ASIS INTERNATIONAL™ Newsletter
UNITED KINGDOM CHAPTER 208
SPRING 2015

ASIS NEWSLETTER OF THE YEAR – WINNER 2013, 2012, 2008 & 2003 – HONOURABLE MENTION 2011, 2006.

Advancing Security Worldwide

Since it was founded in 1955, ASIS International has grown from a national association representing a handful of security directors or managers from large corporations in the eastern United States to a global organisation representing 38,000 security practitioners in 139 countries.

The international focus began very early, with the establishment of the Europe chapter in 1959, which, due to steady growth, was broken apart over the years into various European chapters. Today, ASIS has 95 chapters outside the U.S. and a membership base that spans 139 countries. About 28% of its membership is non-U.S., supported by Regional Advisory Councils in Europe, Asia-Pacific, Middle East, Latin America, and Africa. All ASIS networking groups have international representation.

The international region with the most significant growth in 2014 was Region 12A in the Middle East, representing Abu Dhabi, Bahrain, Doha Qatar, Dubai, Jeddah, Dhahran, and Riyadh. The Region saw a 14% increase in membership during 2014.

As the world economies and security challenges have become increasingly global, ASIS has positioned itself to be the leading nonprofit association representing the security industry worldwide. This has enabled unprecedented collaboration with security professionals in every corner of the globe, all of them pursuing the same goal—the protection of people, property, and assets. This is facilitated by a diverse membership, including not only those in corporations, but also individuals from all areas of government and military, as well as the education community, which is preparing tomorrow's security leaders.

The ASIS Board of Directors is also representative of the global security community. Today, three of the 12 board of directors are from outside of the U.S. In 2012, Eduard J. Emde, CPP, from the Netherlands, was the first non-U.S. president of ASIS.

Each year, global conferences in the Middle East, Europe, and Asia Pacific, as well as the ASIS Annual Seminar and Exhibits in the U.S., bring together tens of thousands of attendees to help them keep pace with the security threats and challenges the industry faces, including the ever-evolving technology available.

One of the fastest growing areas within ASIS is in the development of national and international standards and guidelines. Twelve standards and guidelines have been developed, often with input from experts in other standards developing organisations outside the U.S. Work is underway now on the development of the first International Standards Organisation (ISO) standard.

In recent years, ASIS has translated important documents such as the Protection of Assets Manual into Spanish; five standards or guidelines also have been translated into Spanish.

ASIS certification programs have long been popular worldwide, with nearly 8,000 (1,700 outside of the U.S.) individuals now holding the Certified Protection Professional (CPP), the Professional Certified Investigator (PCI), or Physical Security Professional (PSP) designations. The exams are offered in more than 250 locations outside the U.S. and Canada.

Chief security officers from around the world are eligible for membership in the ASIS CSO Roundtable, the private forum for top security executives, many of them from Fortune Global 1000 or Fortune 1000 companies. Of its 385 members, 106 are from outside the U.S., representing security organisations from 20 different countries. CSO programs have been or will soon be held in Dubai, London, Göteborg, Mexico City, Panama City, Istanbul, India, Brazil, The Hague, and Hong Kong; the group also has participated as partners in London, Budapest, and Berlin.

Although the global security community has been a part of ASIS from the early years, in 2002, ASIS officially changed its name to ASIS International. The ASIS Board of Directors adopted a new logo that symbolised inclusiveness, along with the tag line "Advancing Security Worldwide."

Chairman's Notes


Andy Williams

"I am not Charlie, I am Ahmed, the dead Muslim Police Officer. Charlie ridiculed my faith and culture and I died defending his right to do so."

I read this sentence, which was posted on social media shortly after the atrocities in France a few weeks ago. At first it seems slightly shocking, but actually it perfectly sums up the reality of what happened and must serve to remind us all of the threat posed by the extremists in our midst.

The Police and Security services in the UK are facing unprecedented reductions in funding and that is not likely to change anytime soon. Whilst we are assured that funding for Counter Terrorism will be ring-fenced, I need not remind you that we were also promised that there would be no reduction in frontline Policing, so it is essential that we do our bit.

As a community of security professionals we have a unique opportunity and responsibility to educate those that we serve or support; to understand that this was not a one off event in a foreign country, but actually a warning of what will probably happen here, unless we remain vigilant and prepared to combat future attempts. Review risk assessments, business continuity plans and SOPs to ensure that your employer, client and neighbours are prepared.

This is not about business creation or jumping on the bandwagon, this is about protecting our community from, as our American cousins would say, a real and present danger.

Those of you who were able to attend the AGM and winter meeting in December will know that the membership voted to change the way in which the Chapter is managed. This was a technical change that was recommended to the leadership by our legal advisor and will have no bearing on how the Chapter operates or supports you, it was simply done to ensure that we are fully compliant with UK law.

Lastly, I would like to thank the organisations that supported the Chapter throughout 2014, either through sponsorship or by exhibiting at our meetings; without their support we could not operate. As such it is with great pleasure that I can confirm that Axis Communications, Frontline Security Solutions, HID Global and Quantum Secure have agreed to sponsor the Chapter in 2015. This is in addition to the numerous exhibitors and other supporters we have for the coming year.

I look forward to seeing as many of you as possible at our forthcoming meetings.

Best wishes
Andy Williams CPP FSyI


Mike Hurst

As the reality of the threat posed by terrorism is felt by another country, our thoughts go to the families, friends and colleagues of the victims and to the French nation. Whilst the main responsibility for the detection, prevention and investigation of these atrocities will always fall to the police, military, intelligence and security services, we also realise the increasing importance on the private security sector.

Corporate security professionals with the support of security technology and security services organisations, have responsibility for the protection of the people, property and assets in their care. They need to instil an increased security awareness in their employees; assess the enterprise security risk; identify threats; ensure good practise in all areas and make best use of the technology available.

It is staggering to believe that I still find security managers who are prevented or at least dissuaded from attending security conferences, seminars; exhibitions and other events by their employers.

Quite how they are mean to learn of current threats; keep their skills up-to-date and develop a network of contacts if all they do is sit in an office all day, I just don't know. Since March 2014, facilitated by the ASIS UK Chapter, the ASIS Chapter in France, led by Chairman Eric Davoine has been working with the UK Project Griffin Team (ASIS members Don Randall MBE and Graham Bassett) to launch Griffin in Paris. Initiatives such as this can only increase the city's security and readiness to face future threats.

It is partnerships like this that demonstrate the benefit of being part of a trusted network of fellow security professionals internationally and from experience I know that many meaningful discussions will take place and partnerships forged when we all meet in Frankfurt for the ASIS European Conference in March.

