ASIS Newsletter of the Year 2003, Honourable Mention 2006

The ASIS International 6th European Security Conference in Berlin – A UK Perspective.

Barrie Millett Chapter 208 Vice Chairman

Of all the ASIS International European Security Conferences I have attended this one stands high on my personal success level. Some 500 delegates attended it from not just Europe but from countries across the Globe giving it a truly international edge. Not only was the delegate list multicultural it also had a very broad and diverse professional nature, a varied spectrum throughout the educational sessions and some great exhibitors. This combination I believe was the main factor that made the 6th European Security Conference in Berlin a success for everyone who had the opportunity to attend.

It was also heart-warming to see a strong UK presence at the conference with approximately 90 UK delegates in attendance. As always the conference provided the opportunity to catch up with old friends and acquaintances and also talk to fellow security professionals from across the Globe. Being able to network with so many security professionals, often facing the same challenges as you in managing risks can often put a different spin on a particular challenge you may be facing.

Events started Sunday the 25th March with an ASIS International certification session with Barry Walker CPP. Barry conducted a two and half hour session on the benefits of certification, providing delegates with a valuable insight in to the certification process. This session was a first for the European Security Conference and was attended by a variety of members intending to partake in the certification program.

The calm before the storm......

All exhibitors also had an early start to ensure that the stands were fully in place prior to the SRVP welcome reception. There was a very complementary mix of exhibits, which were located in the coffee break areas providing a great opportunity for delegates to investigate new technologies and services and also catch up with some well-known suppliers.

SRVP Welcome Reception

As always the SRVP Reception was well attended by a variety of delegates, meeting up with old friends and making new ones. This personifies one of the many benefits of membership of ASIS International, networking with colleagues from diverse environments, sharing experiences, generally catching up with issues affecting different people and most of all enjoying the company of people who are passionate about the security profession in a social environment.

Educational Program

There was a varied educational program throughout the conference ranging from, Integrating Security into a Company Going Global, Analysing the Role of the Corporate Security Function, Does Security Add Value, Lose Less Sell More, to name but a few. These sessions not only provided the opportunity for speakers to talk about topics they are passionate about but it also provided the springboard to open valuable debate with the delegates attending.

continued on page 3

THE UK CHAPTER
ASIS INTERNATIONAL
Advancing Security Worldwide™

www.asis.org.uk

THE 208 NEWSLETTER

SUMMER 2007

CONTENTS

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@rippere1.plus.com

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

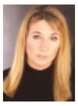
CHAIRMAN'S NOTES

It was good to see Chapter members amongst the 500 attendees in Berlin at the European Conference a number of whom were there as presenters. My thanks go to Barrie for his detailed report. Next year the conference is in Barcelona and it would be great to see a large contingent from 208.

There are two initiatives we are involved in to bring to your attention, the first being discussion with Baroness Henig, the new Chair of the SIA and the other, the outcome of Prof. Martin Gill's Security Research Initiative, which the Chapter together with the SyI, the BSIA, SMT and a number of major organisations sponsored.

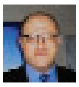
Recently Peter French and I met with Baroness Henig and Robin Dalhberg the D/Chair and had a very interesting session. The Baroness is very keen to meet with and engage with as many people and sectors of the security community as she can, in order that she can really understand the issues and collate views. It was clear from the discussion we had that how multi tasked, diverse and unco-joined our profession is, has already been grasped. I feel positive that the SIA are going to rethink their approach and the Baroness has already invited a cross section of our members to join her at the House of Lords for further talks.

Martin Gill has for the last couple of years being leading research into 'What Industry thinks of Security' and some of you may have seen the launch of his 'Best Value for Business' article in SMT or heard him at IFSEC. They findings are not good reading, for they see security as not adding value to businesses, that security managers were not commercially astute and that really it is ex Military or Police personnel that enter the security profession with limited business skills. Some feedback was also taken from senior members in our profession and they in turn were not very complimentary about our colleagues. Personally I am not surprised with the result, but I am convinced a large number of the derogatory comments are due to misguided perceptions rather than realities, but we have no option but to embrace the issues and together with the SyI, BSIA we will must find a way forward to get security established and in bedded as part of the business management process and we will of course be supporting any initiatives put forward by SyI or the BSIA, and Brian Simms at SMT is also heavily committed to giving whatever assistance and publicity he can. Getting a 'Chartered Security Institute' must be the primary target and to which we will support the SyI. In whatever way we can. We



Helene Carlsson – Joint Editor
After almost 20 years as a security professional in the corporate world (Sweden & UK) Helene thought the time was right to explore the consultancy business. In 2003 she started up her own business and has for the past two years been working with Greymans Ltd as a Security Consultant.

Helene has been a member of ASIS since 1989 and on the ASIS 208 Committee for many years (too many perhaps). She is now looking forward to moving the 208 Newsletter into the 21st century.



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), a member of The Security Institute (MSyI) and has contributed numerous articles to security publications. Mike is Joint Editor of the Newsletter and Webmaster (the new web site is under construction).

Graham Bassett – Advertising and Seminar Exhibitors

Graham has worked in recruitment within the security industry for some 18 years, of which the last 11 were spent as a Director of a London based recruitment firm.

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 travelled and his working career has taken him to various interesting spots around the globe to include a three 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.

will also be looking for opportunities to include speakers on these issues in our forthcoming seminars.

Our June seminar has been 'lovingly arranged by Mike Alexander and Team, with interesting speakers for your delight and I am also very grateful to B.A.T. for their hospitality and with the pre seminar dinner the night before booked I hope we see many of you at both. You will note from the flyers Jude sent out that the cost of guests has been reduced to encourage more of you to bring potential members. The Seminar Team are working hard to identify new quality speakers who can bring differing viewpoints and that in themselves are a draw. Any suggestions????.

Barrie has been working hard on our out of London 'Breakfast Briefings' and we have venues proposed for Birmingham and Bristol, in July and September/Oct respectively. These will be free meetings commencing with coffee and croissants at about 0800 and finishing about 1000. Lynne Davies has also put her hand up to organise a morning meeting in Central London, which will be for ‘Women in Security’, and with Donna Alexander they will be arranging this for September/October. It will again a 'freebie' and will be for women only and Lynne has a specific different idea of how the session will be run.

