The 208 Newsletter

ASIS Newsletter of the Year 2003, Honourable Mention 2006

THE UK CHAPTER ASIS INTERNATIONAL Advancing Security Worldwide™

www.asis.org.uk

THE 208 NEWSLETTER

SPRING 2007

Congratulations!

Chapter 208 Successes

On behalf of Chapter 208 committee and I would like to congratulate the newly qualified CPPs and PSPs on their achievement.

These qualifications are not easily attained and require a great investment of time and effort, but they are well worth it. Apart from the knowledge gained by studying for them, they bring international recognition and respect and should enhance careers – very well done!

We are featuring profiles of some of these individuals in the Newsletter this month and hope to have more in future editions.

Kevin J. Dale, PSP
Bob Martin, CPP
Simon Hales, CPP
Michael A. Pemberton, CPP
Larry T. Handy, CPP
Andrew G. Ralston, PSP
Dan Hooton, CPP
Robert C. Savage, PSP
David J. Hopps, CPP
Andrey O. Shcherbakov, CPP
Ken Johnston, CPP, PSP
Andrew J. Stickley, PSP, CPP
Noah Lane, CPP
Jacqueline M. Walker, PSP, CPP
Lukman A. Longe, CPP
Phillip Wood, CPP

As we thank them, I know they would want to thank Peter Horsburgh (PSP) and Barry Walker and John Julian (CPP) for their invaluable help in running the training programmes along with committee CPP representative David Creswell.

In addition to the above successes, our own Peter French CPP was honoured recently as ASIS International "SRVP of the Year 2006", apparently he did particularly well in the swimsuit round!! On a serious note, Peter has worked extremely hard for ASIS over the years and this is fitting recognition of those efforts.

Also, and I am blushing as I write this, The Chapter 208 Newsletter won an "Honourable Mention" as Newsletter of The Year 2006 in Group 6 (chapters with more than 500 members), tying with the Houston Chapter: there was no outright winner in this category.

The editorial team of Mike Hurst, Helene Carlsson and Graham Bassett, will be happy to accept your praise, pats on backs and offers of free drinks at future ASIS events. I'll just have to save my winner's acceptance speech for next year.

Mike Hurst, Editor

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

Since time in memorial everyone taking on the role of Chair for any organisation or board always opens with the same few words and I shall not deviate from that practice.

Firstly I must say thanks to the membership for intrusting me with this role. I will do my utmost to maintain the standards set by my very illustrious predecessors and will strive to ensure that ASIS UK Chapter delivers its objectives, in order that all the membership feel it is worthwhile. I must also give a big thanks to Peter, Stuart and Patricia for the support and guidance they have given me over the last year. And finally, but by no means least to our committee, without whom nothing would be achieved.

It is only through their devotion of time, energy and enthusiasm in making the UK chapter the success it is, that we all gain. Mike, Helene and Graham must be congratulated on their being honoured for the newsletter: they produce, a really excellent publication. The CPP committee's constant work in promoting the very worthwhile qualification and the results they achieve and congratulations to all those that have just passed their exams. I believe that anyone starting out, or even mid career in the security profession should consider undertaking this or the PSP. This, when conjoined with one of the Master's degrees available gives any security manager as good a proven academic status as any city high flyer. It must make any employer confident that the security profession is as qualified and as important as any other role within a business structure. One of our aims must be to ensure that when an organisation has a need for security input, that there not only is a know source to go to, but also that they have standards to measure against, and that those qualifications are equally valid across the world.

Too many businesses fail to grasp the concept of how security should be encompassed with corporate strategy and business risk. Further, a number have no real respect for or understanding of, the level of security management they require.

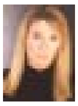
I am a great believer of networking and sharing information across the security community and that we as individuals and all the other associations and institutes must work together for the good of the industry. We must support and work with each other. We have one common goal, but accept with differing purposes and approaches of getting there. I hope that I can contribute to making this happen.

Security is a fast changing environment and ASIS has its part to play in putting the right building blocks in the right places. We can only achieve this with input for the membership. This means ALL taking part in what ever way you can. Writing articles for the newsletter (with rewards for those published), we want to here your views and comments.

We would also like any unusual problems you have encountered during you daily work and how you over came them, guidance you may be able to give on a specific issue that is a current threat or risk. For instance you may find it useful at this time, to review the Cabinet Office, Government Security Units advice on 'Handling Postal IED' so visit:

http://www.cpni.gov.uk/ProtectingYourAssets/PhysicalAttacks/postrooms.aspx .

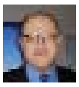
You may be interested and thanks to Chris Brogan, for identifying this web site that concerns investigators being jailed for obtaining information by deception:



Helene Carlsson – Joint Editor

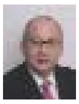
After almost 20 years as a security professional in the corporate world (Sweden & UK) Helene thought the time was right to explore the consultancy business. In 2003 she started up her own business and has for the past two years been working with Greymans Ltd as a Security Consultant.

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) 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 Bassett has worked in recruitment within the Security Industry for some 18 years and is currently a Director with SSR Personnel. He is Chairman of the BSIA Recruitment Code of Ethics and sits on the REC Association of Executive Recruitment Committee (AER) responsible for standards and training.

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.

A keen advocate of Life Training (an alternative to Life Coaching) he is also due to do the "Fire Walk" with Anthony Robbins in October (he must be mad).

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.

http://www.dca.gov.uk/consult/misuse_data/cp0906.htm#responses

We would like people to join the sub groups that help steer the Chapter. You can advise Mike Alexander, Mick Egdell or Donna Alexander of any good speakers you have come across, I mean actually heard, that you think would be of interest and maintain the high standard we have at the Seminars. On that note I will say what an excellent AGM we had. And if you missed it, well don't next time. All the presentations can be found soon on our web site, so those that didn't attend I suggest you visit and see for yourselves the quality and what you missed. So come on, please put a little bit more in if you can please, I assure you it is very rewarding.

I look forward to seeing as many of you as can get to the BBC where another class seminar has been organised. Barry is arranging a couple of meetings up North or the Midlands so watch out for those too.

The final plug is for the ASIS Conference in Berlin in March. We have a number of members, not only attending but also actually speaking. Last year's in Nice was excellent, both the presentations and the company……! So have a look at your diary and get in quick.

My last word on this occasion goes to Peter French, for all his outstanding commitment over a long period and for being a major player in putting the Chapter where it is today. Congratulations Peter, justly deserved, on receiving the Mervyn David award for 2006

Keep safe All

Derek

THE PSP QUALIFICATION – YOUR QUESTIONS ANSWERED

The Physical Security Professional (PSP) certification was first introduced in the UK in 2004. It is intended to provide security practitioners with the ability to demonstrate expertise in conducting physical security surveys, to identify Security vulnerabilities and to perform cost analysis for the selection of integrated physical security measures.

