

## who let the docs out?

### Also in this issue:



Two-thirds of UK firms hit by cyber breach in past 12 months

see page 7



Data is king

see page 14



Pen Test 101

see page 18



# Everyone & everything you need to know about information security

Rather than taking our word for it, look at the facts below:

- 98% of visitors were satisfied attending Infosecurity Europe 2015
- 93% satisfied exhibitors with 80% rebooking at the exhibition
- 160 hrs of free seminars and workshops for 2016
- 315+ vendors and service suppliers delivered a diverse range of new products and services
- ROI £1.39+ bn of estimated future orders, visitors expect to place with exhibitors as a result of attending Infosecurity Europe
- 4,435 professionals earned CPD / CPE credits

## REGISTER FREE NOW

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

## Welcome

### Welcome to the spring issue of Pulse

Thank goodness it's nearly summer again! The first half of the year is always very busy for us as we have to plan for the AGM, Congress, Infosec plus attend a wide range of industry events. In addition, it is the peak time of year for membership renewals. At the AGM, Jane Whitgift and Nigel Payne stood down from our Board and we welcomed Ed Hamilton and Chris Myers on to the Board. Ed has also taken over the Corporate Member chair role from Andy Cobbett who has valiantly held this role for several years and made a considerable contribution in developing the support that we can now offer our Corporate members. Andy remains on the Board with responsibility for Technology. A big thank you to them all for their support.

Congress was a huge success and we had nearly 500 people registered. This year we had three streams and were able to film virtually all of the presentations. So if you missed Congress or want to see presentations that you missed or enjoy some again, they are all loaded up on YouTube and we can provide you with the links. More on Congress is in this issue and please keep 16th March 2017 free in your diary for next year.

On this basis we are quite glad that Infosec has moved to June! We will be there on stand A45 and look forward to seeing many of you there. As usual we will be running a two hour workshop on professional development "Managing Your Career in Cyber and Information Security When So Much is Changing – What Skills Do You Really Need?" and there will be a small drinks party on the stand on Wednesday kindly sponsored by Acumin & RANT.

We are delighted that The Skills Framework content review has been completed and is now available to members in the members' area of the web site. We are currently piloting a more simplified accreditation process for Associate and Full membership and will provide an update on this approach for the next issue of Pulse. The next stage of the programme is to develop a Central Body of Knowledge (CBK) to underpin the Skills Framework and support the Profession. All this work is being led by Pete Fischer who is a Fellow of the IISP and we are very grateful for all his hard work on this and to the members that have contributed thus far.

The industry itself is maintaining its high profile in the media with yet more significant breaches so this issue focuses on the Panama leaks and your views. Aligned to this we have excellent member articles on how we should be dealing with the issues raised, the importance of collaboration and approaches that we should adopt to combat.

Many of you that attended Congress may have seen our first **white paper** on Security market trends and predictions. This was driven by our first member survey last year. An electronic copy of the survey is available on the web site and we will have printed copies at Infosec. We had extensive press coverage and interest on the report and intend to build on this work of developing a voice for the profession going forward. The next survey will be coming later in the summer and I would strongly encourage you to participate and make your voice heard.

I hope that you enjoy this edition and wishing you a lovely summer.



**Amanda Finch**  
General Manager  
Institute of Information Security Professionals

To get involved, email us at [events@iisp.org](mailto:events@iisp.org)



@IISPmedia



## Contents

### Inside this issue

News from IISP .....	02-05
Industry News .....	06-07
Who let the docs out? .....	08-11
ISO Compliance .....	12-13
Data is king .....	14-17
Pen Test 101 .....	18-19
60 Seconds with .....	20-22
What's in a name.....	23
IISP diary .....	24-25

Published by the Institute of Information Security Professionals (IISP). The views expressed in the articles within this publication do not necessarily reflect those of the IISP.

Copyright © 2016 IISP

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without the prior permission of the IISP.

No responsibility for any loss occasioned to any person acting or refraining from action as a result of any material in this publication can be accepted by the publisher.

All trademarks are acknowledged.



New Full Members

We would like to congratulate and recognise fifteen people that have received IISP Full membership status in the last few months they are, Barry Homer, Rev John Hawkins, John Knight, Martin Taylor, Jason Phillips, Edward Petrie-Smith, Amit Shukla, Paul Hobby, Arthur Paxton, Jim Seaman, Mark Bowers, Cameron Young, Chris Hodson, Lee Hezzlewood, Tony Brown.

New Corporate Members

We are delighted to announce two new corporate members to the IISP. Freshfields Bruckhaus Derringer, the multinational law firm joined the Institute in April as Gold corporate members.

We are also happy to announce that the MOD has become a corporate member, they recently commented on becoming corporate members



*The Ministry of Defence is delighted to join IISP as a corporate member and is looking forward to the benefits it will provide to our expanding Information Assurance community, across both military and civilian staff. The Defence Chief Digital and Information Officer, Mike Stone, is a keen advocate of developing and sustaining a professionalised workforce across all areas of Information, including Information Assurance and Information Security. John Cook, an IISP Fellow, heads up the Defence Assurance and Information Security team which sits within Mike's Information Systems and Services (ISS) organisation, under Joint Forces Command. Claire Fry, as MOD Head of Information Professions has an enterprise-wide remit to implement Professional Standards, to deliver new skills (Graduates/Apprenticeships), enhance existing skills, extend capability (at all levels of competence) and to recognise Information and Knowledge excellence. We welcome this opportunity to broaden our engagement with like-minded specialists and communities across Industry and Academia, as well as other Government departments.*

New Accredited Training Courses

**IISP accredit The Open University's Introduction to Cyber Security course**

The course 'Introduction to Cyber Security' created and taught by The Open University and presented by FutureLearn has been accredited by the IISP. The course originally accredited under the GCHQ Certified Training Scheme (GCT Scheme) has been certified against the IISP Skills Framework and covers the areas A1, A2, A3, B1, B2, C1, C2, D1, E1, E2, E3, I1 at level U.

The course is free to undertake and once enrolled students take the course over a period of eight weeks. This course teaches individuals to understand online security and start to protect their digital life. It demonstrates to the individual how to recognise the threats that could harm them online and the steps to take to reduce the chances that they will happen to them.