Calendar Events

Feb-15	
15th - 17th	ASIS 6th Middle East Security Conference & Exhibition, Dubai
Mar-15	
16th-17th	Total Security Summit, Stanstead
26th	ASIS UK Spring Seminar
27th	ASIS Ireland Chapter, 21st Anniversary celebration, Dublin
28th - 31st	ASIS 14th European Security Conference & Exhibition, Frankfurt
Apr-15	
9th	ASIS UK Northern Seminar, Leeds
15th - 17th	Security TWENTY 15, Bristol
21st-22nd	Counter Terror Expo
22nd - 23rd	ASIS 25th New York City Security Conference & Expo
Jun-15	
TBC	ASIS UK Summer Seminar
16th-18th	IFSEC
Jul-15	
7th	Security IT Summit, London
9th	Security TWENTY 15, Newcastle
Sep-15	
TBC	ASIS UK Autumn Seminar
28 - 31	61st Annual Seminar and Exhibits, Anaheim, California
Oct-15	
19th - 20th	Total Security Summmit
22nd	Security Institute Annual Conference
28th	Security Twenty 16, Heathrow
Nov-15	
TBC	9th Asia-Pacific Security Forum & Exhibition
Dec-15	
2nd - 3rd	Transport Security Expo
TBC	ASIS UK Winter Seminar and AGM

61th Annual Seminar and Exhibits
September 28 - October 1, 2015
Anaheim, USA

25th New York City Security Conference & Expo
April 22-23, 2015 New York, USA

6th Middle East Security Conference & Exhibition
February 15-17, 2015 Dubai, UAE

9th Asia-Pacific Security Forum & Exhibition
November 2015
Singapore

14th European Security Conference & Exhibition
March 29-31, 2015
Frankfurt, Germany

INSIDE THIS ISSUE:

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@gbruk.com

Chapter Executive Officer – Jude Awdry,
ASIS UK Chapter 208, PO Box 208,
Princes Risborough, HP27 0YR.
Tel: 01494 488599;
Fax: 01494 488590;
info@asis.org.uk

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

Your Opportunity to Achieve Professional Certification in Security Management Begins Here

David Cresswell CPP PSP of ISMI Certification Ltd will again be running the highly successful CPP (Certified Protection Professional) and PSP (Physical Security Professional) preparation programmes this year and Chapter members or their colleagues or staff are invited to register for the great-value fee of £1250 + VAT. This includes 6 days in class (2 x 3 days to minimise working week disruption), 4 months of marked distance learning assignments, telephone coaching support and access to ISMI®'s unique online library of security management resources.

Having coached hundreds of Chapter members to success, and with almost twenty candidates currently under instruction, David is a globally recognised leader in security management certification training with many years of relevant experience. And the current PSP class (see image inset) is the largest group of UK/European candidates ever to assemble in the UK to study for PSP.

The course materials are first class, extensively referenced and very well-illustrated to help you assimilate the core concepts. Furthermore, David's knowledge and understanding of the examination subject matter and the source materials on which the questions are based is second to none, and he will use his experience to guide you to knowing which parts of which reference sources are most critical to passing the examination.

ISMI Certification Ltd's successful formula is based on 2 x 3 classroom days interspersed with 4 months distance learning and coaching support. The first session in the classroom will give you a detailed study of the domains and likely areas of testing and you will take away a very detailed handout pack. This is followed by a 4-month programme of supported distance learning to help you get to know in detail the source reference materials upon which the examination questions are based. Your assimilation of the materials will be enhanced by completing set question papers which are marked so that you can monitor your progress. The final classroom session will comprise extensive closed-book testing practice in readiness for the examination, where you will practice with up to 800 sample questions.

The programmes are conducted in a rural Worcestershire location, which provides a very tranquil and conducive environment for study.

CPP® classroom dates are 13-15 May and 14-16 October

PSP® classroom dates are 17-19 June and 18-20 November

Contact Janet Ward at enquiries@ismi.org.uk for more details and a registration form or call 01386 871918 for more information.

Worshipful Company of Security Professionals

Proudly presents a Black Tie Spring Dance

Rembrandt Hotel Knightsbridge SW7

With Irie J's Divas

Saturday 28th February 2015

Reception 6.30pm for 7.15pm

Tickets are £96.00 + VAT

Contact Peter.French@ssr-personnel.com

Charity Raffle & Auction Carriages at 12.30 am

KINGS SECURITY SYSTEMS

The evening is supported by ssr-personnel.com Registered Charity No. 1088658

Ten Reasons to switch over to IP and Network Cameras

IP network cameras offer superior images for precise accurate information. Cost savings can be made as only one cable is required for video and power (power over Ethernet POE), negating the need for power outlets at each camera location.

They are easier and quicker to set up, and can offer further features such as remote set up or zoom facilities via your network. With megapixel resolution you get far more detail for easier identification, and formats to cover larger areas of coverage for less cameras.

EASE OF INSTALLATION

Megapixel resolution & HDTV capabilities Intelligence at the camera level Integrated audio and PTZ control Secure communication Open and easy to scale True digital solution

Gateway for new system solutions

Lower total cost of ownership

Smart Analytics to enhance your security as management tools

HDTV cameras can offer much crisper colour rendition and widescreen formats, and we can now offer intelligence at the camera level with the ability to keep adding further functionality over time. This can also offer more efficient monitoring of especially larger systems or specific areas, and relieve the burden on operators with intelligence built in such as alerts, alarming, and detection improvements. Even specific programs such as people counting, heat mapping and dwell time analysis can be added amongst other unique applications.

IP cameras and networked systems allow easier integration with other security ranges such as Intruder and Access Control systems and offer future proof investment. Storage can even be managed via SD cards in some cases enabling you to push the video required at the right time enabling less storage space and wasted storage requirements. IP offers flexibility, scalability easily upgradable and fantastic image quality.

For further information
contact Frontline Security Solutions
www.fsslimited.com

SECURE CARD ISSUANCE – Smart Card Solutions for Higher Education by Serra Luck

Creating a "One Card" Solution for the University

Colleges and universities must keep their campuses safe in as cost-effective manner as is possible. At the same time, each school has its own set of unique demands and challenges, requiring flexible system architectures that satisfy today's demands while providing the foundation to meet future security needs. HID Global's solutions and services for educational institutions are developed from the ground up to solve these challenges and give security officers the confidence that their infrastructure can protect students, staff and faculty for years to come.

Building the Foundation: Reader and Card Technology

The majority of today's institutions still use legacy technology that offers little security. As such, many universities are seeing a rapid increase in fake student ID cards. In order to solve this problem, the best option is to migrate all the way to contactless high frequency smart cards, which combine improved security with the convenience of being able to use a single card for multiple applications, including secure debit and payment capabilities. These smart cards can be used for safe and secure keyless access throughout the campus – in dorms, research facilities, as well as departmental ID verification and meal plan purchases. Overall, the expense of moving to contactless smart cards is outweighed by the long-term cost savings from improved management efficiencies. Moreover, migrating from old to new systems using multi-technology cards and readers need not disrupt day-to-day workflows. For example, universities can retain their existing student ID and issue code numbering system.

Secure Issuance: The Other Half of the Equation

A secure and efficient printer/encoder solution is critical for issuing student ID cards, even – and especially – during the busiest periods at the beginning of each term. Students do not want to stand in line for hours during registration, only to be told that they must come back tomorrow to get their badge. Equally, cards need not be issued every year – each card should be issued for the life of the student's involvement with the institution.

Fortunately, today's printers, card materials and software deliver the highest security by incorporating critical visual and logical technologies for trustworthier authentication and to help deter tampering and forgery. The latest software also makes it easy for administrators to synchronise card encoding information with the student enrolment database, eliminating the possibility of errors while simplifying future changes that might be required.

HID Global's FARGO® HDP® printers exemplify the benefits of High Definition Printing (HDP) printing technology. Unlike traditional Direct-to-Card (DTC®) printers, HDP printers actually print a high-resolution image to a transfer film, which is then adhered to the card. This process provides exceptional image quality and eliminates the possibility of print head damage caused by direct contact with the card's contact chip. While some university card services teams may be nervous about printing smartcards, it is not very different than printing legacy technology based cards, with very similar workflow processes. Secure issuance solutions should be intuitive and require little or no training. Printers should also be field-upgradable so they can meet new requirements, as student ID systems' needs change and evolve. And finally, the software application has to support multiple uses, as well as feature easy-to-use card templates that streamline the card creation process, including synchronising all data used in the card.