Peter Horsburgh CPP PSP, who developed the PSP Review Programme on behalf of the UK Chapter, answers questions about the success of the programme so far. Questions put to him by David Creswell.

Peter, you designed and put together the PSP review programme for the UK Chapter and you have been running it now for three years. What are your thoughts on its success?

I think that as we have achieved a very high pass rate from the outset - typically 80% of all candidates pass the examination first time - it seems to indicate that this programme works very well. One has to remember, of course, that the success of the programme is based essentially on the hard work put in by the candidates, and all of the candidates so far have worked exceptionally hard and this is reflected in the results.

Why are people drawn to the PSP certification in the first place?

For a long time the profession has lacked a qualification which proves an individual's ability to handle the technical aspects of what we do. The arrival of the PSP has changed this situation. This certification goes into depth into such aspects as risk analysis, selection of protective devices and, just as importantly, ensuring that protective devices are operated and maintained to a high standard.

To what sorts of organisations would this qualification appeal?

The certification covers security for a very wide range of purposes. Certainly, any organisation which uses security hardware, and particularly those which are about to start hardware upgrade programmes or security projects involving fencing, alarm systems, access control systems etc. All of these are particularly relevant to the PSP certification.

When a candidate sets out on the PSP certification route, what sort of commitment must he or she make?

Probably, for a reasonably experienced security manager, in other words, someone who fits the prerequisite examination criteria, 2-3 hours a week of private study for a duration of 6-8 months should suffice. The benefit of this would be increased even further if they were then to attend the formal one-week preparation course which precedes the examination.

What has been the feedback from those who have taken the examination during the past three years?

The feedback has been very positive. The preparation course, in particular, has been very well received by both those with an existing high level of technical knowledge and those whose technical knowledge has been significantly enhanced by their PSP study.

In brief, what do you see as the difference between the CPP and PSP certifications and is there value in existing CPPs going on to take the PSP?

The CPP certification is a broad-based security management qualification. It handles all aspects of management, information security, physical security, emergency planning etc. The PSP, on the other hand, is a certification which drills down into the detail of selecting, procuring and managing physical and technical security systems, both hardware and human based. As far as the benefit of PSP to an existing CPP is concerned, there is absolutely no question that for people who have responsibility for physical security, the PSP gives them a far better in-depth view of the requirements for providing effective physical protection.

You have made reference so far to security managers, but how relevant is the PSP to security consultants?

There is no question that we have a large number of experienced and competent security consultants in this country today. However, the one thing that the PSP does, even for an experienced security consultant, is to demonstrate to their clients that they have proved their ability, through an external and internationally-recognised certification programme, to assess risk, to select protective measures and to ensure that they work properly.

LETTER FROM THE PRESIDENT

With 2006 now in the history books and my term as President of ASIS completed, I am excited about all the Society accomplished last year, anxious to see the work we have begun continue our progress into the future, and glad to have the opportunity and forum to share my thoughts with you on what I view as the overwhelming success of our initiatives on a number of fronts throughout the year.

Educational Programs

ASIS International is the preeminent organization for security professionals, with more than 34,000 members worldwide. Our members are men and women like yourselves who are responsible for the security of their enterprise. These individuals also represent the core and strength of the Society, and as such, ASIS is dedicated to increasing their effectiveness and productivity by developing educational programs and materials that address broad security concerns as well as specific security topics.

Again in 2006, our 20+ classroom programs and conferences around the world provided unparalleled opportunities for professional development and thought leadership through educational sessions and networking events, as well as exhibit components featuring exhibits bustling with companies marketing security products and services and those in the market for these products and services. Program offerings ran the gamut of security issues—from terrorism, crisis management, executive protection, and transportation security, to physical security, asset protection, and more.

The cornerstones of the ASIS educational program are the conferences held each Spring in Europe and each Fall in the U.S., and the 2006 iterations of these conferences were better than ever.

In April, the 5th ASIS International European Security Conference in Nice, France registered record attendance with more than 500 representatives from 47 countries.

The conference featured 32 high-level educational sessions from international security experts on subjects ranging from supply chain and corporate security, to homeland security and risk management. Keynote speakers included Dr Harold Elletson, leader of The New Security Programme, Examining Magistrate Jean-Louis Bruguière (France) - considered one of the foremost terrorism experts in Europe and worldwide, and Dr. Amir Kfir of the Adizes Insitute (Israel) - a leading expert in the field of the executive development.

The conference provided attendees, exhibitors, and conference sponsors alike, the unique opportunity to share experiences and ideas on the key issues facing security professionals while also developing valuable business contacts.

In September, the ASIS International 52nd Annual Seminar and Exhibits drew its largest crowd ever—an unprecedented 22,230 security professionals from around the world and across the profession—for its gathering in San Diego, California.

Already recognized as the world's largest event dedicated to security, ASIS 2006 raised the stakes, featuring insightful—and at times, humorous—keynote addresses on leadership and the state of security in today's post-9/11 world from such luminaries as the Honorable Bob Dole and Former White House Chief of Staff, Andrew H. Card, Jr.

In addition, the education program offered 155 education sessions on topics ranging from homeland security, crisis management, physical and IT/information security to investigations, management, crime/loss prevention and other issues of interest and importance to security practitioners at all levels. The Security Insights Program, "Pandemic: Beyond a Crisis" also brought together a panel of experts to explore the likelihood and potential ramifications of an outbreak of avian flu or other pandemic, in a session that was as riveting as it was informative and timely.

The exhibit floor was equally impressive, boasting a record-breaking 950 exhibiting companies showcasing the latest innovations, technologies and services that are shaping the industry today. In fact, more than 200 new products were introduced or displayed at ASIS 2006.

Both our European Conference and Seminar and Exhibits set new standards in educational sessions and unique networking opportunities in 2006, further developing their reputation as two of the industry's most trusted resources for the exchange of ideas, information and experiences.

Certification

Certifications from ASIS International serve an important role in the security profession by providing evidence that an individual has met professional competency standards and mastered a fundamental body of knowledge. The Certified Protection Professional (CPP), Professional Certified Investigator (PCI), and Physical Security Professional (PSP) credentials administered by the Society which were already recognized as among the best in the security profession received an extra boost in July when the ASIS was awarded a coveted "Designation" for its certification program under the Support Anti-terrorism by Fostering Effective Technology Act of 2002 (the SAFETY Act) from the U.S. Department of Homeland Security.

