Derek have raised £5.5k for 'Scope' and the group total was in excess of £65k.

There are now two bikes, each having had one careful owner only, chained to the South East corner of the Tower, free to anyone that wants to collect them.

Chris and Derek are very grateful to all of those who supported them with sponsorship.

Its not too late if you want to now they have completed it.

www.justgiving.com/derekandchris