It's also important to consider the trade-offs of going with a low-end printer versus one that may cost more initially, but reduces expenses over time. For instance, high-throughput solutions such as HID Global's HDP8500 industrial card printer can run operations in parallel, speeding issuance by encoding one student's card while printing another. The HDP8500 also supports both centralised and distributed printing, so universities can pool two or more desktop units at the card services office for large-volume, centralised card runs, as well as individual units at locations such as residence halls where authorised users can print and issue cards to students. This not only alleviates long card pickup lines but improves student convenience.

In addition, students, faculty and staff are not the only people on campus – any university physical access control system platform must also support visitors. Proper visitor registration is one of several important security safeguards that all universities should address, and protecting campus residence halls is of particular concern. When setting up a visitor management system, it is

important the right printer is selected, with the appropriate features and suitable levels of reliability and durability. Also, depending on the campus environment, it may be advantageous to specify vandal-resistant readers.

We are also increasingly seeing visitor management integrated with the university's access control systems to provide a completely secure solution. The University of Arizona has such a campus colleague/visitor system in place. Guest information that is entered into the visitor management database is seamlessly passed to the card office ID management system. The visitor is now eligible for card issuance. The same campus card is issued to the visitor with "tap and go" technology for door access. When the visitor is no longer active in the system, the card is deactivated for keyless access and other campus services.

Another good investment is printers with built-in programmers/encoders, which combine what were previously multiple processes into a single in-line card personalisation step. With this approach, only one automated step is required to synchronise pre-programmed data on the card's electronics with personal data printed on the outside of the card. Users simply submit a card into a desktop printer equipped with an internal smart card encoder, and the card is personalised inside and out. This speeds issuance while eliminating the risk of human error during manual entry, which can lead to large numbers of cards being thrown away. Field-upgradable units enable universities that already own a card printer to add an encoder in the field so they can leverage smart card benefits well into the future. When they're ready to maximise their smart cards' functionality, they'll already have the smart issuance part of the equation figured out.

Protecting students, staff and property is one of the university's most important responsibilities. Contactless smart card technology delivers not only the highest levels of security, but also the greatest efficiency and convenience. By investing in a single-credential access control system that enables universities to print multi-purpose cards themselves, they are able to tailor their card distribution based on their own needs, while at the same providing adequate protection from outside threats.

Listen to HID Global's webinar if you want to learn how to create unique student experience on and off campus

Serra Luck, is Director - End user and Consultant Business, EMEA with HID Global

For more HID Global news, visit our Media Center, read our Industry Blog, subscribe to our RSS Feed, watch our videos and follow us on Facebook, LinkedIn and Twitter.

2014 AGM and Winter Seminar— in pictures

Former MP and ASIS member, Rt, Hon. Bruce George accepting his ASIS UK Veteran certificate.

Andy and speaker, Nigel Stanley

Professor Peter Neumann

Retiring Chapter Treasurer Craig Pickard was touched by the effort made in packaging his farewell gift.

Andy Williams CPP presenting Commissioner Adrian Leppard QPM with the Chapter's Mervyn David Award

Good business all round at the Total Security Summit

As a security professional, your role involves knowing how to avoid and effectively overcome a whole raft of technological and practical issues, such as Access Control, CCTV, Risk Mitigation, Intruder Detection, and much more. However, with new security threats being discovered daily, when do you really get the time to consider what is right for your business?

Well, the Total Security Summit may just be the opportunity you need! This two day security industry focussed event, held on 16th and 17th March at the Radisson Blu Hotel, London Stansted, provides the ultimate business connections experience for over 100 attendees, as well as an inspiring seminar programme presented by these high profile speakers:

- Ian Noble, National Fraud Investigator at B&Q
- Mark Godsland, Safer Cyber Harm Reduction Advisor at Gloucestershire Constabulary
- Lisa Greenwood, Lisa Greenwood Consultancy
- Matt Etchells-Jones, Consultant at Business Crime Reduction Partnerships
- John Spratt, Senior Partner, Head of Company Commercial at Spratt Endicott Solicitors
- Matthew Phelps, Managing Director Eaton's Security Business

In addition to the seminar programme, attendees have the opportunity to discuss security topics within a series of match-made face-to-face meetings and unparalleled networking sessions.

According to previous attendees, Total Security Summit provides "an effective format for instigating new relationships" and here are more opinions from past delegates and suppliers:

TOTAL SECURITY SUMMIT

"The TSS gave a relaxed and unique way to network and target specific vendors"
Partnership Assurance

"Well run and informative two days' excellent opportunity to understand the products on a one to one saves much time rather than booking appointments during working hours" *River Island*

"One of the best organised events I have attended in a long while thoroughly recommended" *Jaguar Land Rover*

"An excellent forum and great environment for meeting suppliers of security products and services and networking with peers"
Turner Broadcasting

The Total Security Summit is brought to you by Forum Events which has nearly 20 years of experience in organising B2B focussed meeting opportunities. VIP delegates are able to quickly identify the best solutions for their business' projects; whilst suppliers can boost sales pipelines by securing new business.

Kirsty Groves, Marketing Manager at Forum Events, said: "We put a lot of work into matchmaking, finding the right suppliers for delegates with purchasing power. In putting people together who are ready to do business, we've cut out so much of the time-wasting that is so often associated with supplier procurement and new business development."

To book your place and to find out more about the Total Security Summit, call the events team on 01992 374100, email tss@forumevents.co.uk or visit the website www.totalsecuritysummit.events

Lenel to showcase Integrated Solutions at IFSEC 2015

Lenel Systems International, a provider of integrated access and video solutions, will present Prism, its open Internet protocol (IP) video management solution (VMS), at the upcoming International Fire and Security Exhibition and Conference (IFSEC).

Lenel Systems International, a provider of integrated access and video solutions, will present Prism, its open Internet protocol (IP) video management solution (VMS), at the upcoming International Fire and Security Exhibition and Conference (IFSEC). Prism is based on an advanced, intuitive and operator-friendly user interface and features OnGuard compatibility. Lenel is a part of UTC Building & Industrial Systems, a unit of United Technologies Corp. (NYSE: UTX). Offered in three configurations (standard, professional and enterprise), and available as a stand-alone VMS or integrated with OnGuard, Prism is scalable, flexible and reliable to meet evolving video surveillance needs. Prism fits in an enterprise video platform by offering customers a single user-friendly VMS for small to large installations, whether they are using Lenel network video recorders or UltraView recording engines.

"By combining OnGuard and Prism industry-leading products with more than 100 open access alliance partners (OAAP), close to 100 OAAP-certified products and supporting more than 300 third-party cameras, customers can tailor the Lenel solution according to their specific security demands," said James Wheeler, Regional Director, Lenel UK and Ireland.

To stop or not to stop, that is the question?

It's a fair cop Guv!

I don't suppose an SIA arm banded Security Guard in your local shopping centre has heard that phrase recently. The days of the long arm of the law with a firm hand on the shoulder of a tea leaf, being enough to put a halt to any wrong doing would appear to be a thing of the past. Even the Police do not command the same respect their predecessors' did ''back in the good old days''. Actually, that is a myth, there may have been fear, but respect went out with National Service! The small time criminal fraternity are a far more confident breed than ever before and this makes a Security Guard's job a very difficult one.

I speak from personal experience of course, having spent many years chasing down shoplifters with the single minded intention of bringing them back with their ill gotten gains in tow. As KPIs go, this was pretty much the only one that mattered. There was even a league table with the amount of bodies hauled back and a separate one for the stock recovered. So who could blame us for waiting impatiently for those immortal words to come across the airwaves from a plain clothes Store Detective (I've got a job going down!) At that point, your cup of coffee and roast dinner ended up on the ceiling, just because of the possibility that there may be a chase involved. I know what you're thinking . . . what a great use of time . . . not!