Guidelines

ASIS guidelines play an important role in helping the private sector secure its business and critical infrastructure—whether from natural disaster, accidents or planned actions.

The Society published one final and one draft guideline this past year, both aimed at helping businesses protect their two most valuable assets, their employees and their information.

The Preemployment Background Screening Guideline. published in its final version, is designed to help U.S. employers understand and implement the fundamental concepts, methodologies and related legal issues associated with preemployment background screening of job applicants.

The premise for the guideline is that hiring a new employee is an important responsibility for any organization. Employers understand the dual benefits of hiring the best people and providing a safe and secure workplace, both physically and financially, for their employees, customers, shareholders and the community in which they operate. A key factor is to know as much as you can about the people you want to hire, and to know that before hiring them.

With useful information concerning the value of preemployment background screening, the importance of the application form, vital legal issues and considerations and the use of credit reporting agencies in background screening, the Preemployment Background Screening Guideline should serve as an educational and practical tool that organizations can use as a resource in understanding the reasons for such preemployment background screening and developing policies and procedures that will enhance their hiring policy.

The Information Asset Protection Draft Guideline seeks to help organizations develop and implement a policy and comprehensive risk-based strategy to protect their intellectual property, proprietary information and other intangible assets.

The premise for this guideline is that an organization's competitive edge is the result of information derived from the creativity and innovation of its personnel, and that the loss of this information would negatively impact the organization's investment in personnel, time, finances, product and/or property. No matter what the specific information is—a trade secret, patent information or other intellectual property—organizations must take measures to protect this most valuable asset, and the Information Asset Protection Draft Guideline, when completed, will provide the necessary guidance in developing these measures.

I am extremely proud of each of the initiatives I've outlined, as well as the many others that editorial space precludes me from mentioning. I am honored to have led the Society at a time of such great growth and achievement, and thankful for the many opportunities my position afforded me to travel around the world and meet so many of you in person.

You too should be proud of what we have achieved together this past year. You are truly the heart of ASIS International. I encourage you to continue your involvement in the Society, and support for my very capable and professional successor, Steve Chupa, CPP, the 2007 President of ASIS.

Again, my thanks for all each of you have done in 2006 to further the mission of ASIS and advance the security profession as a whole.

CPP Profiles

Ken Johnston

Drum Cussac Limited, Technical Security Consultant
Provide technical security services to clients in challenging and complex environments. Responsibilities include but are not limited to – Risk Assessments, Security Surveys (Physical & Technical), System Design and implementation of Integrated Security systems. PSP Since Nov 2006, CPP since Nov 2005

Why did you decide to become a PSP?

Drum Cussac strongly promotes the continuous professional development of its staff and rewards consultants holding recognised security related certification and qualifications. Drum Cussac supported me in gaining both the PSP and CPP certifications. With over 12 years experience in the security environment, delivering both physical and technical security projects I wanted my skills and knowledge recognised through an externally validated qualification. The PSP certification defines my ability and recognises my credentials as a professional security practitioner in the security industry to both peers and prospective clients.

Has it helped your career? If yes, how?

The study program and exam have allowed me to provide enhanced services to our clients and demonstrates that I have the necessary knowledge, skills, experience and dedication to provide a professional service. Drum Cussac have allocated a pay award following the announcement of the PSP results, reaffirming their commitment to continuous professional development.

If No, do you think it will help in the future and if so how?

I believe holding the PSP certification will give me an edge when tendering for contracts and responding to requests for proposals.

Has the PSP helped in your day-to-day job function?

The PSP study program has honed my skills with regards to delivering detailed technical security solutions. It is good to refresh your knowledge and continued learning can only lead to a more proficient service to clients.

What advice would you give to prospective PSP candidates?

This certification requires a good understanding of all elements within the security environment. The PSP is technically superior to the CPP and requires at least 6 months of study before taking the exam. I would recommend getting a helping hand from ARC-Training with their in-house PSP study package or using the ASIS online packages.

SRVP Group 15 (Regions 25-28)

Certification Breakdown for Current Members as of 08 FEB 2007

CHAPTER NAME & NUMBER	MEMBERS	CPPS	CPP%	PSPS	PSP%	PCIS	PCI%
Region 25							
208 - United Kingdom	707	85	12.0	12	1.6	1	0.1
213 - Benelux	265	31	11.6	3	1.1	0	0.5
216 - Ireland	65	16	24.6	0	0.0	0	0.0
249 - France	53	3	5.6	0	0.0	0	0.0
Total	**1,090**	**135**	**12.3**	**15**	**1.3**	**1**	**0.0**
Region 26							
094 - Norway	104	3	2.8	0	0.0	0	0.0
197 - Sweden	174	19	10.9	2	1.1	1	0.5
210 - Finland	66	0	0.0	0	0.0	0	0.0
228 - Denmark	136	0	0.0	0	0.0	0	0.0
Total	**480**	**22**	**4.5**	**2**	**0.4**	**1**	**0.2**
Region 27							
143 - Spain	106	10	9.4	0	0.0	0	0.0
211 - Italy	73	3	4.1	0	0.0	0	0.0
238 - Turkey	32	2	6.2	0	0.0	0	0.0
Total	**210**	**15**	**7.1**	**0**	**0.0**	**0**	**0.0**
Region 28							
107 - Austria	19	1	5.2	0	0.0	0	0.0
160 - Switzerland	55	1	1.8	0	0.0	0	0.5
243 - Aegean	19	1	5.2	0	0.0	0	0.0
251 - Germany	97	5	5.1	0	0.0	0	0.0
252 - Czech Republic	38	1	2.6	0	0.0	0	0.0
Total	**480**	**22**	**4.5**	**0**	**0.0**	**0**	**0.0**
ASIS INTERNATIONAL TOTAL	**34,407**	**714**	**13.7**	**469**	**1.3**	**124**	**0.3**