We also have an offer from Mike Tennant of Tavcom for a 'Hands on' workshop for end users of technical equipment at his Hampshire training centre. This will be a day for 'NON TECHIES', with no mention of wiggle amps and techie gobbledygook. You will be able to ask the question you normally don't like to ask as you can't understand the answer, there will also be plenty of opportunity to play and fiddle with the kit.

We will be restricted on numbers at these events and guests will be allowed, so you are advised to book place swiftly when the flyers come out.

Keep safe. Derek Webster

continued from page 1

Awards

The chapter officers training session proved to be very rewarding for the UK Chapter. At the start of the session a number of awards were presented including the “Chapter Newsletter of the Year Honourable Mention” which I accepted on behalf on the UK Chapter 208 Media Committee - Helene Carlson, Mike Hurst and Graham Basset, who have all worked hard to put together a consistently dynamic Newsletter. Peter French was also presented with an award for all his efforts and leadership as SRVP. Congratulations to you all.

Social Gatherings

The final social gathering of the conference was the Presidents Reception, which was held at the Museum of communication. It was an opportunity to reflect on the previous days and a chance to network in a social environment with new and old friends.

For me and many other people who attended, the ASIS International 6th European Security Conference, it was an immensely successful event and the UK Chapter Committee hope to have the chance to see new and old friends at the 7th European Security Conference to be held next year in Barcelona.

NEWS

208 Appointments

Derek Webster, Chapter Chairman – is pleased to make the following announcements concerning Chapter members.

Emma Shaw, MD of Esoteric Ltd, has been appointed ARVP.

This means that Emma, a great supporter of ASIS and other professional institutes and bodies, will be the liaison point between our Chapter and our RVP Godfried Hendriks. Godfried in turn reports into Peter French, the SRVP for Europe.

Emma, although not a member of the 208 committee, will be able to attend any of the meetings she wishes, and will work to develop relationships with the other European Chapters.

Emma, thank you for taking on this role, good luck, enjoy it and we will support you all we can.

Emma will be doing a short piece for the Newsletter on her role.

David Cresswell MD ARC Training Ltd. has been elected to the Education Sub Committee of the European Advisory Committee.

David, as well as now taking on the lead and reinvigorating our own PDC and the IDG and looking to increase numbers undertaking the CPP and PSP, will have his main focus on organising educational sessions in Europe.

David is a great driver in professional development and I know that he will continue to work tirelessly on raising education standards.

Again David, thanks for taking on these roles and I am sure that all 208 will support you in your efforts.

Chapter 208 Blog
Mike Hurst

Communication with members is vital. As I write the website is being totally redesigned and should be up and running soon. Additionally we have recently started a Chapter 208 Blog which is hoped will complement the Website and Newsletter and prove to be a useful tool. Certainly we are getting a good number of hits on the site.

Can I encourage all members to visit the Blog at http://asisuk.blogspot.com

ASIS Diary Dates 2006/7

2007

27 June	**Pre-Seminar Dinner**
28 June	**Summer Seminar, BAT, London**
September	**T.B.A. Golf Day and Dinner Dance**
19 Sept	**Pre-Seminar Dinner**
20 Sept	**Autumn Seminar, Tate Modern**
24-27 Sept	**53rd ASIS International Seminar, Las Vegas**
15 November	**Pre-Seminar Dinner**
16 November	**AGM and Seminar, Reuters, London**

2008

February 11 – 13	**Asia-Pacific Regional Conference, Singapore**
April 13 – 16	**ASIS International 7th European Security, Barcelona, Spain**
May 2008	**Emerging Trends in Security, Las Vegas, Nevada**

The POWER of Collaboration

Be part of the ASIS Member-Get-a-Member program

About This Program

This Member-Get-A-Member (www.asisonline.org/ReachOut) campaign is really about you. We know that if you are satisfied with your membership in ASIS International, you will encourage other security professionals to join. (After all, it is one of the best professional decisions they can make for their careers.) And we want to reward you for doing that!

This year we have developed a multi-tiered incentive program to reward both individuals and chapters. Awards will be given to individuals who recruit a minimum of 5 members, and to chapters that add at least 15 new members. The campaign runs from January 1, 2007 through December 31, 2007.

Recruiting a Member is Easy!

Recruiting a member is easy when you find yourself interacting with colleagues at meetings, online, on the job, or while networking. Simply tell your colleague(s) how you have benefited from your membership in ASIS and suggest that they visit www.asisonline.org/store/membership.html to learn more about membership and to join.

If they decide to apply for membership, they'll need to put your name and employer (company) or phone number on the membership application line: Person who introduced you to ASIS. If they join, you get the credit. And we keep track of your recruitment activity for you. It's that simple.

Prefer to Refer?

Sometimes, it may be more convenient or more appropriate for you to provide us with contact information for an individual who is a candidate for membership, and we take the next step. Complete the online Referral Form (http://www.asisonline.org/membership/grassrootsCampaign.xml) and submit it to ASIS electronically. ASIS will send the individual(s) information and an application. However, you won't be considered the "recruiter" unless the new member provides your name on the application as the person who introduced him/her to ASIS.

Whether you recruit or refer, you will be contributing to the growth of ASIS International. And you will have the potential to earn some valuable awards, which will be announced at the January 2008 Leadership Meeting.

http://asis.confex.com/asis/2008/cfp.cgi

ASIS International Security Conference: Risks and Opportunities in the Asia-Pacific Regional Conference

February 11 - 13, 2008, Singapore
Submission Deadline: June 30, 2007

ASIS International 7th European Security Conference:
Security - The Essential Corporate Asset
April 13 - 16, 2008
Barcelona, Spain
Submission Deadline: September 30, 2007

2008 Emerging Trends in Security
May 2008
Las Vegas, Nevada
Submission Deadline: Will open Spring 2007
Deadline: October 15, 2007

Peter French

Senior Regional Vice President's Report

The first quarter of 2007 has been busy with our volunteer groups developing a European vision to show demonstrable value to our membership.

The European Advisory Council EAC) met just prior to the Berlin Conference. The EAC constitutes the volunteer leaders from Europe (SRVP, RVPs and ARVPs), representatives from the ASIS Executive and the incumbent President with invited representatives from training organisations and academia. The EAC Chair is Arjo de Jong from the Netherlands.