The Open University (OU) is the largest academic institution in the UK and a world leader in flexible distance learning. Regarded as Britain's major e-learning institution, the OU is a world leader in developing technology to increase access to education on a global scale.

The IISP's Accredited Training scheme provides a valuable service to training providers and enables members to develop skills to progress their careers. IISP accreditation indicates that the course materials and content have been assessed by a Subject Matter Expert to ensure that they meet the stated objectives of the course.

**You can enrol on the Introduction to Cyber Security course here:**

IISP Featured in Media Planet's Cyber Security Campaign

We recently partnered with Mediaplanet UK on the Spring '16 Cyber Security campaign in The City AM newspaper and online at [www.futureofoftech.co.uk](http://www.futureofoftech.co.uk). Read motivating insight from industry leaders and learn more about how security technology is changing businesses and consumers including an article for the paper titled 'The urgent need to combat the skills shortage' written from an interview with IISP Director, Piers Wilson **here:**

IISP White Paper – Security and Market trends

The recently published IISP white paper 'Security market trends and predictions' by Director Piers Wilson has formed the basis for some recent articles in the press on the trends and the white paper itself. Articles have been published in **Computer Weekly**, **Infosecurity Magazine**, **MicroScope**, **Networking Plus** and IT Security Guru in the last few months. **Download here:**

Volunteer to become a member of the Accreditation Committee

We would like to put out a call for volunteers to members that may be interested in joining the Accreditation Committee. Unfortunately within the last few months we have had 2-3 members leave and are looking for members to join. Criteria members should meet to be considered are to be a Full Members of the IISP and ideally be a Lead CCP Practitioner. Find more information about the Accreditation Committee on our website here or contact Bob Nowill or John Hughes for more information [drbob@nowill.net](mailto:drbob@nowill.net) and [john.hughes@secid.co.uk](mailto:john.hughes@secid.co.uk)

Training provider partner – Bob's Business

The IISP have recently accredited the Bob's Business' suite of e-learning modules, a gold standard for information security professionals. IISP require evidence that organisations have a track record of delivering training to the highest standards.

Bob's Business Ltd. are leading provider of cyber security awareness training campaigns which are designed to change and secure the habits of end users, helping businesses to create a 'human firewall' to prevent data breaches and reduce vulnerability.

With a fun and engaging perspective to training, Bob's animated modules demonstrate common human error security breaches in organisations, via an entertaining and engaging narrative based e-learning tool. The solution's unique, storyboard based approach to learning the fundamentals of information security achieves an outstanding 90% engagement rate.

The modules cover an array of cyber security topics, with each bite size module focusing on a specific topic such as passwords, viruses, phishing, email etiquette, identity theft, mobile working, backing up data and information classification to name a few.

Through a blended learning approach, Bob's Business also helps organisations engage with end users and to reinforce key security messages on an ongoing basis, giving CISO's valuable support with their ISMS by managing, training, policy management, incident reporting and compliance.

All of the courses are developed within the controls of ISO/IEC 27001 and scrutinised for relevant compliance with the requirements of:

- The Public Sector Network Code of Connection
- The Data Protection Act 1998
- The Payment Card Industry Data Security Standard 3.0 (PCI DSS)

Course content can be tailored to reflect organisational procedures and policies, and the package includes access to an enhanced learning hub, where clients can integrate policies and any third party content.

High standards of usability, relevance and alignment of its contents to contemporary good practice in information security are maintained across all modules by having a qualified subject matter expert execute independent and formal reviews on the curriculum and its contents. In addition, all modules request user feedback which is then collated, evaluated, and implemented once it has been approved.

**More information about the training can be found here:**



IISP Congress 2016

IISP Congress, which was run in conjunction with CREST again this year, saw a record number of delegates at over 400. The addition of a third stream and a bookshop both proved popular so we plan to further develop these for 2017. Our thanks to all of the speakers and the sponsors for helping to make it another successful event.

**Photos can be viewed and downloaded at:**

**Presentation slides can be downloaded at:**

Filmed presentation can be found on the media page of the IISP website with other presentations and interviews available on the CREST YouTube channel: [www.youtube.com/user/CRESTadvocate](http://www.youtube.com/user/CRESTadvocate)

Next year's event will be on 16th March at the Royal College of Surgeons. Early bird sponsorship packages are available. Please contact [marc@crestandiisp.com](mailto:marc@crestandiisp.com) for details.



ADP Midlands #1 – Mind the Gap – Titania, Worcester

A review of the first ADP Midlands event by Andrea Simmons.

Finally, a local event, really, really local, back in an old stomping ground! Once upon a chapter in my life I was taught how to be an insurance salesman in Security House, Barbourne Road. Funny how the world turns – but that’s something to remember about your career; there will be many chapters, twists and turns. Roll with the punches – but don’t punch on your way up or down as you never know who you will meet or need to ask for a favour again!

Anyhoo, we were treated right royally by the team at Titania on 21st March for an Associate Development Programme evening. The attendees were bright, young and engaged – and deserve better from the industry at large, given the depth of their understanding and the breadth of their knowledge.

We played the “Mind the Gap” game – literally a board game designed to encourage strategic thinking with a view to formalising and reviewing information security management system (ISMS) design within the context of a number of fictitious organisations in a variety of industry sectors. Participants defined requirements and shared their experience with each other. The session was moderated by experienced security practitioners who assessed the quality of the answers and filled in any gaps – well, ok, so that was Amanda Finch (General Manager, IISP) and myself (Director, IISP). Collectively, we’ve seen a lot, that’s for sure!



In brief, the ISMS considerations for the two main chosen fictitious organisations were - see right:

Areas to consider	Floormart	Mango
Info Asset emphasis	CIA	CIA
InfoSec strategy	Role based and process driven	Sophisticated and layered
Policy focus	Dynamic aspect of policies; cyber champions	Policy must map to control aligned to identified risk Consequences and education
InfoSec Awareness Programme – focus on the “What”	<b>What:</b> Align with risks and roles	<b>What:</b> Carry healthy suspicion
	Health and Safety	Don’t click what you don’t know
	Annual leave, HR interaction etc	Protect confidential information
InfoSec Awareness Programme – focus on the “Who	<b>How:</b> Integrate with induction (subliminal)	<b>How:</b> Fake phishing
	Frequency based on role / relevance	Continual presence
	Cyber Champions	Leave your work at the door!