2007 Committee

Derek Webster	**Chairman**	020 7593 2126	derek.webster@psc.gov.uk
Barrie Millett	**Vice Chairman**	07919 176287	barrie.millett@wilsonjames.co.uk
Donna Alexander	**Committee Member**	020 7116 3563	donna.alexander@barclays.com
David Cresswell CPP	**CPP / PSP Rep**	0118 984 1040	davidcresswell@arc-tc.com
Barry Walker	**CPP PDC**	01794 516171	barry.walker@mfdinternational.co.uk
Stuart Lowden CPP	**Honorary President**	01628 535600	stuart.lowden@wilsonjames.co.uk
Graham Bassett	**Media/Advertising & Seminar Exhibitors**	07961 123763	graham@gbassett.co.uk
Helene Carlsson	**Media – Newsletter/Web site**	07802 864485	helene.carlsson@btinternet.com
Mike Hurst	**Media – Newsletter/Web site**	0845 644 6893	mike@hja.co.uk
Nigel Flower CPP	**Membership**	01276 684709	nigelflower@msn.com
Jude Awdry	**Secretary & Admin Manager**	01494 488599	asis@awdry.demon.co.uk
Mike Alexander	**Seminars**	020 7818 4642	mike.alexander@henderson.com
Mick Egdell CPP	**Seminars**	020 7542 5741	michael.egdell@reuters.com
Mike O'Neill CPP	**Seminars**	0118 945 4895	mike@greymans.com
Peter French CPP	**Senior Regional Vice President**	020 8626 3100	pfrench@ssr-personnel.com
Byron Bartlett	**Social**	01303 872777	bj@orgarswick.freeserve.co.uk
Craig Pickard	**Treasurer**	020 7680 5400	c_pickard@lynxsecurity.co.uk

Obtaining Information by Deception

On 7th February there were a number of headlines in various newspapers along the lines of:- UK to jail the data thieves for two years. This refers to a recent consultation document from the Dept. of Constitutional Affairs dealing with the problem of obtaining people's personal data by deception, specifically by private investigators and journalists. The Information Commissioner published a document called "What Price Privacy?" in which he addressed the increasing problem of the theft of personal data. In that publication he made a recommendation to increase the maximum sentence for a breach of Section 55 (obtaining information by deception) of the Data Protection Act from £5,000 to two years' imprisonment.

"People have a right to have their privacy protected from those who would deliberately misuse it, and I believe the introduction of custodial penalties will be an effective deterrent to those who seek to procure or wilfully abuse personal data" – said Lord Falconer, Secretary of State for Constitutional Affairs.

Many of you will at some stage have either conducted investigations or used the services of private investigators. Are you certain that they are not obtaining information by deception? If they are, in the not too distant future you as the client could be facing a prison sentence.

Our privacy laws are similar to those in the rest of Europe, having emanated from the same directive, 95/46/EC. Many of the other member states of the European Community have imprisonment as a maximum penalty and to date the writer is not aware of anybody in Europe having been imprisoned for any direct breaches of Data Protection. Three individuals were recently imprisoned here in the U.K. on Data Protection related matters. It was successfully argued that they impersonated the Office of the Information Commissioner. One of them got away with nearly £250,000.

One of the issues is, how far can the deception go? What Section 55 of the Data Protection Act is not saying is that you cannot, when making enquiries with neighbours, tell a little porkie. i.e. I'm looking for Fred Smith. I was in the forces with him and I've lost touch with him. Any idea how I can find him? In fact the writer has a "get out of jail" card, which is a letter signed by one of the Assistant Commissioners, who said that: "We recognise that a degree of deception is acceptable in the legitimate conduct of an investigation". He may regret having said that, but I have it in black and white.

I would suggest a guideline that you might like to follow is as follows. If you or your investigator impersonate someone whose position is created by statute or local bye-law, then you are likely to have breached Section 55. If you or your investigator obtain information from an organisation such as a bank, DVLA, PNC, then you most certainly will be committing an offence under Section 55.

If you need banking details, criminal records, telecommunication records, credit card details, etc., there are provisions within the Data Protection Act 1998 for you to obtain them. Unfortunately, there are a number of hurdles that you need to clear before the organisation that has the information is able to provide it to you. Even if you clear those hurdles they are still not mandated to provide the information to you. This is similar to what the police experience. If they want information from an organisation then they have to comply with the Data Protection Act, so what is so special about companies or private investigators?

There is still the practice amongst security departments to exchange information on the QT. It is referred to as data sharing. It is effective, which is why security departments do it. This exchange of data is, in many cases, unlawful and as such could well breach Section 55. If you are going to exchange data with one another then put it on a formal footing. The Association of Chief Police Officers exchange information with the likes of the Financial Services Authority, the Law Society, DVLA, etc., and they have it on a proper footing by way of protocols and memorandum of understanding. Why would the security industry have any more rights than ACPO?

While you are all feeling badly done by, let me give you some comparisons with our fellow European states with regard to the maximum penalties they face for serious breaches of Data Protection.

Austria	Imprisonment up to one year, unless it also breaches the Austrian penal code, and then it could be 10 years
Denmark	4 months
France	5 years
Germany	2 years
Greece	3 years
Hungary	3 years
Italy	3 years
Poland	3 years
Spain	They have actually fined a company in excess of 1,000,000 Euros
Russia (not part of the EC)	If you breach their Federal Law and Commercial Secrets, as it is called, you could end up serving 10 years

The results of the consultation can be found at **www.dca.gov.uk/consult/misuse_data/cp0906.htm~responses**

Chris Brogan MA

AGM 2006

We were delighted that Reuters hosted our AGM this year and thanks go to them and organiser Mick Edgell.

The event was, as usual well supported. Sponsors, FIRST SECURITY GUARDS and exhibitors ARC TRAINING INTERNATIONAL, BELL SECURITY LTD (TRACCESS DIVISION), ESOTERIC LTD, FIRST SECURITY (GUARDS) LTD, IRIYS INFRARED INTEGRATED SYSTEMS LTD, NEDAP GREAT BRITAIN LTD, UNIVERSAL SECURITY SYSTEMS LTD and WILSON JAMES LTD all helped to make this a great day.

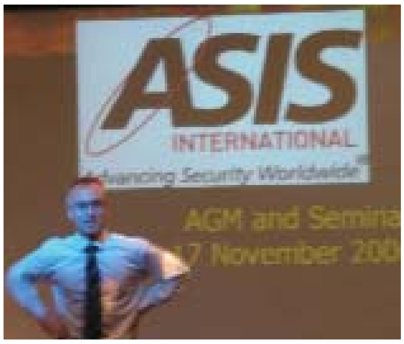
The attendees seemed unanimous in the belief that this one of the best seminars we have run, largely due to our two Keynote speakers.

Marcus Child's two sessions "The CEO Prospective - Keeping Business in the Forefront" and "The People Business – Ideas on delivery and keeping management motivated", were animated, entertaining and thought provoking. Anyone who has seen Marcus speak will understand what I mean.

Also thought provoking and a little bit scary was BT's Ian Pearson's (acknowledged as one of the world's leading futurists) presentation "The Future: Impact on Security and Risks to Business". I am still pondering over some of the subjects he covered.

We were pleased that Anthony McGee, of Cranfield University, was able to update us on the ASIS sponsored research project - Security Management – Education & Qualifications 'A Professional Project for Corporate Security'.