How to get it wrong!

I remember one such call. Off I went to back my guys up, fully expecting it all to be over quick enough to finish my coffee whilst it was still slightly warm. Not the case this time, having found myself clinging onto a credit card fraudster, who for some strange reason wasn't keen to accompany me back to the holding room within a well known department store. In fact, he was so keen not to come back with me, we ended up rolling around on the ground with him taking a generous sized chunk out of my forearm with his beautifully polished set of gleaming white and gold teeth. Of course I didn't stop him on my own.....I had my ever keen but rather inept team members hanging on to each other with their eyes closed.....that was helpful! Whist all this was going on, the goods that had been "purchased", I use the term loosely, were being driven off by his rather attractive female accomplice. Now in my defence, I was very new to the role and my team had little or no training with how to detain a suspect correctly. You can be assured, that changed very quickly and the policy of this particular company was given far more weight in terms of how it dealt with detaining people.

If you're out of action, who's protecting the stock?

So, a trip to A&E for myself and one of my Keystone Cops, all for the recovery of a big fat zero. Admittedly, this was a comedy of errors, one that unfortunately I was leading. However, how many other incidents have there been across the country where well meaning shop staff have put themselves in danger all for the sake of a £20 jumper. I would suggest this is a daily occurrence. The fact is, the current batch of undesirables will be far more keen to get away than you are to bring them back . . . after all, they are potentially losing their liberty. So, surely this raises the question "what should we do?''

Can we stop it being stolen?

Having worked on the customer facing side of several retail giants as well as running their security teams, I find myself asking this question of staff at virtually every presentation I give on loss prevention. The response varies, but on the whole, sales assistants want to know that a shoplifter will be stopped, detained and the Police called. This is understandable, as they are the ones being made to look stupid by these bad guys. When I hear this, I generally ask one question: how do we stop bad people stealing from us?Of course, there isn't a straight forward answer! That said, it doesn't do any harm to plant seeds in the minds of those on the front line. Shouldn't the question be "what is more likely to put someone off stealing"? The fact that they could get caught and have their liberty taken from them, or make it so difficult to steal that they simply go elsewhere. A few years ago, there was a study performed with career shoplifters, asking this exact question. "What would put you off stealing from a particular store"?The majority of the interviewees said "knowing I have been seen by the sales assistant". Uniformed security guards hardly got a mention. If you think about it, you approach a customer . . . if they are honest they are usually happy to have been seen and are more likely to stay in the store and spend their hard earned cash. However, a dishonest person is doing everything not to be seen, hence the hoodies and dodgy fake police sunglasses. Of

course I'm type casting, but many will agree, good old shoplifters like to try and blend in, but don't always make a great job of it! There are of course the ones who are very clued up and even the best store dec has trouble spotting them.

Deter or detain?

A retailer will often employ uniformed security guards to act as a deterrent, and if they are standing by the doors next to the EAS barriers, that arguably is a great deterrent.However, what if every sales assistant isn't just thinking about making that sale? What if they approach customers, even the shifty ones? One of two things are likely to happen . . . the potential shoplifter will either try and front it out, smile and say''no thank you'', or, maybe give you some attitude. Either way they normally walk out. Ah yes, but if you change your policy and try to deter every shoplifter rather than detaining them, will you be seen as an easy touch? In all honesty, yes you will. However, if you just stop every shoplifter and that means spending time watching them, ensuring you see the selection, ensuring you see them conceal the goods, ensuring they still have the goods on them when they leave the store; then make the arrest, leaving you vulnerable to possible violence, get them back to the store, keep a close eye on them whilst waiting for the Police, write statements, wait for a court date many months away, go to court which means you're not in the store stopping more shoplifters. The man hours involved with detaining a shoplifter are hugely expensive, especially if you have to pay overtime to cover you whilst you're out giving evidence. If you are a retailer that is just doing one or the other, ask yourselves the question, should I stop or not!

One size doesn't fit all!

The way I see it, customer service and security go hand in hand. A great Security Guard will always give fantastic service to a genuine customer or one that is not so genuine. As a customer, would you want to be approached by a uniformed guard? . . . I would suggest not! Firstly, it could look like you're being accused of something in a very public arena, but more importantly isn't that what retailers are paying sales assistants to do. Arguably, uniformed Security Guards on the shop floor don't really work for deterring theft. They stand out like a sore thumb, which means eagle eyed shoplifters know where they are. It doesn't take a genius to realise not to steal when you see a uniform. So, steal something when you don't see a uniform. However, if there are no uniforms, your guess is as good as mine who is security and who is a sales assistant. If you study the shop floor from above (CCTV) as I have done, you will see suspicious people leave the store just because they have been acknowledged. That could be as subtle as a smile or a nod from an assistant. This of course is a win win for retailers, as stores will be judged by test shoppers on their ability to acknowledge every customer.

Get the balance right, you'll end up the winner!

Don't get me wrong, if you don't stop shoplifters anymore, you could end up with shrink figures that have a very adverse affect on your bottom line. You most definitely do not want to be seen as an easy touch, as that will leave you open to every local scrote paying you regular visits. As with anything, you want to have a balance. Time spent training your staff to acknowledge customers and making that second nature will reduce your losses and increase your sales, that is an absolute guarantee. At the same time, ensure your Security Guards are dressed the same as your assistants, that way they can do their job just as well but can also give advice and great service.

In summary, the more shoplifters you can deter, the less stock will walk out of the door. Detain when appropriate, but only when the odds are very much in your favour and that means, do not put yourself in undue danger for the sake of a few quid. Time looking into patterns of fraud and theft and finding alternative ways to protect that stock, is far more of a proactive strategy than simply waiting to react to incidents. After all, bottom line profit and happy customers are what really matters, aren't they?

Andy Leon is a retail manager with a career spanning 30 years with names such as John Lewis, the Burton Group and B&Q. He found his niche within Security and has used this, along with a passion for customer service to increase stock availability whilst driving down loss. His desire to share knowledge is infectious and he strives to raise security awareness amongst those on the front line every day.

Viewpoint: 'The Licensing of Private Investigators' – Chris Brogan

The Home Secretary Theresa May has finally decided that private investigators will require a licence under the Private Security Industry Act 2001 to take effect some time in 2015.

The fine details of this proposed regulation have yet to be released, but while we're waiting I thought I might share the following thoughts with you.

Over the years there has been a great deal of difficulty in establishing a definition of a private investigator and/or what he/she does (http://www.statewatch.org/news/2012/jul/uk-hasc-private-investigators-report.pdf). For the purposes of this article I'm suggesting it's likely to be a non law-enforcement or public authority investigator.

Section 3 of the Private Security Industry Act addresses the offence of not having a licence when engaged in a licensable activity. "A person guilty of an offence under this section shall be liable, on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding Level 5 on the standard scale, or to both" (Section 3 (6) Private Security Industry Act 2001).

Now there's nothing new in that. Any of those companies or individuals that have already had to comply with the Act will be familiar with these offences. The point that I want to address here is around 'licensable conduct' and what that looks like in the real world.

Section 3 (2) lists ten activities of licensable conduct. What is common throughout is that the conduct has to be in connection with a contract. If there isn't a contractual agreement with the person/organisation that the licensable activity is being provided for then you don't need a licence. The old chestnut of in-house security officers not being licensed readily springs to mind.