Local pizza delivery mid-session really helped to fuel the collective brains and the end result was quality sharing and exchange. The quality of articulation was exceptional – and rightly rewarded with Easter Eggs, given the season that was in it!

London Branch Meeting – Q1

A review of the event by London Branch Chair Ryan Rubin

The IISP’s London branch held its first quarterly meeting of 2016 at the end of Q1 at Protiviti offices in The Shard. The evening was an immediate sell-out with places being booked to full capacity within 24 hours. Our distinguished speakers, Paul Dorey (CSO Confidential) and Joel Harrison (Milbank) addressed the audience on two topical areas that are presenting a challenge to many in the information security community. The first, presented by Joel, was an informative discussion about key insights into the new General Data Protection Regulation (GDPR) that has recently been put in place across Europe. Joel covered several aspects of GDPR and its implications on companies handling EU citizen data and the notable changes arising from this regulation including increased fines, requirements for consent, and changes in liability for processors and controllers to mention just a few. Joel also presented some highlights of another European directive (NIS) and who is likely to be in scope for it in the future.

Following a brief networking session, Dr Paul Dorey took to the floor and presenting a lively discussion on the Role of the CISO in communicating to the Board. Paul’s key message was that the CISO’s role is much like that of the Rosetta stone in being

able to act as a translator between different communities within the organisation. He outlined key tips on presenting to senior management in an effective way by losing the jargon, staying clear of the “FUD” factor, and presenting a sensible informative plan that enables senior management to understand cyber / info security from a business rather than technical perspective. The evening concluded with a “call to arms” to establish a group of volunteers to help drive further initiatives within the London branch for the rest of 2016. Look out for the next Branch meeting which will be held in Q2 2016.

News updates from Secretariat

IISP Secretariat staff member Sarah Smith recently completed her climb up Kilimanjaro, read how she got on here.

After spending 9 1/2 hours on the delayed Air Kenya plane we saw a herd of Zebra grazing as the plane came into land at Nairobi airport. We had a quick dash to our connecting flight and arrived at the gate just as the plane was due to depart – luckily they let us on and more surprisingly our bags made the plane too!



On the flight to Kilimanjaro International airport we got our first glimpse of the mighty mountain that was going to become our home for 5 nights.

Our group consisted of 12 people, plus the trek leader and an English doctor, we then had a local crew of 57 who carried our kit, their kit, tents, tables, chairs, cooking equipment, food, water, porta loo! Etc.

**Day 1** we transferred to the Machame Gate where we began our Kilimanjaro climb with a trek through rainforest to the first camp at 3000m, approximately 18Km. When we arrived our tents had been erected and hot drinks and popcorn were waiting for us in the mess tent.

We were up early on **day 2** for the steep ascent (840m) through moorland and some stunning views up to the Shira Plateau where we camped and rested (9km).

**Day 3** was our ‘trek high’ - ‘sleep low’ day, this technique is used to assist with the acclimatisation process We trekked through barren moon like landscape right up to Lava Tower for lunch (750m ascent) and then down again to the next camp (640m descent) (15km).

The morning of **day 4** we scramble up and over the famous Barranco Wall, with its Alpine Dessert vista and fantastic views of Mt Meru in the distance. Lunch was at Karanga Camp and then onward & upwards to high camp (650m) where we had dinner and 3 hours sleep (!) before getting up for the final push to the summit! (13km). One of our group had to leave camp immediately due to being diagnosed with Pulmonary Edema.

Up at 10.30pm a hot drink and the ‘pole pole’ (slowly slowly) trek began by torch light we headed up towards the summit in the darkness. We stopped at Stella Point, not for a pint but sweet tea and to see the sun rise over the Serengeti and take in the Artic like vista of the Glaciers glowing orange in the first light of the morning. Then the last 45 minute trek began, traversing the roof of Africa, to have our photos taken at the highest point in Africa, 5895m above sea level! (7km)



Then it’s the 2hr scramble on scree back to Barafu camp for a couple of hour’s kip before lunch and more trekking down to Millennium Camp. Those suffering from altitude sickness felt better down here. (23km)

After a big thank you to the local crew and the obligatory singing and dancing, we descend on Mweka Trail to the Park gate for a lunch of fried chicken and chips and a Kilimanjaro beer! (15km)

We were transferred back to our hotel looking forward to a warm shower unfortunately the bar came first and by the time I got to the shower there was no hot water left! Oh well a few beers, cold shower and curry what a way to finish an amazing adventure!

I under took the Challenge of climbing Mount Kilimanjaro to raise much needed funds for the Shakespeare Hospice in Stratford Upon Avon and would like to thank everybody who generously donated some of their hard earned cash. For anyone who would like to make a donation my just giving page is still open [here](#):





## Panama Papers: full database of offshore companies published online

A group of investigative journalists has published the names of thousands of offshore companies at the heart of the Panama Papers – a massive trove of data on the finances of the rich and powerful. The International Consortium of Investigative Journalists made data on 200,000 entities available on its website on Monday.

The files contain basic corporate information about companies, trusts and foundations set up in 21 jurisdictions including Hong Kong and the US state of Nevada. The data was obtained from Panamanian law firm Mossack Fonseca, which said it was hacked.

For the full story go to: 

## White hat hacker replaces payload in Locky ransomware



A white hat hacker appears to have hacked into Locky ransomware rendering it ineffective. In a blog post, Avira said that a sample it was looking at showed something far less sinister than malware.

"In place of the expected ransomware, we downloaded a 12kb binary with the plain message 'Stupid Locky,'" said Sven Carlsen, team leader of

Virus Lab Disinfection Service at Avira. Locky has been infecting computers and locking their files since February. It has hit targets in the US, Europe and some parts of Asia. It normally comes via an infected Word document.

For the full story: 

## Walmart Confirms Card Data Theft

US retail giant Walmart has confirmed reports that a number of its customers have had their payment cards compromised and bank accounts drained, according to a police statement.



The Fredericksburg Police Department has issued a warning to Central Park shoppers after it became apparent that at least 37 people who visited the local Walmart store earlier this year (in either March or April) became victims of this theft attack. Police are currently investigating the incident to find out exactly which registers were tampered with. Meanwhile, customers who shopped at that location in either month are encouraged to contact their financial institution and request a new card.