Priorities this year are education and membership benefits. An Education sub-committee has been established at November EAC meeting under the chairmanship of Joop Verdonk, Director of the Security College BV in Oegstgeest.

The group has planned and will deliver an educational programme on the 21st June in Brussels. Following consultations with the European Commission, this programme will be addressing the issue of Executive Protection. Opportunities for sponsorship are still available.

The EAC also co-ordinated the certification session held on the first day of the Berlin Conference, of which over a 100 participants registered to attend. The theme this year was around the career benefits of certification. Following this success, it has been agreed that we will deliver at the European Conference each year a practical revision programme.

ASIS will provide two educational programmes each year in Europe. Where practical this will be to encourage non-members to participate with probable locations being Slovenia, Croatia, Serbia, Turkey and the Baltics. If you are interested in delivering a module on corporate security, anti-corruption, piracy or counterfeit prevention our Brussels office will be pleased to hear from you.

The Professional Certified Investigator (PCI) Certificate introduced in 2004 has been well received in the relevant North American sector. The Chapters in Europe will be asked to support the development of a European PCI. Our intention will be to create an examination based on European legislation. This will be aimed above the national level. Our aim will be to create a study platform that will identify how national boundaries interact with emerging European legislation and institutions such as Eurojust.

As ASIS members we have a global community of 35,000 security professionals. We need to reach out to our European members, becoming relevant to their professional lives where possible. As part of this membership benefit a feasibility study has been agreed by the EAC on setting up a Public Affairs function at our Brussels office. The required funding will need to be generated by in-region functions such as training courses and the annual conference.

Next year's conference will be in Barcelona, 13th – 16th April 2008. A fantastic, vibrant City, our Spanish hosts will generate a warming welcome as we return to Spain after the 2004 Madrid conference. We hope to attract at least 600 attendees, exceeding our record attendance this year.

Our Assistant Regional Vice Presidents are heading up a cross-Chapters initiative to encourage more joint social and educational sessions. If the ASIS strength is our cross national membership, the ARVPs under the co-chairmanship of Sven Leidel from Hamburg and Bill Enright from Dublin will deliver this initiative.

At the EAC we review the actions and direction of ASIS Europe. We recognise that we are part of a global organisation and that we need to have common aims. As with any growing organisation we seek to establish our relevance in the professional world. Our latest meeting certainly underlined how much work has been completed in the past 12 months and significant developments that we can expect in the next year.

Chapters and their volunteer leaderships' enthusiasm continues to be one of my personal motivations in being one of 20 global SRVPs. I was invited by our Czech Republic Chapter to open a security conference they have sponsored over the last 4 years. Over 300 public and private attendees were at the meeting which maintained a key note session and 4 simultaneous tracks. This has now become the largest private security conference in the country drawing over 20 nationalities. Perhaps members across Europe would be interested in delivering a session or perhaps consider sponsorship, please contact David Nagy, chairman of the local Chapter.

At the annual Washington DC inauguration of the President in January, a group of SRVPs met to discuss areas that affect membership and the SRVP role. Michael Cummings, the Society Treasurer, was in attendance. He listened to a number of concerns that the SRVPs had and the initiatives they wanted to see enacted.

One over-riding theme from our North American members is that they perceive that the Society does not seem to fully reflect the demographics of the membership on the Board of Directors.

This is not an issue regularly taken up by non-American membership, but we should be assured that membership at the senior level do see that we need greater participation from international members in the decision-making processes. To this aim I would ask all ASIS members to actively participate in the elections to the board in the coming months.

Please consider that a huge commitment is given by those that offer themselves for election to fund their visits and freely give their time.

We presently have one Board Director located in Europe. This year another BoD candidate will stand from the region. Please look at the reasons he provides for wishing to be on the Executive Team and see if you can support his application.

If you have any issues you would like me to bring up, then please email me pfrench@ssr-personnel.com or call +44 20 8626 3100.

Does Security Add Value?

Martin Gill

The Security Research Initiative is a three-year programme of study focussing on research to improve understanding of the security sector. It is supported by the UK Chapter (208) of ASIS International, the British Security Industry Association, and The Security Institute, and is sponsored by 13 businesses, namely: Advance Security; Case Security; HSBC; Mitie; Johnson Controls; KPMG; Norbain; OCS-Resolution; Spinnaker International; The Corps; Wilson James and Wyeth Pharmaceuticals.

The first study looked at procurement, and attempted to answer the question so often put by the security sector, 'why do companies say they value quality and then award contracts on price?' According to procurers such a view is to misrepresent them. Some procurers pointed out they do value quality and don't award on price, others questioned whether security really added value at all. They noted that the security sector was associated with providing people to walk around buildings or a few pieces of equipment and technology, and were doubtful there was much of a case for arguing for quality over price, especially when, they argued, security suppliers were only too prepared to undercut rivals.

As a result of this Perpetuity worked with the Certified Institute of Purchasing and Supply (CIPS) to produce a guidance document for procurers that tackled some of the pressing issues for those wanting good security, such as 'what do you get from a good security supplier that you don't get from a bad'. A free copy of the report is downloadable from our website (www.perpetuitygroup.com). Moreover, the findings led the team to consider the issue of whether security adds value in more detail.

Security professionals around the world were interviewed to understand whether they felt they added value and to better understand ways in which security can add value. The results were fairly damning. When senior security personnel were asked what percentage of their peer group met the demands of modern security management the most anyone answered was 25%. Security managers were criticized for being unable to speak the 'language of business' and for not really understanding different elements of the security function. Some security personnel freely admitted that they did not feel they added value. At the two extremes were those who saw security as either 'an inevitable cost on the bottom line' or 'a business enhancing service that contributes to company profits'. A copy of the report is also downloadable from the website (www.perpetuitygroup.com). Clearly the latter is a much better proposition for a group that aims to seek chartered status and to be recognized as a profession.

In order to promote the business enhancing possibilities of security professionals, the findings of the Security Research Initiative have been used to launch the Best Value for Business Campaign. It has two main aims:

- To highlight the role of security sector professionals in enhancing value to the organisations they work for
- To improve the perception of the security sector as a business enhancing service rather than just as a cost on the bottom line.