The AGM also marked the end of Stuart Lowden's 2-year tenure as Chapter Chairman. Thanks go to him for all his efforts and we look forward to Derek Webster's reign.



Esoteric Awarded NSI Gold Quality Award

We are always pleased to promote achievements by ASIS Members and we were delighted that Esoteric (which has been a great supporter of the Chapter for many years and is headed by ASIS Professional Development Committee member Emma Shaw) chose our AGM as the occasion to receive their NSI Gold award.

Guildford based Esoteric has become the only company in the UK providing electronic sweeping services and covert investigations services to have achieved an NSI Gold Quality Management Award BS EN ISO 9001:2000.

The company, which is the leading provider of electronic countermeasures and covert investigation services, received the highest recognition of their commitment to customers and quality management, the National Security Inspectorate's (NSI) Gold Award. The award was presented to them by the National Security Inspectorate's (NSI), Marketing Manager, Julian Stanton at ASIS UK AGM on 17th November 2006

Gold status is only awarded to companies who consistently meet the industry's highest standards through ISO9001 Quality Management as well as the relevant British and European Standards.

Emma Shaw, Managing Director stated, "We are committed to providing an exceptional service to our clients through excellent service delivery and quality management. We are unique in receiving this award for our specialist range of services and very pleased to receive this accolade"

The NSI is the UK's leading inspectorate for the security and fire industries, an independent, not-for-profit organisation. For over 30 years the NSI has been protecting customer's interest by insisting on the highest standards and operating the toughest inspections regimes. Companies are inspected regularly for their continuous delivery of the highest standards to their customers. The NSI also operates a customer care support process, underpinning the reliability and integrity of companies it inspects.

Gill Head, Sales & Marketing Manager,
ghead@esotericltd.com

Understanding the impact of identity fraud

Martin Gill and Gemma Keats

Identity fraud is on the increase – according to CIFAS the UK's fraud prevention agency - identity fraud has grown by 500 per cent since 2000. The financial impact is considerable, the Home Office estimate a cost of £1.7 billion per year in the UK alone. Identity fraud is committed when a criminal uses another person's identity to obtain goods, services or credit fraudulently. This may involve applying for store and credit cards or opening bank or mobile phone accounts in another person's name. American research has highlighted the emotional stress suffered by victims as well as the practical difficulties in rectifying the damage to credit rating. Similar findings emerged from work undertaken in the UK by Perpetuity Research and Consultancy International (PRCI) Ltd on behalf of CIFAS. This research focused on the impact of identity fraud on victims.

It began with a questionnaire circulated to over one thousand victims of identity fraud of which 212 were completed and returned. Analysis showed that victims' identities were most likely to have been used to apply for store cards, credit cards and mobile phone accounts, and in many cases multiple accounts were also opened in their name (e.g. store card and credit card). Approximately half of the victims reported that their experience of identity fraud had greatly affected their stress levels, whilst slightly more said that it had caused them considerable inconvenience. One in depth interview with a victim in another study highlighted the emotional impact identity fraud can have. Her handbag was stolen containing items such as her driving licence, cheque book and credit cards. These items were subsequently used to apply for store cards, mobile phone contracts and three attempts were made to cash her cheques. She described how this experience had made her paranoid that someone would break into her home and she worried that another fraudulent application would arrive in the post.

Unsurprisingly multiple victimisation caused more stress levels and the longer it took to solve problems the more stressful it became. Also victims with a higher income tended to be more likely to report that identity fraud did not affect their health or stress levels greatly. Previous research suggests that it typically takes 300 hours for an identity fraud victim to clear his or her name however over half the victims in our study said that dealing with the aftermath took less than 24 hours. Nevertheless, more than 1 in 10 said it took longer than a week.

In the majority of cases victims of identity fraud do not suffer significant financial repercussions as a result of their experience; the costs incurred are typically covered by the service providers and financial institutions involved. However financial losses can be incurred by the victim in resolving their situation; victims who completed the survey for instance noted the cost of telephone calls, postage, printing and travel. In addition identity fraud could also have an affect on a victim's credit rating causing potential problems and delays when making credit applications.

Statistically the chances of being a victim are low, but it has only been possible here to briefly discuss the victims' experience, a more detailed discussion would reveal that it was typically annoying and a hassle. In more severe cases, where identities had been adopted to run up multiple debts in particular, victimisation took on a more intrusive form, indeed some described it as a type of personal violation. Sometimes the identities fell into offenders' hands as a result of a burglary and sometimes ex partners were felt to be implicated. But one of the most striking findings was that victims mostly did not know how their identities found their way into illicit hands.

It is essential then that individuals and businesses alike are aware of the risks of identity fraud and the steps that they can take to help prevent them from falling victim to it. There is a wealth of information and guidance available which provide simple and easy tips to do just this. Steps include:

- Checking your credit report regularly to ensure that no one has been using your identity to obtain credit.
- Regularly checking your bank / credit card statements for unusual or suspicious transactions.
- Shredding all documents containing personal or financial information before throwing them away or recycling them.
- Memorising passwords and pin numbers instead of writing them down and using different numbers for all your cards / accounts.
- Checking the identity of anyone who asks for your personal or financial information before giving it to them if appropriate.
- Keeping a record of those numbers you would need to ring if your credit or bank cards were stolen – cancel them immediately after they are stolen.
- Keeping passwords and pin numbers separate from credit and bank cards.
- Re-directing your mail if you move home and informing all relevant financial companies and service providers of your new address.

Martin Gill is Director and Gemma Keats a Research Assistant for Perpetuity Research and Consultancy International.
www.perpetuitygroup.com

CPP Profiles

Bob Martin

Managing Director, RFMSolutions Limited

Global and Organisational Strategy for security integration

Why did you decide to become a CPP?

Having 20 years of security experience within the PetroChemical industry, and having introduced a single integrated FM/IT/Security global solution in the diversity of situations within that industry is one thing. Having a globally recognised security practitioner's qualification is quite another thing. Experience is invaluable, but a qualification of the standing of the ASIS CPP proves beyond doubt the ability of the individual. It was therefore the challenge to achieve the certification to prove competance in the delivery of security solutions.

Has the CPP helped in your day-to-day job function?

From the first introduction to the CPP learning literature it has helped me. My scope of knowledge, (which was already fairly broad), has been increased way beyond my expectations. I now have a much wider perception of the industry as a whole, which has already been demonstrated in my discussions with clients. Had I not have been successful in attain certification, I would still have learnt so much that all the time and effort would have been well spent.

What advice would you give to prospective CPP candidates?