For the full story go to: 

## British manufacturers urged to step up their cyber-security plans

EEF, the Engineering Employers' Federation, surveyed over 650 respondents in the technology, consultancy and professional services as well as government, education, financial services, insurance, banking and other sectors, sampling from a range of small, medium and large businesses in the UK.

The findings show that 46 percent of manufacturers failed to increase their investment in cyber-security over the past two years. Two in ten firms are not actively making employees aware of cyber-risks. And 56 percent say cyber-security is given serious attention by their board. Only 36 percent of manufacturers have an incident response plan in place.

For the full story go to: 



## Two-thirds of UK firms hit by cyber breach in past 12 months

At least two-thirds of UK businesses suffered a cyber attack in the past 12 months, according to government figures. The Department for Culture, Media and Sport explained that most of these assaults were viruses, spyware or malware, and Ed Vaizey, minister for the digital economy, added that firms need to do more to protect against such threats.

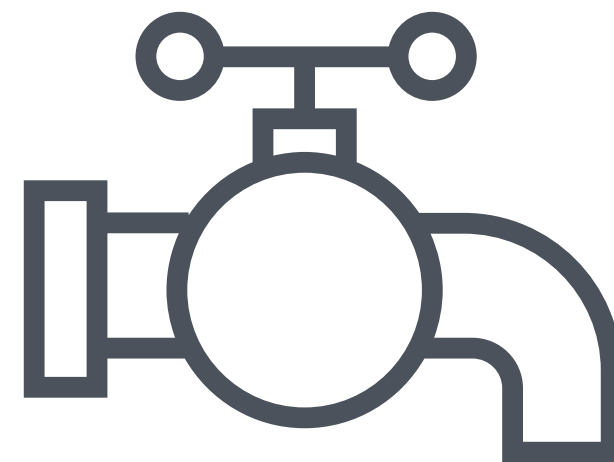
"The UK is a world-leading digital economy and this government has made cyber security a top priority. Too many firms are losing money, data and consumer confidence with the vast number of cyber attacks," he said. "It's absolutely crucial businesses are secure and can protect data. As a minimum, companies should take action by adopting the Cyber Essentials scheme which will help them protect themselves."

For the full story go to: 

## Cybersecurity Reports Out From AT&T, Cisco, Dell, Google, IBM, McAfee, Symantec And Verizon

These big players in cyber have published their annual security reports for 2016. Each one brings its unique view on cybercrime, and cyber defence strategies.

For the full story and to download the reports: 



## NHS trust fined for 56 Dean Street HIV status leak

An NHS trust has been fined £180,000 after a sexual health centre leaked the details of almost 800 patients who had attended HIV clinics. The 56 Dean Street clinic in London sent out a newsletter in 2015 that mistakenly revealed the recipients' email addresses to one another.

Patients were supposed to be blind-copied into the email but instead details were sent as a group email. The Information Commissioner said it was a “serious breach of the law”.

For the full story go to: 



# who let the docs out?

The recent 'Panama Papers' data breach dominated the news for weeks. Whatever your views are on the rights and wrongs of offshore tax havens, the loss of 2.6 terabytes of highly confidential data by law firm Mossack Fonseca was shocking in itself.

The data was released to journalists some time last year and therefore the theft went unnoticed for some considerable time. To make matters worse, there is yet to be a definitive explanation of how it happened. Was it the work of an insider, a disgruntled ex-employee or an external hacker looking to profit? Wherever the blame lies, if the company had had the right controls in place, it should have been able to identify the spike in excessive data egress, establish the source and track them down, even if it had not managed to stop it in the first place.

This is one of the most public incidents of this type, but it is far from the first and unlikely to be the last. How could this happen in a large professional company that holds such important, valuable and potentially explosive confidential information? Why, despite everything we already know about data breaches in the past, are organisations still failing to maintain good controls: logging, monitoring and reporting. Why is basic good security practice still not being followed?



**Eerke Boiten,**  
Senior Lecturer, University  
of Kent

**Here is what some of our members think:**

What security measures were Mossack Fonseca lacking?

The leaking of the Panama papers was a serious security incident for Mossack Fonseca. Analysts have looked at the services that the firm offers on the web, and found **a large number of actual and potential security holes**. But were outdated versions of Outlook Web Access and a Drupal client login portal really the way through which the files made

their way to journalists? What about the firm's message to customers, that their email servers had been compromised? Maybe we can simply reason along the lines of "if they didn't even get this basic security hygiene right, no chance they'd have more advanced security measures". But we can probably deduce a bit more, more directly.

For one, the leak does not consist of information gathered from passing emails only. The press stories so far suggest that journalists have had access to complete customer files, for connected collections of customers and shell corporations. The **Sued-Deutsche Zeitung story on the process** talks about these complete files, too. Those folders, including scanned paper documents, wouldn't likely have appeared in their entirety in emails. Even if the firm was using dubious methods of file-sharing between different branches, files of connected shell companies wouldn't normally all have appeared. Not even over the extended period in which this leak materialised.

If it was an outsider attack (as claimed), maybe they did get in through one of the holes visible in the web-facing side, and managed to escalate their privileges to a point where they could access customer folders. If so, we can add a lack of separation of control between their various systems to Mossack Fonseca's long list of security sins.

However, with such escalated privileges, the attacker must have appeared as an insider from the system's perspective at that point anyway. Firms holding sensitive data should have been alert to insiders' unusual scale of access – the cases of Chelsea Manning and Edward Snowden should have forewarned them of the risks. An outsider getting inside access would have needed a digital transfer of the terabytes of information from inside the system to the outside world – again the scale of this exfiltration should have rung alarm bells, and it should have been caught and stopped by a data loss prevention system. We can safely assume that no methods to detect suspicious use of access privileges were in place either.

In the PhD research of Dr Chris Bailey at the University of Kent, he explored access control systems that automatically reconfigure themselves in response to the detection of unusual or dubious patterns of access. Attacks like Manning's and Snowden's were illustrative use cases for this research. You can see the system in action, on the gamified situation of users cheating on a snakes-and-ladders game, at <https://saaf-resource.kent.ac.uk/>. This site also has links to the research papers describing how the idea of self-

adaptive architectures is applied to role-based federated access control systems.