Contracts in English law

A contract in English law requires four components. There has to be an offer. Clear and unambiguous. There has to be an acceptance of that offer. Clear and unambiguous. Consideration has to change hands. This does not mean money. Consideration is just something of value. It could be a service for a service. The contract also has to be considered legally binding between both parties.

Now consider the position of ABC plc, a large UK bank/corporation with lots of subsidiaries and/or associate companies. The investigation department is part of the head office structure and they supply investigative services to their branch offices and their subsidiary and associate companies.

These subsidiary and associate companies are separate legal entities under UK company law. (Companies Act 2006) ABC plc can sue or be sued by their subsidiary/associate companies. These individual companies, for reasons of motivation/individual corporate structure, are independent profit centres and their incomes and expenditure are reflected in their annual balance sheets. Look at any set of balance sheets of a plc company and you're likely to see reference to balances due to and/or from subsidiary or associated companies.

I suggest that the above scenario is very familiar with any reader who has worked for a large concern. These concerns are, probably through ignorance, running risks that could have consequences of a financial, reputational and legal nature. If these risks ever mature where will the blame lie? Who owns the risk where security-related issues are concerned?

These investigative services are being supplied under contract and, as such, it's my submission that:

- *The individuals providing this service should be required to hold a licence. Section 3 (2)(b) of the Private Security Industry Act 2001.*
- *The directors of ABC plc – the company that's providing these services under a contractual basis to their associate/subsidiary companies – should be licensed. Section 3 (2)(a) of the Private Security Industry Act 2001. That includes the non-executive directors whether they have a seat in the House of Lords or not.*
- *The managers of these companies providing these services should be required to hold a licence. Section 3 (2)(d) of the Private Security Industry Act 2001.*

Opening the floodgates of litigation

Now, if my submission is correct then the investigator actually providing the service is likely to be committing a criminal offence and could be prosecuted. If he is he runs the risk of not being able to obtain a licence in the future because of the negligence of his employers who failed to recognise their responsibilities under this legislation. His employers owe him a legal duty of care and in this scenario they would be in breach of that legal duty of care.

I suggest that it would require only one successful case for the floodgates of litigation to open with the likes of Liberty

and/or Big Brother Watch clamouring to offer their support.

This isn't the first time that I've raised this argument, albeit previously in relation to manned guarding. I have on nine separate occasions raised these points with the Security Industry Authority (SIA) at varying levels, all the way to the top. On the last occasion an SIA official told me that he would look in to it and would come back to me. I told him that eight of his colleagues over the years had told me that same story and they hadn't. His forceful reply was that "he would." That was some time ago and I wait patiently.

Next year, private investigators will require a licence. Life is tough enough for them as it is. This will be the third regime to which they will have to submit control of their activities (The Office of Fair Trading – Consumer Credit Act 1974 as amended by the Consumer Credit Act 2006, the Information Commissioner's Office – Data Protection Act 1998 and the Security Industry Authority – Private Security Industry Act 2001).

These investigators will be competing on an un-level playing field with their in-house colleagues, I suggest that they'll have little compunction in drawing these potential illegal activities to the attention of the authorities and any other bodies whose interests may be furthered by these revelations.

How can you manage a risk if you don't know what it is?

I hope that I've helped you identify some of the risks that you and your organisation may already be running. There are many more that could result from the above scenario. Risks breed risks.

It's a well known legal maxim that the unforeseen consequences of legislation far outweigh the foreseen consequences. This doesn't mean that we have to be unprepared.

Chris Brogan
MA LLM MIBA FSyI,
Partner, B&G Associates
020 8567 6944

This year the Commando Spirit Appeal is again on a mission to raise serious funds for the work of the Royal Marines Charitable Trust Fund. The Commando Spirit Series of challenges offer participants the opportunity to test their mettle against true to life Royal Marines tests and we are now looking for people to sign up to show their courage for those who risk their all.

THIS YEAR OUR CHALLENGES INCLUDE:
Escape The Dunker – the underwater escape training
The 30-miler – Survive The Yomp in the rugged Scottish Highlands and
Take The Leap – the commando abseil from iconic buildings across the UK.

FACEBOOK: http://goo.gl/za1Hc4
PINTEREST: http://goo.gl/EBaoW5
TWITTER: http://goo.gl/FYwG4Y

Test your limits with @CdoSpirit challenges and raise funds for @RMCTF
Have you got it? http://goo.gl/j5Lfwl

However you help us, you'll be contributing to the Commando Spirit Appeal for the RMCTF, supporting Royal Marines and their families in need.

ROYAL MARINES CHARITABLE TRUST FUND

THESMA ANNOUNCES NEW 'STUDYFLEX' PROGRAMME FOR ASIS CPP, PSP, PCI PREPARATION PROGRAMMES AND ACCREDITED SECURITY MANAGEMENT COURSES

At TheSMA (The Security Management Academy) we are not only security trainers but security practitioners. As such we understand that it is often difficult to juggle work and study commitments; and occasionally impossible to guarantee attendance in the classroom, especially when resources are stretched.

Designed with the busy security manager in mind, TheSMA has launched their unique 'Studyflex' programmes allowing those with busy work schedules up to twelve months to complete their course through a combination of home study and a choice of course dates and locations.

Our programmes are led by industry renowned trainers, Barry Vincent MA, MSc, CPP, PCI, FSyI, and Bob Knights MBE, MSc, CPP, PSP, SIRM, FSyI, who have successfully delivered ASIS certification programmes for over 5 years.

The CPP and PSP programmes commence with an initial period of tutor-supported self-study, with the completion of set assignments. Barry and Bob will provide full guidance, direction and support for the duration of this period.

There will then be an intensive 5 day classroom and review, geared towards consolidation and testing of knowledge with focused tutor-led revision, culminating in a full mock exam of 200 questions (conducted under exam conditions). The tutor will highlight any areas for additional focus to equip you for success in the examination.

These flexible programmes have been designed to offer you the maximum support towards attaining this high level certification. You will benefit from the full support of the experienced TheSMA training team, its expertise in the knowledge of the certification syllabi, valuable revision aids and the flexibility to tailor the learning process to suit your individual requirements.

THESMA
the security management academy

We are pleased to offer twelve months' subscription to the CPP and PSP programme to new and returning Chapter members for £1250 plus vat.

Subscription also includes access to our operational security centre for advice and mentoring, through our sister company Security Exchange Limited. Security Exchange comprises a core team of security specialists managing a worldwide panel of experienced consultants; and supported by 24/7 multi-lingual call centres in the three principal time zones; Europe, The Americas and Asia-Pacific.

Please contact Caroline Bashford, Director of Training at TheSMA, at cb@thesma.co.uk or call her on +44 1491 699685 to find out how TheSMA's 'Studyflex' programme can help you manage your studies more effectively.

Are you keeping up in salary stakes?

Peter French MBE CPP

Most HR functions cannot access the same salary data for the security risk discipline that they can for most traditional functions. Pay increases for most corporate security functions in 2014 have increased on average by 3.2% in the most industrialised countries in Europe. Good news is that bonus pools are increasing across a number of sectors including financial services, extractives, oil & gas, pharmaceuticals and logistics. Bonus payments to respondents have increased by an average 25%. Executive salaries across many functions in 2015 will remain relatively flat in Northern Europe, whilst salaries in Southern Europe, which have been subject to reductions in the past 5 years, will show increases in the coming year.