A reasonable amount of the course material by default is US centred, but with a bit of lateral thinking it can be adapted to the non-US environment, which then makes it all relevant.

Mike Pemberton

Conoco Phillips, Algeria Security Manager

Responsible for the security of all Conoco Phillips personnel and assets within Algeria.

Why did you decide to become a CPP?

To further my career I required an internationally recognised professional security qualification and the CPP is the most widely accepted qualification in both my industry (oil and gas) and internationally.

Has the CPP helped in your day-to-day job function?

Yes it has, whilst I had a lot of practical "hands on" experience, studying for the CPP examination has given me a more in depth understanding of the security management function and a far broader knowledge of security principles and practices.

What advice would you give to prospective CPP candidates?

The study guide and training seminars are invaluable however you must still read the books

The Convergence of Traditional and Logical security

James Willison

Since 2004 many of those involved in the leadership of ASIS have sought to encourage and promote the movement we now know as the Alliance for Enterprise and Security Risk Management. Timothy Williams articulated the vision of those early beginnings when he said, “Convergence is more than just the latest buzzword for security professionals. It’s the direction in which security is moving—and moving quickly—with us or without us.” In January 2006, Jeff Spivey stated, “Our collaboration with other associations examining convergence is a very valuable strategy to ASIS and the other Alliance members. More collaboration will strengthen each association as we all strive to meet our members' needs.” In 2007, in the UK, an open forum for all members of the Alliance is being planned to further this unity. It is worth our while to look closely at this important area and see how we can all help to increase the effectiveness of the security policies entrusted to us.

In many global companies physical security and information technology (IT) security are ensured by two separate sections. There are two heads of security who occasionally meet to discuss relevant concerns and then return to an ever increasing range of security matters and deal with them as effectively as they can. Of course thankfully there are many gifted security professionals protecting companies from attack and fighting crime but would this effort be strengthened by a more united front? Military history for example has shown that when several nations have attacked an empire building nation on various fronts it eventually collapses. But one nation cannot resist large scale military invasion without some level of support from another. Many 20th century wars would fit this idea and other empires, for example the Napoleonic, have eventually been defeated when attacked on two or more fronts.

Of course we are all too aware that internet security issues can severely disrupt a business and there are now many more vulnerabilities to safeguard against. But what is becoming increasingly apparent is the rising support amongst security professionals for the convergence of physical and IT security. This is in part due to the realization that it is becoming more and more difficult to ensure information security without an intricate relationship with the physical infrastructure. It is often the case that the IT security team is part of the IT department and the physical security team is led by the facilities or health and safety section. The philosophy of management may well be rather different even if both are seeking to keep in harmony with company policy and vision. Company culture and aims are paramount but can the purpose of security in maintaining and protecting these always be achieved when the two teams are also accountable to two different masters?

Convergence is now becoming such a widely held view that the editor of CSO magazine recently remarked,

“Indeed, considering IT or any other kind of security in isolation from the rest is a serious misunderstanding of the larger purposes of security as a broad strategic activity. In our view, convergence can't come soon enough.” (www.csoonline.com)

The issue of the convergence or integration of physical and IT security has actually been a possibility for over twenty years. For a few it occurred at the birth of computer security in the early 1980s but for most it seems that the two have been separate and part of two quite different sections. Usually the IT department developed the tools and strategies for the IT security team and only became involved with the physical security team when their support was needed during the investigation of a corporate crime. But the development of a more holistic approach to security management has led to the call for the two areas to converge and so detect crime more effectively. The concern now is for business security management. Authorised access to company information is of particular concern to both teams and their unity in achieving this is crucial.

In recent years there has been a proliferation of articles on the World Wide Web encouraging such unification. There certainly seem to be more in favour than against. This may be due to the concern that when the two areas work in isolation the risk that vulnerabilities will be missed increases. Therefore it would be better to communicate and integrate more rather than less.

In a perceptive treatment of the subject, ‘The Case For Holistic Security’, Caroline Ramsey Hamilton writes,

“There are several reasons for this convergence between information security and physical security. One of the primary reasons is because physical security elements have become increasingly computerized and networked.” (www.riskwatch.com)

In 2002 a survey of IT professionals attending the Microsoft Exchange Conference (MEC) indicated that 21% were merging or planning to merge network and physical security. The pie chart below shows the results. According to Aladdin Knowledge Systems a further 20% were unsure. This is clearly favourable since they could be persuaded that integration is the best strategy for the future. The research also stressed that 90% of those who answered in the affirmative represented companies with more than a thousand employees.

Figure 1 indicates the findings of the Aladdin Knowledge Systems survey of over 500 IT professionals at the MEC 2002 in Anaheim, California. (www.aladdin.com)

In particular the subjects of identity management and access control have been of central importance to both teams. It is crucial for a company to have an effective policy on these matters particularly now that the Data Protection Act 1998 and the Sarbanes Oxley Act 2002 exert their influence on organizational behaviour. It would be fair to claim that companies which allow their staff and contractors to have several different logins and use various ID cards are more at risk from false logins than those who adopt a single login and use smart card

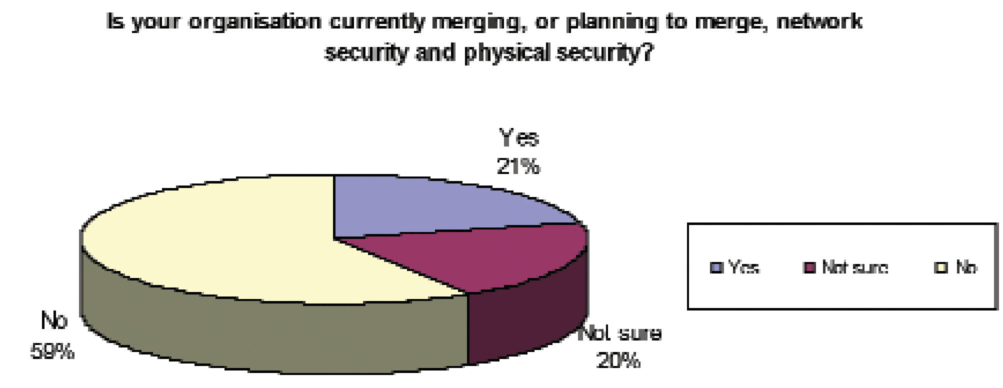


Figure 1. Organisations Merging or Planning to Merge Network and Physical Security.

technology to access both physical entrances and computer systems.