Oscar O'Connor,  
Consultant

Organisations continue to lose sensitive information, despite the availability of solutions and the ever-increasing volumes of publicity surrounding security breaches, because of industry-wide problems in the relationships between technical and “business” communities. In my experience across more than 30 years and 20 sectors, the relationships between IT and “the business” have been strained at best. Trust is hard to find and until and unless we in the technical community, and especially those of us in the security field, learn a little humility when presenting the case for protective monitoring, security controls etc then we are going to see a lot of hands on ears and hear a lot of la-la-la-ing. If the security message is not gaining traction with decision-makers, perhaps we are not selling it correctly? Security is a hard sell because buyers of computer systems and networks have an inherent belief that what they buy should be secure already and when we position information assurance and cyber security as an additional cost, we do nobody any favours. CIOs are naturally cautious about telling their boards and stakeholders that they need to spend more money to make the networks and systems they manage secure... are we surprised? We shouldn't be. Let us not blame the user, but with humility and rational argument seek to educate and advise and most of all aim to deliver value back to our customers/employers.

Mark Kendrew,  
Director of Apollo  
Communication Intelligence  
& Security Ltd

As data leaks grow in likelihood and impact, security officers must collaborate to succeed

*The leaking of sensitive documents can have serious consequences for the reputation of the companies involved. The Panama Papers have shown that leaks can damage the careers of business leaders and customers associated with the compromised documents. The insiders involved usually have authorised access to the leaked data, making them one of the most difficult threats to tackle. In this article, Mark Kendrew, explores how information security leaders require the skills and experience to engage and collaborate effectively with business leaders and IT service providers to proactively address these threats.*

Businesses are increasingly reliant on sharing information with their customers and business partners, more often over IT services provided by third parties. This has increased the likelihood and potential impact of both malicious and accidental data leaks involving insiders. In the same way that businesses must collaborate to achieve their strategic goals, information security leaders must build trusting partnerships with the business and IT service providers to identify, prevent, detect and respond to these growing threats.

Identify: Developing a shared understanding of the specific insider threats

Data leaks can be caused by different insider actions. Malicious insiders can act either alone for personal gain, retribution or a sense of public duty; or in collusion with external parties motivated by commercial gain, crime or espionage. Non-malicious insiders can cause accidental data leaks through the loss of IT equipment or the inadvertent publication of sensitive data. The characteristics of each type of insider threat are different, requiring business leaders to better understand which threats may affect them.

Information security leaders and IT service providers must understand the different types and sensitivities of data being used by the business. They also need to know the value placed on such data if lost, stolen or corrupted, which is essential for prioritising and designing controls.

*Therefore, collaboration is crucial for matching relevant insider threats to the sensitive data being used by the business to quantify and prioritise the data leakage risks.*

Prevent: Deploying effective IT-enabled security capabilities

There are many IT applications available to help prevent data leaks. No application currently exists that is capable of offering the full range of services needed to tackle insider threats. Therefore, there is a need for IT and information security teams to work together to deploy and support a range of different applications, each providing specific security functions.

Information Security Officers, IT service providers and business leaders must work together to deploy and join together appropriate combinations of IT-enabled functionality to create effective data leakage prevention capabilities. Business engagement is essential for success because it is the information users that must adopt any new ways of working arising from the change.

*Therefore, collaboration is crucial for successfully implementing a range of IT security tools that can be combined to create the specific IT-enabled business capabilities needed to reduce data leakage risks.*

Detect: Reliably confirming data breaches earlier

IT-enabled capabilities can be used to monitor user behaviours and to alert of possible abnormal behaviours. However, such indicators and warning signs cannot be relied upon to identify all breaches.

Business leaders have access to other information about their staff that can point towards an increased risk of data leakage. For example: some staff might be involved in sensitive commercial negotiations; poor performing staff might be at risk of being let go; and staff with financial difficulties might be prone to bribes. This intelligence, when combined with alerts from IT security systems is essential for identifying people to watch and for confirming breaches more reliably.

*Therefore, collaboration is crucial for sharing multi-source intelligence about potential breaches so false alarms can be ruled out and true breaches confirmed.*

Respond: Taking effective action to manage data breaches

Once a data leak has been confirmed, business leaders have obligations to their shareholders, customers, Regulators and the Press that will drive their response priorities. Security leaders will be looking to work with the IT service providers to identify who was involved and assessing the full extent of the leak. It is essential both parties understand each other's perspectives so that any response appears coordinated, under control and well managed.

*Therefore, collaboration is crucial for providing an effective and coherent response that protects business reputation and maintains shareholder confidence.*



Adrian Bishop  
Head of Engineering,  
Huntsman Security

Dealing with Insider Attacks

The cold hard truth is that insider attacks are extremely difficult to defend against – and almost impossible to avoid. What we describe as an “insider attack” could have many origins: whether from an individual accessing and taking sensitive data for whatever reason, selfish or otherwise; a simple mistake; or even a systems fault, such as a website glitch that provides users with access to more information than they were expecting. Regardless of origin and intent, the main

threat from most insiders is that they are impossible to see coming or prevent, since the only way to really safeguard against them is to prevent anyone from ever doing any work.

With this in mind, businesses need to be monitoring their systems in such a way that any suspicious insider activity is detected and flagged as quickly as possible - whether that comes from truly malicious action or a simple mistake. This detective capability not only helps the security team, but the fact that there is effective oversight also acts as a deterrent to malicious activity in the

first place. One way to improve detection capability is to use technology that autonomously monitors and learns how users access systems, so it can detect anomalies that indicate a potential threat in real-time. By monitoring all systems in this way, there is a chance to mitigate any potential attacks quickly and without major incident.

Education is also important; the risks of such attacks must be translated in terms that are meaningful to the whole business, not just the tech teams. For example, there's little value in telling the finance director that there's a new whaling scam they need to be wary of, as chances are they won't know what you're talking about. However, if you explain that criminals have found a way to create fake emails that look like they have genuinely come from company CEOs, to con finance teams into making payments into illegal accounts, they will have a far better idea of what to look out for.