2014 has seen Cyber security become a hot button item on most company board members' dashboards. Over 50% of CEOs consider that they lack the expertise in-house to deal with a serious issue. With C-suite executives seeing themselves as serious stakeholders in the problem of cyber risk most complain about the lack articulation of the issues and subject matter. There are also major differences in the way organisations deal with events, a recent CSO roundtable survey found that less than 27% of respondents have an in-house forensic capability; over 60% had an investigations function, mainly through analysts, and less than 11% would classify these as cyber investigators. In Europe we have had a number of incidents where banking organisations' IT spending, even those under regulatory oversight, has been very poorly invested, creating organisations that can be a danger to customers and shareholders. The emergence at JP Morgan that recent data hacking was committed through vulnerabilities in their 3rd party suppliers is a key example where organisations would in the past be aware of their own strengths, but a layering of suppliers, who do not share information, is causing quality rifts in service security. Comment from regulators is recognising that cost reductions programmes are driving out experience as well as quality.

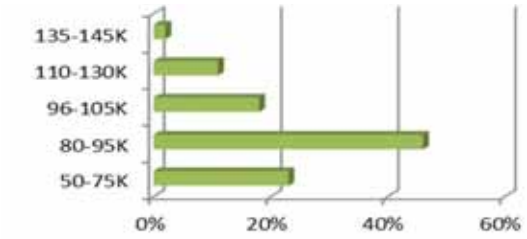
Fraud prevention, in the physical aspect, is around robust approvals, understanding geographic trends, criminal demographics and the ability to respond quickly; attributes that you cannot readily see in the virtual space.

How can you increase your income?

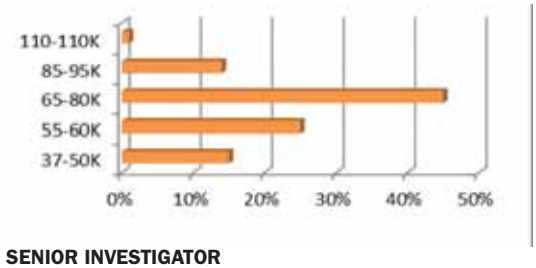
You could change jobs, but is there that much movement in the market? Can you change the perception of the role that you are doing? Can you converge your role with those who offer greater value to the corporation? Professionals who do not have indicators on the dash board run the risk of being irrelevant to the organisation, and it then proves difficult to demonstrate value. Those who are successful in the boardroom are those who understand and resonate from the corporate business environment and credo.

SSR® Personnel incorporating Executive Profiles is a dedicated recruitment consultancy for security risk and engineering.

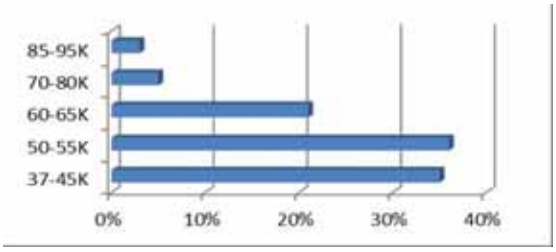
EUROPEAN SECURITY HEAD
Regional reporting, policy implementation, promulgates corporate policy. Responsible for physical and information security. Budgetresponsibility £5m - £10m



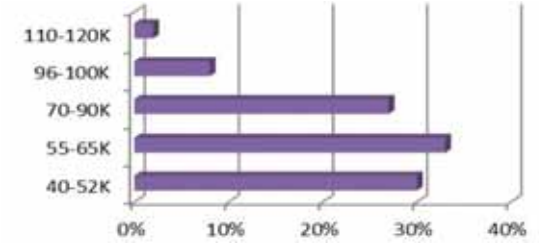
NATIONAL SECURITY HEAD
Responsible for all physical aspects of corporate security and maintaining standards across an estate. Budgetresponsibility £2m - £10m.

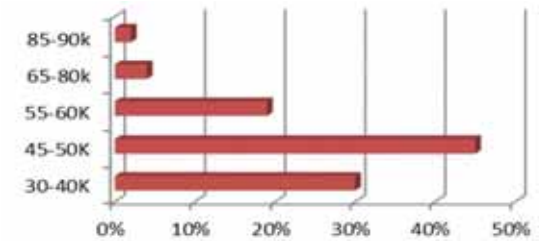


SENIOR INVESTIGATOR
Responsibility for more than one country's operations. Active across all security breaches, due diligence, product diversion, counterfeit and auditing functions for the corporation.



REGIONAL INVESTIGATOR &DUE DILIGENCE MANAGER
Supply chain management implementing corporate procedures.





MAIN HQ SITE SECURITY MANAGER
Physical and information protection, proactive, local policy implementation and development. Budget responsibility £2m - £5m+.

(Cyber) Security: where does it fit in Michael Porter's 'Value chain'? - Alan Jenkins

One of the biggest challenges facing the security community (whether practitioner, vendor or service provider) has been how to convince the business leadership of the value of any investment into its security effort, whether it is protecting infrastructure, people or – more topical, perhaps – information and particularly intellectual capital, eg R&D outputs, on which future business revenue is dependent. The lack of a quantifiable 'value-add' from security outputs has frequently led, for example, to physical security being seen as a secondary activity of Facilities Management, while HR frequently resists any suggestion that it should own the background checking of staff, despite the overlap with the on-boarding process, and IT is often outsourced with too little regard to security provisions. This lack of perceived value from security is despite its having been identified as one of the Principles of War by such luminaries as Sun Tzu, von Clausewitz and Liddell-Hart. Most recently, the 2011 edition of British Defence Doctrine categorises Security as:

" . . . balancing the likelihood of loss against achieving objectives. It demands managing risk, protecting high-value assets and resilience. Security does not imply undue caution or avoiding all risks, for bold action is essential to success. Neither does it demand over-committing our resources to guard against every threat or possibility, thereby diminishing relative fighting power."

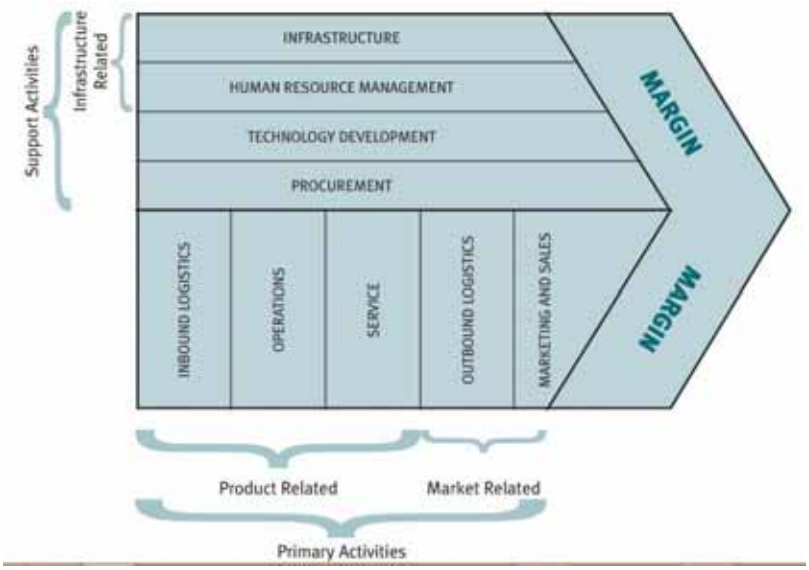
In the same document, it defines cyberspace as

" . . . the interdependent network of information technology infrastructures - including the Internet, telecommunications networks, computer systems, as well as embedded processors and controllers - and the data therein within the information environment. As the world is increasingly interconnected with an associated growth in the use of cyberspace, (the UK's) ability to operate in cyberspace is vital to national interest and enables (UK) national security, prosperity and way of life. Defence is increasingly dependent upon cyberspace and can expect adversaries to exploit this dependence. The UK government assesses the cyber threats to its interests and mitigates these through resilience measures, awareness and rusted partnerships. Activities in cyberspace are an essential element of our routine business and are fundamental to planning and conducting operations."