It is perhaps the area of identity management and the requirements for verifiable audit trails made by the various acts mentioned above which will actually bring IT and physical security into the same arena. The case for a smartcard solution to the problems raised by identity management is a very strong one. In the light of the continual growth of internet commerce and the interconnectivity of networks the need for an authentic and secure identity in global organizations is indisputable. It also prevents unauthorised remote access by staff who have either left the company or who have 'borrowed' passwords from their colleagues. If this is true then the two teams in any corporation which deal with access control and whose responsibility is focused on ensuring that a person has authorization both to enter the building and logon to the network should work together on this issue.

The evidence of my research reveals that many security leaders believe global organizations would benefit from the integration of their security teams under the leadership of a chief security officer. It is also a widely held view that he or she could quickly respond to any security issue in the confidence that they are fully supported by their staff. This single point of contact is of particular importance to the board of directors.

All in all, this is just a glimpse into the whole area of converged or holistic security. One which deserves the attention it is now receiving.

James Willison : Since joining ASIS in April 2003 James has worked closely with security leaders from the traditional and digital arena with a desire to enrich the process of convergence. In July 2005 he was awarded a Master's degree by Loughborough University for his research on, "The case for the Integration of Corporate Physical and IT security."

ASIS Diary Dates 2006/7

2007

14 March	*Pre-Seminar Dinner*
15 March	*Spring Seminar, BBC, London*
25–28 March	*6th European Security Conference, Berlin, Germany*
24 – 26 April	*Infosecurity Europe 2006, London*
21 – 24 May	*The May Series, NEC, Birmingham. (IFSEC, The Facilities Show, Safety & Health Expo, International Fire Expo, Police & Public Security)*
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*

NEW MEMBERS

Chapter 208 extends a warm welcome to the following new members:

Christopher Aldous	
Richard Bailey	Advance Security UK Ltd
Paul Burke	
William Bush	Wyeth Europa
Mark Carruthers	ArmorGroup
Chris Cerroni	
Frank Davis	FCO Bogota
Barry Dawson	Advance Security UK Ltd
Mark Dinsdale	
Allison Drake	
Hugo Gillum-Webb	Advance Security UK Ltd
Geoff Graham	Control Risks
William Gray	
Wayne Griffiths	
John Hall	Glasslock Ltd
Toby Harding	
Peter Heals	Bell Security Ltd
Geraint Jones	
Neil Kerr	
Richard Kocher	TRL Ltd
Barrie Last	
Jamie Macpherson	
Ivan Marsh	Camelot Group PLC
Leslie Martin	Arena Security Management Ltd
John McHugh	IEDS Ltd
Christopher McKenna	
Hugh McLeod	HSBC
Greg Morganti	Advance Security UK Ltd
Graham Organ	Direct Drive Transport Solutions
Russell Penny	
Letitia Poole	
Maria Pulera	
Mark Purnell	Armorgroup Services Ltd
Norman Russell	Barclays Bank PLC
Ian Saunders	
Simon Scales	
Andrew Scott	Post Offices Ltd
David Solomons	
Tony Stead	UK Armed Forces
Stephen Steeds	Bell Security Ltd
Mark Stevens	
Peter Sutton	
Dorota Szulc	Hansard Security Services Ltd
Damian Taylor	Control Risks
Trevor Tomlinson	
Julian Tubbs	
Allan Tweedale	Marriott International
Paul Whitbread	Weatherford
Andrew Wilson	

Crisis & Contingency Planning is Part of the Risk Assessment Cycle

Peter Speight, Director of Security Risk Management – Reliance Security

Crisis Management is a systematic response to unexpected events that threaten the people, property and operating continuity of the organisation.

In my opinion, one of the leading authorities in this area is Peter Consterdine of Future Global Plc who wrote 'Crisis Management builds upon the practises of emergency management, the principles of risk management, and the elements of risk and crisis communications, the concepts of business continuity and contingency planning and security considerations.' (Consterdine, 2005)

Research shows that only 25% of U.K. organisations have a regularly tested disaster-based business plan. Even fewer have run full scenario testing of other, core recovery plans. Companies that cannot demonstrate clear and comprehensive risk management strategies will be penalised by an already harsh insurance market. Conversely, insurance companies may lower premiums they charge if they can be convinced that a disaster recovery plan is adequate. Company officers are increasingly held liable for such issues as 'Corporate Killing'. Clearly most organisations are only prepared to deal with emergencies at the incident site, and often, due to legislative requirements, for example, fire, and evacuation plans/drills.

'The systematic models of Turner and Perrow appear to suggest inevitability for organisational failure. The homeostatic model (Adams, 1995) suggests that an unconscious or instinctual need to create risk will always balance out against those that are eliminated. Problems with risk, irrationality and the complexities of social communication and regulation again point to the need for more resources applied to response, rather than prevention.' (Borodzicz, 2005, p.73) 'Prevention, where possible, is always better than the response after things have gone wrong. In the complex world we now inhabit, a failure to be able to respond to failure is of equal concern.' (Borodzicz, 2005, p.73)

There is a lot of groundwork to do, particularly in establishing the capabilities at any location/locations to manage/execute a crisis plan. Firstly, somebody would need to define the Objectives & Principles e.g. the definition of a crisis, but not specify or categorised the range of threats they feel need consideration – they may say "a company faces several threats that could cause crisis within the UK and all other subsidiary companies".

And the tasks will normally include:

- All site risk assessments
- Preparation of Crisis & Contingency Manual
- Establishing a suitable Crisis Management Room
- Training
- Scenario-based testing

Within the manual, it is necessary to develop some specific 'Action Guidelines're, say, Abduction, Product Contamination, Extortion, Bomb Alerts etc. If the sites include manufacturing facilities, I believe it is essential to develop a 'Disaster Manual', and if we are dealing with an ex-pat community in a Third World geography, then 'Evacuation' must be dealt with.

My thinking is that 'base level' procedures are put in place for emergency management. Whilst 'Corporate' would require a 'Crisis Management' plan in place, avoidance of a crisis usually depends upon the management of emergencies, so as to prevent them turning into a crisis. It is necessary to detail a whole range of potential incidents, roll some up into the Security Manual, with site guidance instructions and then ensure that the emergency communication – up the line - is well established.

Consideration needs to be given for a separate 'Communication Manual' and the question asked 'can this aspect of crisis management be adequately covered in the main crisis manual'?

In terms of 'structural characteristics', it is of vital importance to the 'emergency management system' that it has the same structure at site, company, country etc with clearly defined job descriptions, defined competencies, tasks and processes.

My preferred structure for a team consists of Director, Co-ordinator and three core modules (Communication, Data/Documentation, Logistics), this is not far removed from normal 'Corporate' requirements, however, the recommendation would be that the country M.D. should be the Head/CMT and you may need to evaluate this.