As more of our information is saved on company systems and technology finds its way into so many other parts of our lives, it will become harder and harder for businesses to locate insider threats before they cause a problem. There is a real risk that organisations will be overloaded with information on potential threats; a problem that is only going to get worse. The challenge is spotting which, out of a blizzard of warnings, are those that pose the greatest danger to the organisation. When it comes to insider threats, a rapid response is critical, as the longer a threat remains active, the more damage it can cause. As such, businesses need to automate as much of the threat resolution process as possible. If their systems can analyse and prioritise potential threats, whilst automatically addressing the low-level problems, security teams can be freed up to deal with those that present the greatest danger to the business.



# ISO COMPLIANCE, CERTIFICATION AND ACCREDITATION EXPLAINED



**Graham Parker**  
Managing Director, Parker Solutions Group

The International Organisation for Standardisation (ISO) produces thousands of standards every year covering multiple topics and disciplines. A certain group of those standards known as management system standards are designed to support organisations in delivering products and services which are higher in quality, safer, more secure, more resilient, and environmentally friendly.

These standards are well known such as ISO 9001 (Quality Management), ISO 27001

(Information Security), ISO 14001 (Environmental), ISO 22301 (Business Continuity) and the soon to be launched ISO 45001 (Health and Safety).

Some organisations are required to implement these standards and some other to demonstrate their compliance to them. Within the industry there is a lot of “noise” about compliance, certification and accreditation, and the difference between these terms. So what do they actually indicate in reality?

### Compliance

Any organisation can choose to implement a management system standard and use the standard to drive improvement and manage risk. They can choose to meet the requirements and perform internal audits as part of their overall management system.

When an organisation implements such standards there are no mandatory requirements (demanded by the standards themselves) to undergo an external audit. Essentially any organisation can implement the standard and claim to be compliant.

Customers of such organisations may ask that their suppliers meet certain standards and in some cases suppliers may simply state that they are compliant however some customers may go one step further and ask for evidence or choose to audit their supplier. For organisations with multiple customers, this could certainly be a large burden having to handle multiple customer audits through the year. This costs time, resources, and often coinage to produce the same evidence time after time.

### Certification

Certification to ISO standards for an organisation is simply a way of proving that an organisation does indeed comply with the relevant standard(s). It does not involve implementing extra requirements or controls, and if an organisation has already become truly compliant, certification should be a simple next step.

Certification involves an audit being performed by an independent organisation known as a certification body. A certification body will usually perform an audit over two stages.

Stage one is a high level review of the management system, whereas stage two is used to look at the management system in much closer details to provide evidence of compliance in various areas.

A good certification body and their auditors will approach the audit from a positive perspective, attempting to find evidence of conformity and are not in the business looking to “catch people out” or to deceive people. In the event that non-conformities

are found (by failing to fulfil requirements of the standard), then agreements can be made on how this will be addressed, which in some cases may need a re-visit and in others it may be acceptable to correct the non-conformity over a longer period of time.

If an organisation meets the requirements and is recommended for certification, then the certification is awarded for a period of three years. During that time, the organisation must undergo annual surveillance audits. Surveillance audits are much smaller than the original audit and are designed to check whether the organisation is maintaining and improving its management system.

What are the benefits of being certified?

If an organisation has taken the time to become compliant then getting certified can have the following benefits:

- The organisation can easily prove compliance to customers and interested parties
- The organisation is independently recognised for its efforts
- The level of auditing from customers can often be significantly reduced as independent certification can increase assurance
- Many organisations are now demanding that their suppliers are certified to ISO standards

### How do we choose a good certification body?

There are many factors to take into consideration but first we should describe an important matter. There are no rules or laws preventing anyone from setting up a company and calling it a “certification body” and awarding certificates. So how can we be sure that a certification that has been awarded by a “certification body” is credible and reliable?

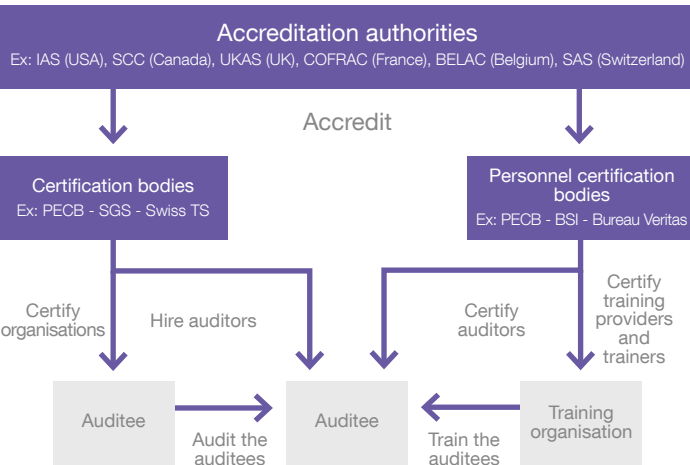
One response is accreditation. In order to demonstrate that their certification processes are fair, credible, and trustworthy certification bodies should follow a standard known as ISO 17201. ISO 17021 lays out how a certification body should operate in order to provide confidence in the certifications they award.

When a certification body is compliant to ISO 17021 they can be audited and accredited by an accreditation authority. Most countries around the globe have a national accreditation authority (sometimes more than one) which accredits certification bodies. These bodies are all members of the International Accreditation Forum (IAF).

So when selecting a certification body always check whether they are accredited by a member of the IAF. There are some “certification bodies” which are not accredited or are accredited by organisations which are not members of the IAF. This does not by default mean that their service is poor; however it is much harder to prove credibility without such recognition.

The following graphic shows the role of accreditation authorities and certification bodies:

### Certification Schema



### Does my certification body have to be accredited by the accreditation authority in my country?

The IAF has a simple motto “one accreditation international recognition”. Some certification bodies work globally and undergoing accreditation audits in every single country in which they operate in would not make sense. So all IAF members recognise each other. Indeed it is a requirement for accreditation authorities to do so “Accreditation body members must declare their common intention to join the IAF Multilateral Recognition Agreement (MLA) recognising the equivalence of other members’ accreditations to their own.”

So as long as your certification body is accredited by a member of the IAF then this is the major point.

### What else to look for?

Other factors in selecting a certification body would include, their credibility, their geographic presence, the price (of course) their knowledge of your industry and competence of their auditors. The latter is extremely important. Ensuring the audit team has the right skills, experience, and knowledge is fundamental to have a positive audit experience.