In the coming year one of the main security magazines, Security Management Today (SMT) will carry a range of articles aiming to highlight just why security is value adding and a range of issues surrounding that proposition. The campaign will look at:

- Education and training, which includes a focus on business rather than just security skills
- Influencing organisations, by promulgating the potential security has to influence different aspects of organisational work. The research found that even where security functions were delivering value they were not telling colleagues.
- Staffing issues, including the need to attract people with business acumen.
- Structures facilitating recognition, this includes the development of a plan to achieve Chartered Status.

The work is only just beginning, but it represents a real chance to influence the future direction of our sector, not least in tackling one of its greatest Achilles Heels, the rather negative views held by many that it is a second rate sector of marginal importance and rarely more than an unwelcome cost. It is not an easy route to take but unquestionably a most important one.

Martin Gill can be contacted at
m.gill@perpetuitygroup.com

Unique Collaboration between Academia and the Security Industry

As of June 2006 The Institute of Economic Research at the School of Economics and Management at Lund University, Sweden has entered a 'Learning Partnership' together with Sweden-based security firms ASSA ABLOY, Axis Communication and Securitas Systems (Bell Security in the UK), referred to as LUSAX. The aim of the partnership is to get a better understanding and develop theories about the mechanisms at work when the IT and networks become integral to the technological platform.

Currently five researchers are involved in the project, stretching until 2010. Associate Professors Thomas Kalling and Konrad Tollmar head the project.

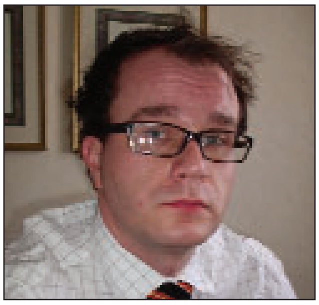
The main motivational drive for the project is the convergence between the IT industry and the security industry, in turn driven by the increased demand for security in general and computing and networked security measures in particular. The technological shift impacts both end-customers and industry constellations, which form the basis of for three research tracks. Doctoral Student Benjamin Weaver heads the day-to-day activities of the track on the industry mechanisms and dynamics at play as a consequence of the industry convergence. Doctoral Student Paul Pierce also has an industry focus, although specialising on understanding the role of partnerships, inter-firm collaboration and alliances on the supply-side. The third student, Markus Lahtinen, studies the impact of technology on the preferences, work and organisation of the security and the IT function(s) of end-users.

The programme has an international outlook, and targeted markets include the United States, United Kingdom, Germany, France and Spain. Thomas Kalling makes the following comment on the project:

Our role is to act as an independent research institution that helps build up a cutting edge centre for academic and scientific knowledge about one of the most interesting sectors of modern business. The project is relevant for the whole industry and the end-users; when technology changes there is a common concern – from manufacturers to end-users – to understand what the causes and effects are. The shifts are highly intriguing from a technological, industrial, and economical perspective, and we are delighted to be part of this vast network of interesting stakeholders.

One of the questions being investigated is how to manage the need for a changed skill set and culture in the industry – moving to becoming 'computer & security engineers'. Not only is the shift visible on the supply-side but also on the end-user side; indicating the increased importance of integrating the "CIO community" into the security purchasing process. Understanding these questions is a common concern for any practitioner in the industry. Consequently, the project participants are keen to interact with professionals in the field to tap their knowledge, experience, and opinion on the dynamics of the industry.

Please visit the LUSAX-webpage for further information:
http://www.lri.lu.se/en/research/learningpartnerships/lusax



**Markus Lahtinen,
Doctoral Student**

**Thomas Kalling,
Associate Professor**

The Necessity of Incident Management

by Neil Hare-Brown, Chief Executive Officer, QCC Information Security Ltd

The Need To Record

Incident management exists as a defined process within the security sector, it is commonly used as a broad term for logging, recording and resolving incidents. However, new ideas and technological development within incident management are regenerating the procedure and imbuing the practice with increased applicable business relevance. New web-enabled technology is enabling not only the recording of incidents, but also the analysis and overall projection of long-term operational risk. For incident management to be truly effective in boosting operational performance, controls needs to be implemented by security professionals as a business decision. Organisations need to implement the technology, which can correlate incidence and security risk. The recording of incidence is based around the principle of pattern recognition – the recording of incidence creates a detailed picture forecasting future threats. The principle of investigation and what can be learned from previous threats is a crucial part of security incident management; ultimately, the key to effective security incident response is preparing for and managing the potential conflicts between investigation and recovery.

Security As A Service

Recent high profile incidents have demonstrated multi-national corporations risk massive financial loss and significant damage to their reputation when critical security incidents occur. Nationwide, Halifax and TKMaxx have all recently suffered huge reputational damage due to security lapses. The Nationwide example of the stolen laptop is particularly pertinent. They were fined £980,000 by the Financial Services Authority for failing to have effective systems and controls to manage their information security risks. According to the watchdog, these failings came to light when a laptop was stolen from a Nationwide employee's house in August 2006. This example illustrates an organisation that was not organised when dealing with a security incident, and did not prepare and test appropriate response action; hence, the financial penalty and damaging loss to reputation.

With increasing regulatory control and ethical scrutiny by the press over poor risk management and security controls implemented by large organisations, there is a clear need for a security incident management system which forms an ideal response function when a breach occurs. It is necessary for such a system to link directly into operational risk management reporting so that actual experience can form quantitative input to more realistic risk modeling. If Nationwide had such a system they would have seen that the risks of poor control over mobile computing and protection of personal data could not be accepted.

Research in incident management converges on the fact that the overall cost of dealing with crisis management is relative to the time-lag in which an incident is reported; essentially, the quicker an incident is recorded the less expense is incurred. A policy of incident management ensures companies are organised when dealing with security incidents; they can prepare and test appropriate response actions or learn the lessons that may help them to better evaluate their safeguard actions. Ultimately, organisations increasingly need to be prepared to respond to an incident before the incident occurs.

Organisations Exposed

Recently investigations were made into the incident management controls in place within a range of medium and large organisations. Within a sample of 99 respondents the research revealed that over a quarter (27.7%) of security experts were not happy that the system they use would suitably protect the confidentiality, integrity and availability of sensitive data. The policy of incident management was highlighted within the survey as being a particularly effective security strategy. 94% of respondents (93 of 99) stated that an effective incident response and management process could reduce the impact of serious incidents. Large majorities agreed that an effective incident response and management process could save an organisation money in protective controls (73%), reduce the number of serious incidents (66%), reduce the number of less serious incidents (58%) and reduce the impact of less serious incidents (82%).