Another area for discussion is there a requirement for site 'Emergency Response Teams' and, if so, how constituted! Additionally, there will need to be alert states and a process put in place whereby intelligence from whatever source is constantly evaluated so as to keep the 'Alert' systems relevant and timely.

'Any Emergency Management' should be designed to allow mobilisation of the right resources with the relevant expertise for the problem at hand i.e.

- Facilitate full concentration on emergency management tasks
- Allow business to continue as normally as possible
- Enable 'the company' to show competence in the face of the unexpected

Corporate Communications need to be involved; certainly in the preparation stage and their future involvement will be defined by evaluation. Certainly, they should be part of an issue-tracking network, whereby any issue with a potential impact to the company is identified and transmitted to the Emergency Management Co-ordinator. They may also co-ordinate 'advocacy' activities in defence of the company's positions. Ideally, they should fulfil the following 3 requirements: -

- To signal trends for potential issues identification
- To provide support for issue preparedness
- To provide advocacy support

BUSINESS CONTINUITY MANAGEMENT (BCM)

At this juncture, it is important to consider the wider issues of crisis management as they extend to the recovery and continuity issues. It is not sufficient for those who may be involved in the management of a crisis, even if handled successfully, to pat themselves on the back and consider the job well done and concluded. Often the conclusion of the crisis is the start of the eventual restoration of business functions.

The planning for business continuity extends the work on emergency handling and crisis management and recognises that successfully handling incidents and events is only part of the overall requirement to get a business back up and operating as before. The objective of business continuity is to return the organisation to normality as quickly and as expediently as possible, with minimum losses.

Business Continuity Planning (BCP); understands the business and establishing what is vital for it's "survival following a major disaster affecting normal operations"

BCP can be viewed as a four-stage cycle:

1. Mitigate – to reduce and manage risks
2. Readiness – all measures which need to be in place, especially planning, warning systems.
3. Response – the management of the emergency, or crisis.
4. Recover – once the incident is over (or even during), the continuity plan should identify the requirements for the return to normality.

It can be seen from the above the natural overlap which occurs between the identification of risks, their management by means of security analysis and necessary adjustments outlined in the security strategy, the establishment of the crisis plans and the implementation of business recovery strategies.

Business continuity is about establishing key processes and business functions and what resources departments will require and within what time scales, to re-commence those processes and functions that have been determined as critical to the business.

Organisations have many dependencies, both internal and external, which support their critical processes and functions. These may include, but not exclusively, suppliers, customers, I.T. systems and manufacturing processes. The critical needs of departments need to be analysed and ranked in order of importance, for example:

- ESSENTIAL
- IMPORTANT
- NON-ESSENTIAL

Each functional area of the organisation should be analysed to determine the potential consequences and impact associated with several disaster scenarios. The assessment process should also evaluate the safety of critical documents and vital records.

This assessment is carried out by means of the Business Impact Analysis (BIA). The BIA is the second stage of the crisis/disaster recovery process and it identifies what would be the impact on the organisation's goals if critical processes and functions were disrupted or lost. The BIA enables the organisation to focus BCP activities on essential business elements

Mitigation is primarily about managing and reducing risks whatever their source and can be covered with the Risk Assessment & Security Audit process.

Readiness is the 'in-house' insurance policy and covers all the preparedness measures, notably planning. It includes internal warning systems, communications, control teams, equipment & resources, casualty procedures, essential services, media policy, critical records and welfare arrangements.

Security too, is part of readiness and terrorist activities should serve to sharpen awareness of it. With the production of the Security Manual, this aspect of 'Readiness' should be in progress? A well-conceived security plan based on sound intelligence, business acumen and common sense provides protection and ensures an appropriate response to criminal incidents other than terrorism.

This process involves a great deal of work, not just in the composition of the Manual, but in its integration with 'site' procedures and subsequent training and education procedures.

'Major crises – from Challenger, Bhopal, Tylenol or Chernobyl to Exxon Valdez and Braer – are no longer exceptional events. Indeed the risk of crisis is even becoming structural as large networks become more complex, more vulnerable and more independent … crises continue to become more frequent and destabilising.' (Lagadec, 1993, p.45)

Lagadec is not alone here: as crises become more numerous, visible, and calamitous, organisations have no choice but to accept them as inescapable reality that must be factored into their planning and decision making. (Lerbinger, 1997

MAJOR DISASTERS

'Are a serious disruption to life, with little or no warning, causing or threatening death or serious injury to such numbers of persons, in excess of those, which can be dealt with by the public services, operating under normal conditions at that time. Which calls, therefore for special mobilisation and organisation of those services.' (Wilson, JQ. & Slater, T, 1990, p.6)

We only have to look at a selection of past incidents, which made world news, such as the deaths of the Apollo Space Capsule Crew who perished in a fire during practice drills in January 1967, and the crew of the Soyuz XI Space Capsule who died following the capsules decompression during the re-entry in June 1971.

Other examples clearly illustrate our inability to accurately predict the probability of disaster scenarios occurring. For example, Three Mile Island, 26th April 1986, Piper Alpha, 6th July 1988; and the explosion in Guadalajara, 22nd April 1992, to mention but a few. Other disasters like the San Francisco Earthquake, 18th April 1986; the Bangladesh floods in September 1988; and Hurricane Andrew in August 1992, remind us that nature has the power to create even greater mayhem.

Therefore, the faith that of an organisation was able to prevent or provide mechanisms which would help prevent the losses sustained from such events was for many managers in the past simply not credible. As a result, it can be argued their efforts were focused upon protecting their organisations through the purchase of insurance.

An example of such management was the tragic fire at the Bradford City Football Stand on Saturday 11 May 1985, when over fifty people lost their lives. As early as August 1969, the Fire Prevention Association had published an article in the Journal (No 83: pp 322-324) giving details of several fires that had taken place in football stands, like the one at Bradford and warned of the fire risk associated with them.

If this information had been brought fully to the attention of the security management team at Bradford City, they could have acted upon that risk and the incident averted. This is one area where both roles could combine to prevent risk.

Over the years, research has been carried out into disasters and large-scale accidents. It was found that many do display similar features and characteristics. Some organisations now realise that it is possible for them to take positive steps that will significantly reduce their risk. This, to some extent, is based on the fact that insurance coverage cannot be purchased for many of the risks that organisations face, for example, gradual pollution and security managers must assess these risks and use information to devise and implement strategies.

To be continued – Peter Speight's investigation into crisis and contingency planning will be concluded in the next newsletter. For the complete article, please log onto www.asis.org.uk