### About the author

Graeme Parker is an experienced Cyber Security, Risk Management and Governance professional with proven experience in implementing and developing effective management systems against various ISO standards. He is the Managing Director of Parker Solutions Group.

**If you have any questions, please contact him at: [graeme@parkersolutionsgroup.co.uk](mailto:graeme@parkersolutionsgroup.co.uk)**



# DATA IS KING



Bill Buchanan  
Edinburgh Napier University

We live in an era where data is King, and it often a focus for an intrusion. The scope of data breaches are now massive, and often focus on insider help to gain privileged access to data. No firewall in the world will stop an insider copying the complete Exchange Post Office onto an SD-card, and walk out the building.

Overall the solution is to detect data “at-rest”, “in-motion” and “in-process”. Many existing system detect the transfer of documents in network transfers, but with the increasing usage of encryption tunnels, it is becoming a challenge to detect this. Dell estimate that within five years, 99% of network connections will be tunnelled.

For documents “at-rest”, normally there are operating access restrictions applied, but these do not embed restrictions outwith an organisation domain, and are often fairly limited in their scope. An administrator often, too, have large-scale access to all documents in the organisation. Encrypting data at its core, whether it is emails or documents, and defining restrictions on its access is thus a key factor in protecting organisations from large-scale data breaches. Unfortunately the lack of tools and general understanding of cryptography are providing key barriers to adoption. The protection of email, for example, is often just the usage of an encrypted tunnel

to protect the email, which only protects the email as it travels over a network, and does not protect at its source or destination.

Few companies properly protect their documents, or use encrypted email messages for their sensitive information. While there are often technical access restrictions on document, when it comes to defining the access policies on documents we still often use operating rights to restrict access, and for many companies and government departments the classification involves adding “Commercial-in-Confidence” or “Secret” on the cover page, or at least in the footer of the pages.

Unfortunately the world has moved on, and the distribution of documents is now so much easier, and Web crawlers have no respect for these marks. The minute a document connects to “any” network, it can be contactable by other computers, and the minute a document resides on a computer with a connected storage device, it can be copied.

Last year a top secret plan named: Operation Temper and entitled “Counter Terrorism Post Paris Large Scale Military Support to the Police” was uploaded onto the National Police Chiefs Council (NPCC) website, and reported in the minutes of a meeting on 22 April 2015. It terms of sensitivity, this must be viewed at being one of the most sensitive documents around, as it provides details of things to adversaries. It gave details of the deployment of over 5,000 heavily armed troops on the streets of UK cities, on a major terrorist attack, and focuses on simultaneous events happening across the UK. The details also outlined the guarding of key targets by the troops and police.



## Document classifications

In the UK government, departments use a number of classifications for documents, and which typically focus on the risk of harm to life and limb. The highest levels are:

- Top Secret. This is the highest classification, and could cause “exceptionally grave damage” if the document was released. This might relate to designs for the storage and transport of nuclear material, or for military operations.
- Secret. This document would cause “serious damage” if it was leaked.
- Confidential. This could cause damage to national security.
- Restricted. This could cause undesirable effects.
- Official. This defines that it a posting from a government department.

Issues related to terrorism would typically be placed in the Top Secret or Secret classification, as the plans would give benefits to those who plot malicious activities. The access to the documents would be highlighted as restricted, and only given access to those with the highest levels of clearance.

Companies too often require classifying their documents, and again these focus on the harm of the company and/or their employees:

- Restricted. which requires the highest level of access control, as a release of the information could cause major problems to the company or employees.
- Confidential. which could do harm to the company or its employees if it was released
- Internal Use Only. which can disclose information only within a company but could do harm to the company or its employees.
- Public. which can disclose information to a wide audience without any risk to the company or its employees:

Apart from national defence, the classification of documents can also focus on the risks to individuals around sensitive information. In the document below the Department of Defence filed a government security clearance questionnaire about Steve Jobs where he divulged that he took LSD between 1972 and 1974.



Figure 1: Steve Job's admission of LSD taking

## What goes wrong?

Perhaps the issues with this case are the lack of due process and due diligence in the leaking of the documents, and one must wonder about the methods that are used around cryptography and document access, if a sensitive document like this can be leaked onto a government Web site. With the usage of crawling agents, even documents which are not viewable and be cached in an instance. The document is now likely to have been captured by crawling agents around the world.

The minute a document hits a Web site with a public IP address, it is likely to have been captured for the World. Even when a document is taken off a Web site, it is often still accessible through Google's caching facility.

The methods applied in Data Loss Prevention (DLP) are now being extensively applied in a number of industries, especially in the finance sector. This includes the scanning of network traffic for things like credit card details, and malicious phishing. Data which does not look right is automatically put into a holding area for further inspection.

Over the past few years, companies have been working hard on protecting their systems and, especially, their data, so that sensitive information does not leak out. So with Sony's data now appearing on Wikileaks, we see embarrassing information about their executives, but it is highly sensitive information that should always be protected, and that is the information that could risk life and limb.

With the NPCC data leak, it was a document that related to terrorism plans that was leaked onto a public-facing Web site. One must thus worry about the processes applied in that a non-encrypted or protected document containing information around the protection of citizens could be leaked to the Internet.

The traditional viewpoint of documents is that there is a single copy of them, and that they are static things. These days copies of documents can be produced in an instance, and distributed widely. In DLP (Data Loss Prevention), though, we get the concept of data existing (Figure 2): at-rest (on the disk); in-motion (on the network); and in-process (in the memory of a computer). Data must thus be protected in all these states, but, unfortunately, many people just think that everything is secure if they have encryption on their disks.

Organisations need to understand that documents need to be protected in each of the states defined, so that there is no good in protecting access to a document on a network drive, and then not protecting it when it is transmitted over the network, or actually used within the memory of a computer. A visual marking of the security of a document will do little if an adversary just deletes the security marking.