Both can be translated into the commercial realm with very little change required, whether your enterprise is in the business-to-business or business-to-consumer space, it is likely that both the Internet and Intranet play a large part in the day-day operations of most businesses. Any disruption, whether from an internal or external source, is likely to have a negative impact on business outputs, with an attendant cost and, often, reputational damage also. Increasingly, it is the latter that is getting the attention of Board members - both Executive and Non-Executive - and other stakeholders, including Shareholders, Market analysts and partners up and down the Supply Chain, not to mention national governments, legislatures and regulators. However, much of this attention is on reducing risk as opposed to adding value and is, therefore, a secondary driver for business where the primary driver is that of growth and, where applicable, adding shareholder value.

So, where does security fit in our business models and respective commercial strategies? It could be argued that, all too often, security is an after-thought for business, a 'reluctant' spend and almost invariably a 'cost centre', coming off the bottom-line with little or no contribution to the top-line. Given that it is almost universally acknowledged that security must use the language of business when seeking to make the case for further investment, who can we cite in support of our pitch, whether in the elevator or the Board Room? The list is not long and therein, perhaps, lays our greatest weakness – the value of security is neither recognised nor appreciated by the business until, perhaps, it is too late . . .

In his 1985 publication 'Competitive Advantage: Creating and Sustaining Superior Performance', Harvard Business School's Professor Michael Porter introduced the value chain as a tool for developing a competitive advantage. This seminal work has influenced many MBA students since its introduction and thereby been reflected in many business strategies since.



Topics include:

Sharing of value chain activities among business units.

Using value chain analysis to develop low-cost and differentiation strategies.

Interrelationships between value chains of different industry segments.

Applying the value chain to understand the role of technology in competitive advantage.

Porter concludes by considering the implications for offensive and defensive competitive strategy, including how to identify vulnerabilities and initiate an attack on the industry leader – something which should be of particular interest to security. See Figure 1 on previous page.

The goal of these 'Primary Activities' is to create value that exceeds the cost of providing the product or service, thus generating a profit margin. Any or all of these primary activities may be vital in developing a competitive advantage but it should be remembered that they likely vary by industrial sector and are best considered at the business unit level. For example, logistics activities are critical for a provider of distribution services, and service activities may be the key focus for a business offering on-site maintenance contracts for office equipment.

Porter went onto identify four generic categories of 'Support Activities', the details of which are industry-specific and frequently conducted at the corporate rather than business unit level:

1. *Procurement - the function of purchasing the raw materials and other inputs used in the value-creating activities.*
2. *Technology Development - includes research and development, process automation, and other technology development used to support the value-chain activities.*
3. *Human Resource Management - the activities associated with recruiting, development, and compensation of employees.*
4. *Business Infrastructure - includes activities such as finance, legal, quality management, etc.*

These 'Support Activities' are often viewed as "overhead" but some businesses have successfully used them to develop a competitive advantage, e.g. to develop a cost advantage through innovative management of information systems.

Your attention is drawn – if needed - to the absence of any mention of security as either a Primary or Support Activity and therein lays the rub.

We, the security community, frequently talk about security as being a horizontal activity cutting across pretty much all business activities but does anyone else recognise this supporting activity as being critical to success? Despite its merits, the idea of security convergence has struggled to gain widespread traction perhaps because its value-add has been less than clear. It seems that Porter did not consider it worthy of such recognition, unlike Quality Management for example, so is it any wonder that our business leaders view our contribution in a similar fashion? It falls to us, then, to better argue our case for increased 'value-add' recognition if we are to support business growth and change the still widely-held view that security exists to get in the way and say 'No'. We need to analyse the myriad ways in which security supports at least, if not enables, the business to succeed – 'Value Chain Analysis' with a focus on security.

In order to better understand the activities leading to a competitive advantage and hence value-add, Porter begins with the generic value chain and then goes onto identify the relevant business-specific activities. Process flows are mapped and these flows used to isolate the individual value-creating activities. Once the discrete activities are defined, linkages between activities should be identified. A linkage exists if the performance or cost of one activity affects that of another. Competitive advantage is obtained by optimising and co-ordinating linked activities to maximise both efficiency and effectiveness. The business' value chain should link to the value chains of upstream suppliers and downstream buyers. The result is a larger stream of activities known as the value system.

The development of a competitive advantage depends not only on the business-specific value chain but also on the value system of which the business is a part. This also links to current enterprise security thinking with respect to the supply chain as more than one primary supplier has been compromised by upstream contributors in respective supply chains.

This is a topic that merits more development than is possible in this 'starter-for-10' article.

This article first appeared in Risk UK Magazine

http://en.wikipedia.org/wiki/Principles_of_war

JDP 01 (Ed 5) UK Defence Doctrine

Porter, Michael E. (1985). Competitive Advantage. Free Press. ISBN 0-684-84146-0.

http://www.quickmba.com/strategy/value-chain/

'Alan has accrued some 25 years' experience in all facets of security, law enforcement and, latterly, information assurance and security risk management, with increasing focus on 'value-at-risk'; having served for some 17 years as a Royal Air Force Police officer. He has held 3 CSO/CISO positions since 2008, most recently at Babcock International Group, where he was their first CISO and latterly Group Security Co-ordinator also. He is the UK Chapter Lead of Convergence and Cyber Security.

Benefits of Big Data Analytics in Security – helping Proactivity and Value creation

— Dr Vibhor Gupta PhD

Enterprise security at most organisations is tasked to deal with all aspects of threats and risks which arise due to nature of their business, geopolitical situation and socioeconomic conditions. Given the spate of recent incidents globally, a lot of attention is drawn towards cyber security. However, as most organisations recognise, this attention is not limited to only the cyber side of security but all elements, which relate to protection of information and people at their organisation.

So, for instance,

Policies around access to critical areas (physical or virtual) are defined, implemented and monitored more tightly

To reduce the probability of 'insider threat', organisations are including measures to vet and audit each individual person (or logical account) who have requested or already have access to these critical areas

Boundaries of these physical or logical areas are finely defined taking into account local operations and industry regulations

All aspects of security such as cyber, data, people, assets and site are being looked at from a holistic perspective with reference to the core business objectives

In addition to this, Security departments are becoming (or increasingly intending to be) more proactive to identify risks and threats as opposed to being reactive to issues which might have already impacted their organisation's business, people and/or reputation. In this interest, various tools and technologies are deployed to capture data across the aforementioned areas. And with most of these technologies now connected to the network, it's becoming relatively easier to integrate them as it offers a cost effective alternative to manage various operations which otherwise are divided across different people and systems.

Given the wealth of data which security departments are capturing through their various activities or systems, they are using it in novel ways to identify and resolve risks (exceptions) which otherwise would go unnoticed till they manifest into issues. The principles of these novel approaches are seldom classified into 'Security Intelligence' and 'Behavioural Analytics'. To share a few examples:

A global bank comprising of a large workforce (>150K people) and over 100 sites across the world was keen to identify instances where their people were 'remote' logging into their IT systems despite being (physically) inside their premises. Such exceptions relate to possible duplication of an identity record, which is a serious threat. As the bank discovered, the 'best' (cheap, quick and replicable) way for them to approach this was to apply simple principles of data integration and visualisation across their base logical and physical access control systems. By doing so, the security team was notified of any such exceptions in real time. This allowed for an instant investigation and helped the bank mitigate their risk significantly

A fortune 500 organisation had multiple reported cases of expensive equipment stolen from different buildings around the main campus area. They suspected the thefts were occurring after hours but analysis of access records from their physical access control systems alone wasn't very helpful. They had hundreds of people working late at that site on a regular basis so they were unable to identify a manageable number of suspects. But, by applying analytical intelligence to an integrated set of time and attendance data; and physical access data, they were able to resolve this.