However, only 43.1% of the same sample (31 of 72 respondents to this question), described the response and management process used for dealing with information security incidents as "Formal & Regularly Exercised," with 20.8% (15 of the 72 respondents) describing their processes as "Informal-Ad-Hoc." The lack of organisations having a system for calculating the cost of information security incidents revealed a similar disparity. 77.8% of the 72 respondents did not have a system for calculating the cost of information security incidents; similarly 86% of these respondents said the ability to accurately calculate the cost of information security incidents would definitely add value to their organisation and job function.

The security standard ISO/IEC 27001 offers a set of security controls, which ensures the continuous verification of all elements of the security systems through audits and reviews - a process which must ensure the continuous improvement of all elements of the security system. 36.1%, 26 of the 72 respondents based their Information Security Risk Assessment process on ISO/IEC 27001 or 17799, but less than half of this sample (47.2%) expects to implement an Incident Management process in line with the advice given in key action area 13 of ISO/IEC 17799:2005.

Our research reveals it is increasingly difficult for security experts to justify the cost of protective controls in their organisations, despite the apparent need for more effective architectures and processes to be implemented. It is highly revealing that only 54% of all 99 respondents believed their security incident management system was sufficiently funded.

A Simple Solution

In order to properly plan and prepare an effective response to information security incidents, it is essential that the security incidents organisations are likely to experience be classified by type. There is an overall need for clarity about the terminology of definitions used in information security; ambiguity in the classification of incidence can potentially cripple what is required to be a very exact process. It is equally important to be able to recognise fundamental security risk. Incidents are rarely high tech, they are usually the result of human misuse and typically non-malicious. The threats of cyber-terrorism and malicious hacking are undoubtedly very real, but as the Nationwide incident illustrates, the cause of a critical security incident is often more mundane.

An incident management procedure can reduce the impact and assist in preparing, planning and minimising impact. It is a strange trend within multi-national corporations that they invest hugely in business risk, but don't concentrate on the potential operational risk prevalent in computer misuse. Operational risk analysis is often based on highly qualified results of questioning various personnel about their perception of threat and impact. Whilst this is effective to an extent the process can be highly subjective and a more quantified process has tangible, increased benefits.

Conclusion

I have attempted to sketch the reasons why I feel incident response and management is essential policy within the security field. Organisations need to be primed to respond and react to events as they occur. There is, I believe, a genuine need for technology which is crafted with this managerial concern in mind; a software which automatically and accurately calculates the cost of a security incident - an important justification for return on security investment. Accurate recording of security incidents within an organization will over time provide increasingly accurate data on both the likelihood that an incident of a particular type may occur, and also the impact of the particular incident.

Technology, which enables incident data to be immediately cross-correlated with asset-based risk models, can enable real-time intelligence on operational risk experience. This will considerably assist in providing a better quality of risk. Ultimately there is a need for a full report of operational risk, enabling a realization and control of critical assets. This supply of critical data is particularly important in insurance and financial services.

The absolute need to include information security management in organizational policy is paramount. When a company is imbued with this technological faculty, an organisation will be inimitably secure: prepared when dealing with security incidents, and able to set up and test appropriate response actions, whilst learning the lessons that may help them to better evaluate their safeguard actions.

Neil Hare-Brown is Chief Executive Officer, QCC Information Security Ltd.

Spring Seminar

Mike Hurst, Joint Editor

Space is limited in, this, another 16 page edition of, the Chapter 208 Newsletter. I will therefore keep this Seminar report necessarily brief. I will say however that this was another excellent meeting with well informed and interesting speakers held at a really good venue. There was a definite 'buzz amongst the 100 attendees. For those of you who were not able to attend, I look forward to seeing you next time.

Thanks to our hosts the BBC and the seminar sponsors Wilson James. We again had great support from exhibitors ARC Training International, Bell Security (TRACcess Division), Esoteric Ltd, Nedap Great Britain Ltd, Pentagon Protection UK Ltd, and Universal Security Systems Ltd: thank you you to all of them,

A seminar without speakers is, merely a coffee morning, so our sincerest thanks go to the individuals who took the time and effort to share their experiences with us. They were Eddie Halling (BBC), Chief Superintendent Stephen Grange, QPM MA and Inspector Robert Murdie (Police Service of Northern Ireland), Roger Cumming (Centre for the Protection of National Infrastructure) and Commander Jerry Alford and Superintendent Al Thomas (Hertfordshire Constabulary).

Thoughts from the Back Benches

(Former) Chairmen's Notes

After serving the chapter as Chairman for two years, and the dedication and hard work that that entails, many people would think that former 208 Chairmen have done their bit for the Chapter. However your editorial team disagree and feel that the sage-like wisdom of former Chairmen needs an outlet.

PATRICIA KNIGHT

When Mike asked me to reminisce about my time as Chairman, I suspect he thought I would write an emotional piece about how wonderful if was and how I miss it so! Not quite the way I view it. When Bill Wyllie and Geoff Whitfield cajoled me into taking on the Chairmanship, I was dubious to say the least. Bill avoided eye contact when he said that it only took up about a day a week but being a trusting soul, I believed him.

Joking aside, the reality is that being Chairman is much what one makes it. One could sit back and do very little, of course: the Chapter is strong enough to survive without an active Chairman. However, my predecessors were gentleman with profound senses of responsibility and I was not about to let the side down. As the Chapter grew in size and stature, so did the workload, therefore I made a few changes to the structure to ease the burden on all the hard working volunteers on the Committee. Our Chapter is a credit to all the folk who have laboured unsung for so many years. To misquote our much quoted statesman Mr Churchill: "never …….. was so much owed by so many to so few".

By contrast, many of the members are apathetic: they turn up (or not) to seminars and are never heard of in between times. With a membership of around 700, it is extraordinary that the maximum number of attendees at seminars is around 120, and the maximum number attending dinner/dances is around the same.

This situation pervades throughout the industry. There are a small number of people who do everything: they give their time, energy and often funds because they believe that the industry is worth working for. It certainly needs working on. In an industry where security, honesty and integrity ought to be synonymous, it is disturbing how much dishonesty exists. It is even more disturbing to realise that so many people do not know it exists.

If we are apathetic, then nothing will change. How many people do we know who make false claims about their qualifications, exaggerate on their CV's or claim a higher rank than they held in order to impress? How many companies do we know that claim that their systems/equipment can do everything bar fly to the moon or cheat in tenders? How many end users do we know that are dissatisfied with the systems they have been sold and the service they receive because they were not told the truth in the first place?

ASIS, the beleaguered SIA, Skills for Security and the Security Institute all contribute in different ways to addressing these issues. Qualifications, training, validation and mentoring are key factors that can pave the way to a brighter future for our industry. We need to encourage young folk to join by showing them that there is a career path in a profession of which we can all be justly proud. I may be a cynic but I think I shall be long gone before this idyll materialises.

Another issue that elevates me to my soap box is the prolific paper chain that we now have to endure in order to get anything done. It causes chaos and delays and also, stifles creativity. The ironic thing is that this situation was created in the name of efficiency. We are told that if we create procedures and then prove that we are sticking to them, we must be good at what we do. What no-one admits is that if we create procedures and paperwork for the sake of doing so, we cause more problems than we solve. The only people who are happy are those that like to walk around with clip board in hand, feeling important, looking busy but rarely actually achieving anything. Lots of talk, lots of paper and they feel smugly self satisfied that they have done a good job. Not so: just endless delays whilst more paper work is created; more money being made by people teaching you how to create paperwork and the poor end user, as always, is the loser. What is really needed is bucketsful of common sense – a commodity sadly lacking in certain areas of our industry.

Having said all of the above, I do enjoy my work so I shall continue to run my Company, ensure that we give the best possible service to our clients and do my best, along with my loyal and trusted colleagues, to create a profession out of our industry.

BILL WYLLIE

I first learned of ASIS nearly 20 years ago, when, newly-emerged from the Army, I started my first civilian job, as security manager of the national oil company in Bahrain. An Indian national who was the General Manager of a Dubai-based company providing US-manufactured technical security solutions in the Gulf and Sub-continent region asked me if I had heard of ASIS, and discovering that I had not, thrust the application forms (no website then!) in front of me.

That was the start of a membership that has since taken me through 10 years in the corporate security world, 2 years as the MD of someone else's security consultancy, and 7 years as the sole-trading head of my own (not in that order!) In a variety of jobs, I found ASIS membership to have great networking value and so, somewhere in all of that, I failed to duck during a search for a Secretary for Chapter 208. That in turn rolled me into the Vice-chairmanship and, finally, the Chairmanship of the UK Chapter.

So, all those years and 36 countries later, what have I learned about ASIS? Well, it's now called ASIS International, and a clue to that aspect of the Society lay in my very recruitment to it, as I outline above. A Western expatriate working for an Arab employer, I was recruited by an Eastern expatriate working for a US employer in a different Arab state. For me, that is the beauty of the Society - the international scope and size of the membership. The current edition of Dynamics tells me that there is one ASIS International member in La Paz: if I were heading there on business, I would e-mail him in advance to see if we could meet up - past experience tells me that I might well make a new friend and a useful local contact.

But I think that I am right in saying that, for most of us, it is Chapter 208 itself that is dearest to our hearts. The Chapter has long held many fine functions, ranging from seminars to golf days, and from undergraduate briefing days to balls: during my time as Chairman, we also had the great pleasure of hosting the European Conference in London. All Chapter events are successful, all are enjoyable, and all maintain the Chapter's reputation for some of the best security networking around.

The success of the Chapter's programme, of course, rests with the Chapter Committee, the membership of which is ever-changing. Since I ceased to have the time to be involved in the running of the Chapter, it has been tremendous to see how a succession of Chairmen, Committee members and activists have not only continued to maintain the traditional high standards, but also to bring innovation and freshness to the Chapter's life.

The professional security environment in the UK is, as ever, challenging and changing. But it is good to see that Chapter 208 continues to maintain that excellent network of practitioners for which it has long been famous. Yet longer may it continue!

Security Consultancy

By Peter Speight

As the dust begins to settle from the last twelve months or so of licensing security operatives, signs are beginning to appear on the road ahead, which are unsettling to say the least, and not least, the implications of designing training competencies by committee. The Close Protection sector, both in the design of the training scope and qualification and vetting of approved training organisations gives grave cause for concern.

I'll come back to licence training design later, as my principal area of concern is in relation to the wider implications of licensing security consultants and specifically the scope of what may be determined as 'licensable activity'. It's no secret that the launch of this sector has been pushed back to the end of 2007 and this is likely to be an optimistic estimate, which, if my concerns have some credence, is no bad thing.

If we work backwards from a licensed officer deployed on a site we will come to a point where the ground becomes less firm and uncertainty creeps in as to whether we are in licensed territory. Clearly, the role of contract security personnel is a licensable activity, but they didn't appear as if by magic, but, rather, were deployed as a consequence of concerns about the security of a range of assets at risk from a range of threats.

Rarely will security personnel operate in isolation from a range of other, contributing, security issues, be they physical, systems and procedures specific to the site. Equally, these other attributes to the security effort didn't materialise out of thin air but, hopefully, were the product of a well thought out security strategy, which had concluded that a judicious mix of all these options was right for the protection of the site. That having been said, experience tells me that seldom is the mix of security a product of a cohesive strategy, rather it is an ad hoc approach to the installation of electronic systems, manpower, procedures and physical protection but, leaving that aside for the moment, and assuming that a written strategy is in place, we need to know what this was itself the product of.

The strategy document results from the conclusions and recommendations of the Security Audit, which, would have highlighted both the positives and negatives of the current security operation. However, the Audit is practically worthless if it is not itself informed by and following on from the Risk Assessment; the genesis of the whole process. Analysing threats, both external and internal, arising from nature or the efforts of man; identifying assets at risk and the threats they would be vulnerable to; assessing the risks that would flow from a specific threat to a specific asset; establishing probability and consequence and finally prioritising for a range of risk management options – the risk assessment sets the scene for all that follows.