They first defined a 'usual' behaviour o f an individual and groups of individuals, i.e. which areas they access the most and at what times.

Then they looked for exceptions, i.e. if certain individuals or groups accessed certain areas at times, which fell outside their 'usual' behaviour.

By doing this analysis, a single employee stood out and his access pattern also coincided with the thefts. The next time the employee entered a new area after his normal hours, the Security Operations team was notified, following which a guard was sent to inspect the building. The thief was caught red-handed. This approach not only helped them resolve a mystery but also provided them with a strategy to prevent similar activities in the future.

A highly secure Research and Development organisation spent enormously each year to perform background checks for every person accessing their campus. Reduction of their security budget led them to change their policy such that they decided to perform 'risk assessments' on each individual and they re-ran checks only on those who represented the highest risk. However, this simply led to a cut in the frequency of checks and raised their risk significantly. So it was critical they re-defined the way in which they derived their 'risk assessments'.

They started by factoring each individual's level of access, the time they had been with the organisation and the time since they last went through a background check. This information was coupled with their known 'behaviour' (which areas they access frequently and at what times) to compute a 'Risk Score'. Background checks were mandated for individuals with a high Risk Score and those who showed a sudden increase in their overall Risk Score. This helped a great deal in maintaining their high security levels (no issues reported since) whilst reducing their operational cost by approximately 85%.

There are several other use cases, which highlight the benefits and values which security departments are creating using the principles of 'Security Intelligence' and 'Big Data Analytics'. To outline a few,

Site utilisation metrics – to what degree is a site being used?

Key performance indicators – how well are the security operational teams doing based on their service level agreements.

Impact analysis in case of changes such as change of security policies or existing technologies such as access cards and access control systems.

Supporting the green agenda by reducing the energy usage in areas which are not used heavily based on the data analysed.

However, all great ideas require a successful execution (implementation) for their 'greatness' to be recognised. During this study we learnt of the following tenets, which were key to successfully achieving the above:

Identify the use cases, which should be addressed through the endeavours of 'Security Intelligence' or 'Big Data'. Base these on the experiences of known risks, threats and exceptions.

Look for extensible solutions that can contribute to the bigger picture if that should become necessary. Scalability and extensibility are easily achieved when out of the box solutions are deployed as opposed to customised ones. This helps organisations protect their investment as such solutions can be geared to handle changes of other third party systems or business processes.

Partner with systems vendors that specialise in the security vertical and connect to applicable systems (such as Access control, logical human resource systems, security devices) in a non-customised/ non-bespoke manner.

Avoid generic "Big Data" solutions from vendors that don't understand security. Domain knowledge is very important given that one size doesn't fit all. Domain knowledge coupled with reference-able experience of a solution provider implied cheaper, shorter and scalable implementation.

With the above it's evident that security departments globally are recognising the opportunity to be a business enabler and are aligning their objectives so their organisations can run efficiently. This is a welcome deviation from the traditional view of security being a reactive and investigative team only which was unfairly labelled as a 'cost centre'.

Dr Vibhor is the ASIS UKChapter Technology Lead and can be reached at vg@asis.org.uk

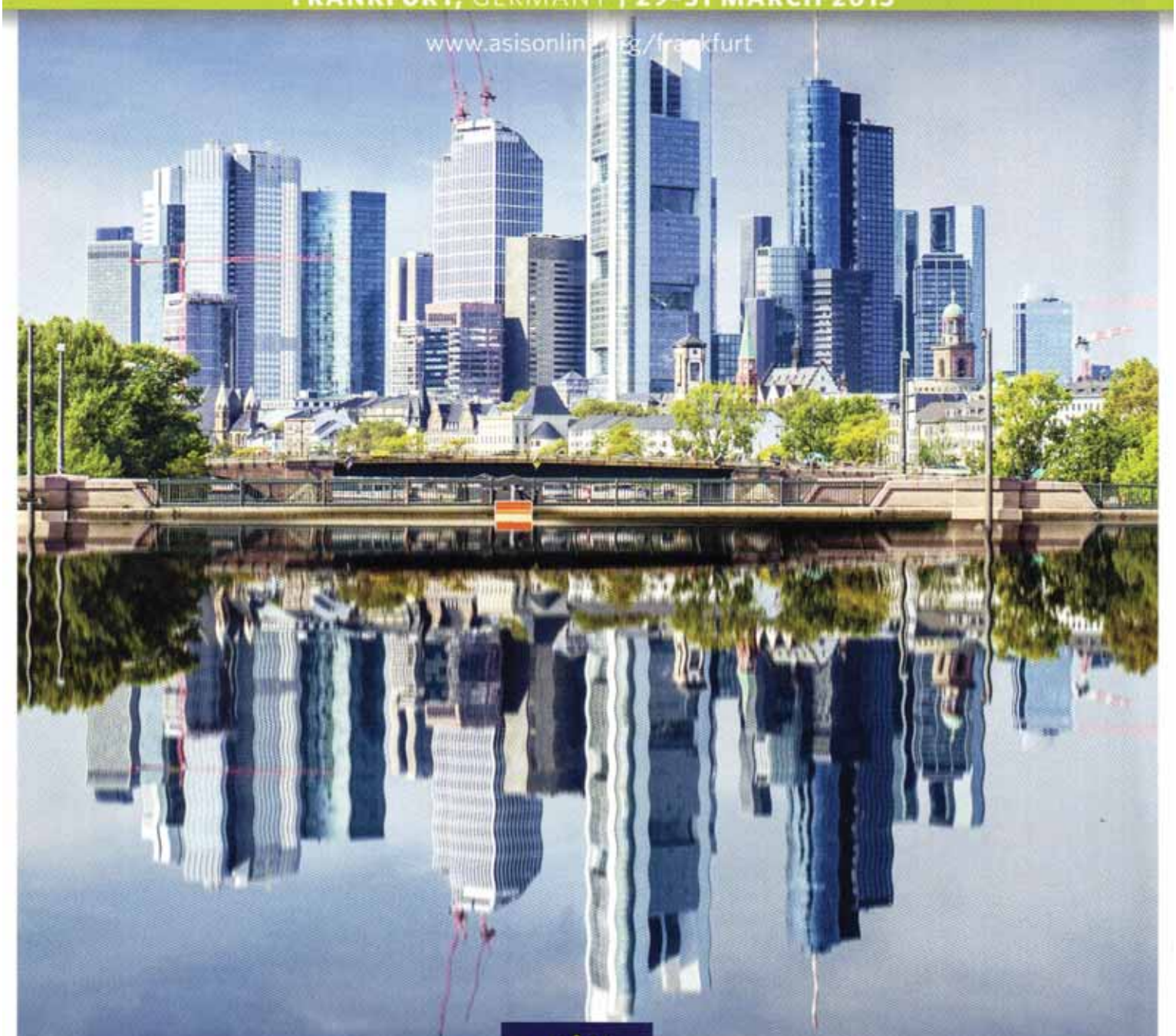
ASIS INTERNATIONAL
Advancing Security Worldwide

14TH EUROPEAN

SECURITY CONFERENCE & EXHIBITION

FRANKFURT, GERMANY | **29-31 MARCH 2015**

www.asisonline.org/frankfurt



ASIS EUROPE