Working back the way we have come, the Security Audit now sets out, in great detail, to establish how the current security manpower, procedures, physical security and electronic systems help, or hinder the management of those identified and prioritised risks. Outlining the above is not intending to teach people to 'suck eggs' rather it is to set the scene to allow the question to be asked which is what part of this extensive, complex and sophisticated process is intended to be, or should be a licensable activity.

One assumes that if a consultant carries out a security audit, particularly as it has security in the title that it is likely to fall within the statutory remit, but I'm very unsure about the activity concerned with the risk assessment. Branching out from the risk assessment into various, specific areas it becomes even more remote and I'm thinking of Crisis and Contingency management. Is it the intention of the SIA to include this work as licensable? If they do I think there will be an uproar from the Business Continuity Management (BCM) consultants for whom Crisis planning is an integral part of their Business Impact Analysis and subsequent planning and if they don't, security consultants are likely to end up with a serious identity crisis where part of a day will be spent carrying out a licensable activity and the other part not.

It gets worse. Proprietary Information security has been a 'football' that is often kicked around within a corporate structure between IT, HR, FM and the Security Department (if one exists) and if one looks at the Information Security standard BS7799 the traditional security issues of manpower procedures, access management, systems and physical protection have an obvious part to play, but will the whole process require a licensed practitioner to conduct it. The potential scope for a consultant's licence is vast and this article has really only scratched the surface. We haven't looked at the technical depth of knowledge a consultant should have, as in the case of, say, CCTV, or should a consultant have a good working knowledge, but be extremely skilled at putting together a comprehensive Operational Requirement (OR) so as to negate the 'box sellers' being able to determine the scope and nature of an installation.

Turning back to the subject of statutory training, this can only happen when National Standards have been established and following that, the Core Competencies developed that all training delivery must cover. My concerns about these flows from the experience of the Close Protection field. Unlike door supervision and security guarding there was no recognised, national training or standards in place prior to the legislation and both standards and training competencies had to be established. In a democratic society this means by committee and in any community with strong-minded individuals, everyone has to 'push' their view.

So, having started out to design a horse the finished product ends up with stripes, a long neck and two humps as did the CP competencies. We have included in the required CP knowledge, licensing and drug legislation and control and restraint for the physical intervention!. When people are taken to task we discover that these inclusions were not because they have a part to play in CP operations, but as the CP license is 'superior' it allows CP operatives to work on doors or in security, thereby needing to know about drug and licensing legislation and twisting someone's arm up their back. We simply cannot have the same imperative to shape training competencies, which are not role related, rather license dictated.

Finally, and still on training delivery there are three further problems and both have arisen from the CP experience. The first is the lack of vetting of the training providers by the three awarding bodies - there are now something like 50 centres approved to deliver the statutory 150 hours of CP training, more than there were before the legislation, with the vast majority having little or no actual CP operational experience. Training manuals were not 'mapped' against the core competencies by two of the awarding bodies in accordance with the rules and thirdly the examination for the CP licence verges on the banal. Experienced operatives are finishing the exam in 15-20 minutes and it has been said that someone taken from the street and given the exam could, with a common sense approach, achieve a pass. All this can't afford to happen with the consultancy licence. If the SIA are guilty of anything it is not policing training delivery and simply being goal oriented to want to process numbers at the sake of quality. They simply want to demonstrate how many people are licensed. I feel we need to be heard this time if arbitrary decisions are foisted on us.

Peter Speight MSc PgD IOSH MIRM MSyI
Director of Security Risk Management
Reliance High-Tech
Peter.Speight@relitech.co.uk
Doctorate Student at Portsmouth University Covering:
Security Risk and Crisis Management

Hear4U

The Company of Security Professionals is recognised as the charitable arm of the security profession. It formed as a Guild in the City of London in 1999. It now has Company status and by the end of this year will be a Worshipful Livery Company standing alongside the likes of the Worshipful Company of Drapers and the other 107 Livery Companies that form the backbone of City life.

The Company has a charitable fund administered by Trustees and the current Master also has a charity for their year in office. This year the Master is John Purnell and his charity is 'Hear4u' which he established and launched in June 2006. His view was and is that the security profession has been generally good to us and he would like the Company to put something back into it.

Sadly illness, injury, stress and other related problems knock on everyone's door at some time. The main objective of Hear4u is to enable individuals from the security profession to return to good health and gainful work as soon as possible. Hear4u is part of the Company of Security professionals Charitable Trust and is administered by a sub- committee of the Trustees supported by an Administer (Ann Freeman) and a medical advisor (Dr Charles Goodson-Wickes)

Hear4u operates at three levels:-

1. Access to web based information – www.hear4u.org.uk
2. A free confidential 24 hour Help Line – 0800 3160201. Qualified staff will provide medical advice and counseling – irrespective of means or circumstances.
3. Access to therapeutic and rehabilitation services in deserving cases, subject to qualification thresholds determined by the Trustees. An application form can be downloaded from the web site or obtained through the Help Line.

The Company of Security Professionals is now extending this full service without charge to ASIS UK members. Please visit www.hear4u.org.uk and see what it offers.

Calls to the 24 x 7 confidential Help Line are paid for by The Company of Security Professionals. In order to ensure that it is not abused members will need to quote ASI 807 followed by their ASIS membership number.

We would like to encourage those in the security sector to make use of this facility. We will be encouraging organisations to fully promote this as a member service. Please feel free to do so.

Qualification is Essential for the Future Credibility of the Profession

ASIS Chapter 208 was delighted to welcome the Right Honourable Bruce George MP to present CPP (Certified Protection Professional) and PSP (Physical Security Professional) certificates to UK recipients at a recent certification celebration dinner in London.

Bruce George MP, apart from being a very prominent international politician, has been a life-long campaigner for UK security industry regulation and holds ASIS International certifications in particularly high regard.

Addressing newly certified professionals as a "corps d'elite", he called out to those managers and consultants in the security industry who continue to operate under the peculiarly British practice of the "competent, but unqualified, amateur" to embrace formal qualifications such as the CPP and PSP. Until formal qualification is the norm, rather than the exception, he warned that we would continue to be viewed by other professions as "semi-professional".

Singling out ASIS International certification holders as a model for the future shape of the profession, essential for the transition from what he referred to as simply the "security industry", he declared as unacceptable a prevailing view that while security officers and supervisors require training, security leaders can somehow rely on their former military or police service credentials, and lamented the fact that the SIA hadn't tackled this issue head on. His remarks struck great resonance amongst the forty Chapter members who attended the dinner.

As well as recognising the achievements of the certificants, two of whom - Jacqueline Walker CPP PSP and Ken Johnston CPP PSP - had now achieved dual certifications, the Chairman thanked those involved in the administration and delivery of the CPP and PSP programmes for their continued commitment to raising standards within the security sector.

An added feature of the evening was a raffle in aid of Comic Relief, which raised £700. Thanks go to all who donated prizes, especially the Rt Hon Bruce George MP, and to ASIS International European Senior RVP Peter French CPP for his company's exceptionally generous gesture.

For details of certification programmes, contact davidcresswell@arc-tc.com

Standards – We need them!!

Roger Bird, Senior Manager, Chief Security Officer, Lloyds TSB Bank Plc.

At some point during our professional working life we have no doubt run up against the dreaded "standard". How often have we then looked to the skies as we try to understand the rationale behind these documents and more importantly how on earth it is to be used – especially as there are times one wonders whether any end user has been involved in its development to assure practical application?

I have certainly felt this frustration. Consequently when attending the 2006 European Security conference in Nice I was one of the first to offer my services to an initiative instigated by Roger Warwick to seek ASIS involvement in the development of standards documents.

What I did not appreciate at the time was the scale of the task before us and the opportunity that was to be presented to us to directly contribute to the development of activities that will impact a far wider international audience.

My original expectation was very much around providing input to ensure that an end user perspective was captured in any new or revised standard.

The type of standard I perceived influencing were specifications such as alarm / CCTV and /or physical criteria. All very much practitioner based activities that would support my argument when seeking internal executive support to deploy effective security (and not go for the cheapest option!).

Furthermore I saw it would provide an opportunity to develop and integrate the views of other ASIS members which could then be collated and fed into the process.

From the initial meeting in Nice and subsequent telephone conferences a quorum of three was established. Roger Warwick who resides in Italy and has led this campaign would seek to influence the Italian Organisation for National Standards (UNI) and provide the focal point for liaison with ASIS International as a whole. Likewise Stephen Payne who is based in Geneva would coordinate activity with the Swiss Association for Standardisation (SNV), whilst I would liaise with BSI to provide the feeds into British standards.

The positive response from these bodies together with CEN and ISO has subsequently identified opportunities for ASIS to provide an international voice and perspective of security professional to national, regional, and international standards development.

Roger Warwick's initiative and progress to date was the subject of a seminar at the 2007 European Security Conference in Berlin. This together with aligned discussions has set into motion exciting changes at ASIS. A global shift is taking place at ASIS, with standards development becoming an international initiative with ASIS guidelines aligned with the standards initiative. ASIS has applied for and received liaison status with the ISO technical committee, ISO/TC 223: Societal Security that will be developing security related standards.

Since the introduction of the ISO 9001 Quality Management System Standard there has been international recognition of the utility of management system standards and approaches. Worldwide organisations both public and private have become aware that in order to maintain resilience, competitiveness and performance they need to engage a system that manage their risks.

To support these objectives two work streams are underway which will provide direction on activities to enable business to understand and address the array of hazards and risks that they face.

One is an international effort in the final stages of development before becoming an ISO / PAS (publicly available specification). The ISO/TC 223's Societal Security: Guidelines for incident preparedness and operational continuity management provides a system for preparing for and responding to disruptive incidents.

The second is the development of the world's first security and operational continuity management system that will allow third party auditing and certification. This latter specification standard will seek to address an all hazards- all risks approach to security, incident preparedness and operational / business continuity using similar systems methodology to the ISO 9001 (quality). ISO 14001 (environment) and OHSAS 18001 (occupational heath and safety) management systems standards; enabling parallel or integrated implementation of security, environmental, health & safety, and quality management system standards.

Specifically the new standard would support business preparation, planning and management in order to: -

- Understand the environment within which the organisation operates, the existence of constraints and threats to the company that could result in significant disruption.
- Determine the parts of the organisation and business that are critical to its short and long term success
- Quantify the impact of threats, risks and vulnerabilities on critical operational(business) functions and processes, and identify the infrastructure and resources required to enable the organisation to continue to operate at an acceptable level

- Documents the key resources, infrastructure, tasks and responsibilities required to support critical operational functions
- Establish processes that ensure the information remains current and relevant to the changing risk and operational environment
- Ensure that relevant employees, customers, suppliers and other stakeholders are aware of their preparedness and continuity arrangements and where appropriate have confidence in their application.

All very much common sense activities but surprisingly few companies appear to have formerly developed, catalogued and regularly update their responses in these areas. Accordingly the potential for undertaking such activity within a structured framework that can be audited and certificated can only elevate the status of a security professional within their respective area of operation.

It should also be reflected that the ASIS executive are fully supportive of this work and have already secured the services of Dr Marc Siegel as Security Management System Consultant. An adjunct professor at San Diego University he initiated the concept and spearheaded the effort to develop the Israel National Standard: Security and Continuity Management Systems and is on the ISO/TC 223 Technical Committee where he was the principal author in the task group that wrote Societal Security: Guidelines for incident preparedness and operational continuity management.

In the UK I have been seconded as ASIS representative on ISO/TC223 British Mirror Committee who will provide input from the UK to ISO/TC223. As this develops I will be seeking input from UK Chapter colleagues to ensure that the views and experiences of end users are captured.

In Europe Roger Warwick together with Stephen Payne will be working with their National bodies and ISO to ensure similar input is collated and provided.

In addition, ASIS will be developing a work space on its web site to facilitate communications for the security standards initiative.

At the same time as the above activity is ongoing the day to day work of BSI and other national standards committees continues. Accordingly input from ASIS members is essential and to this effect volunteers from all ASIS International chapters in all security sectors are requested to sit on national standardisation organisations working parties to provide input to these groups and collate feedback from ASIS Members. Anyone interested in cooperating with any of these organisations should contact me via the ASIS web site or by email at asis.standards@pyramid.it

Similarly anyone who feels they have a contribution to make to the ASIS standards initiative should also contact ASIS standards initiative via the on-line workspace on the ASIS web site

Over the coming months I together with Roger, Stephen and Marc will look to provide updates on progress via the web site, this newsletter, Eurodynamics and national seminars.