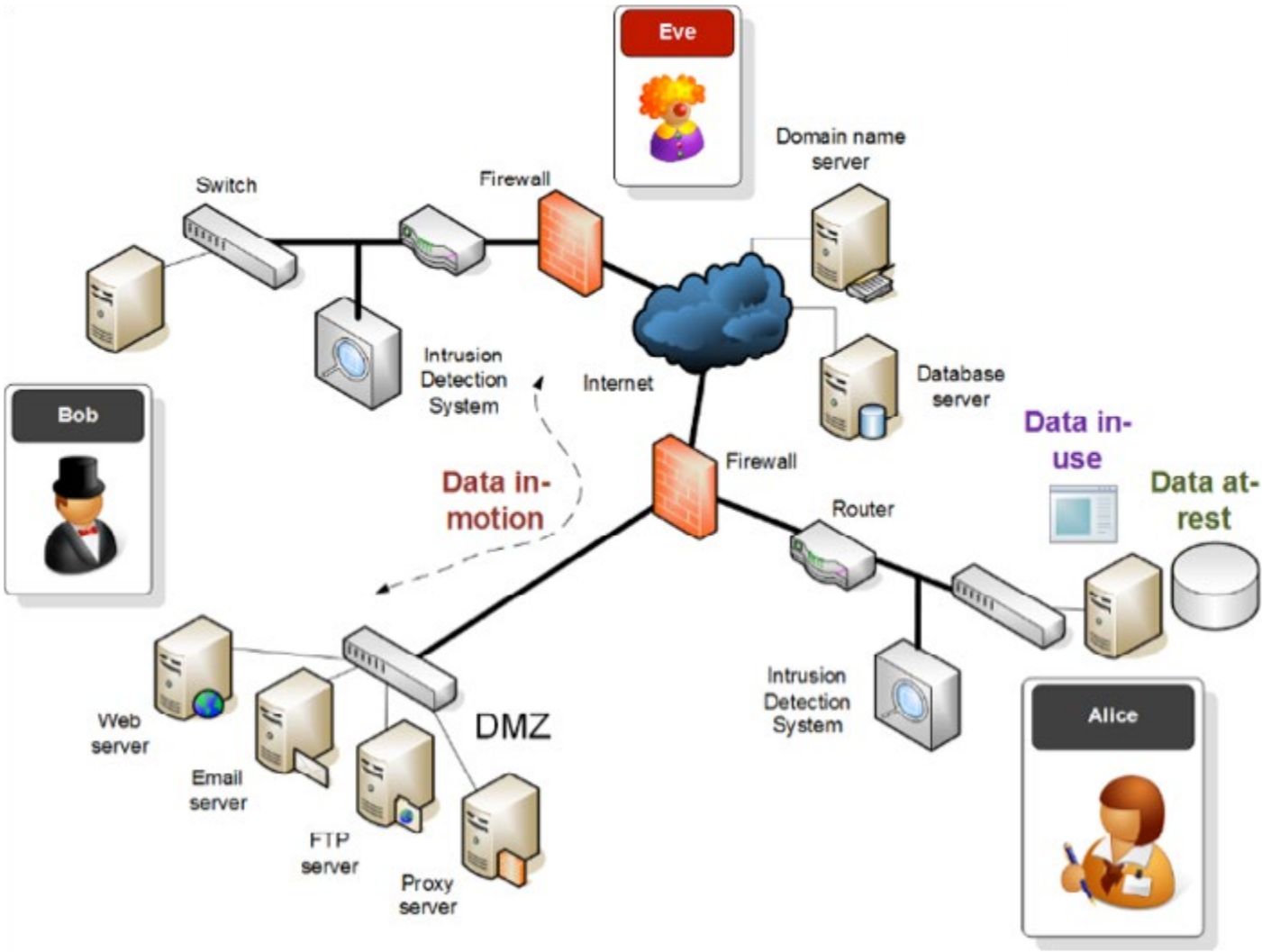


Figure 2: At-rest, in-motion and in-use

The terrible security restrictions of Microsoft Office

Many companies restrict the editing of a document or add a password. Unfortunately, from a security point-of-view, the methods used by Microsoft Word to protect documents are almost laughable. Previous versions of Microsoft Office have virtually no security levels applied, and it was easy to break any restrictions. Newer versions use the DOCX format, which is actually a ZIP file, where a reader can change the file extension of the file and gain access to its contents (which are defined in XML). It is not a difficult task to change the rights of access on the document after this. While newer versions of Word improve the restrictions, they are still open to password attacks, as users will often put simple passwords on their documents. File which are protected by a password must be seen as weak practice, and just slow down the progress to gain access to a document.

So Many exit channels ...

There are so many exit channels for a document, and as long as it is stored on a disk, there can be ways for it to leak out of the system. The best way to protect it is to apply encryption. For a database, if possible, every record should be stored with a different encryption key, as intruders can often gain access to the password which stores the key.

The usage of passwords in protecting an encrypted document is also a worry as we severely restrict the number of encryption keys that are used, such as from a 128-bit encryption key, which a space alien with quantum computing would struggle to crack, to a tiny little encryption key of just 20 bits (which your mobile phone could crack!).

For exit points, the minute you connect a network to the document, there are many ways the document can leak out, especially through the usage of a secure tunnel, in which network scanners will not be able to detect it. With the increase in storage around SD cards and with USB sticks, there is an easy way to get the document off the system. So auditing agents should also be capturing events, not just from the network, but also on the usage of the storage devices and on the running processes on the system.

So what can we do?

Well, at the lowest level, we can never stop the copying of documents, as someone can take a picture of a screen. What must happen is to restrict sensitive documents so much that it is extremely difficult for them to gain access, with many tripwires along the way to detect their accesses.

For organisations the placing of restrictions on documents is the last line of defence, and means that someone has managed to get over all the other hurdles to gain the document. Generally, as illustrated in Figure 3, there should be increasingly levels of identity and access control as we go nearer the sensitive documents and these should be placed separate from other less sensitive documents.

In sensitive areas, full auditing should be required so that all accesses to documents can be checked, and logged, and these should be monitored through an aggregated event log (such as with SIEM integration). In some environments, the events are monitored 24x7 by human security staff. Along the way, there should be checks on accesses, especially for multi-factor authentication. The best methods use biometrics, such as fingerprint, retina scan, and handscans, along with geo-location. Increasingly mobile phones are being used as an “out-of-band” authentication method, where access is gained by sending a one-time code to the users registered mobile phone, and then this is placed into the Web login page.

Overall, too, it does not harm to have humans involved in approving things that are published or moved to certain places, as humans tend to spot when something is not quite right. Most security products are based on standard signatures of activity, so an adversary can often know the signature, and then find a way round it.

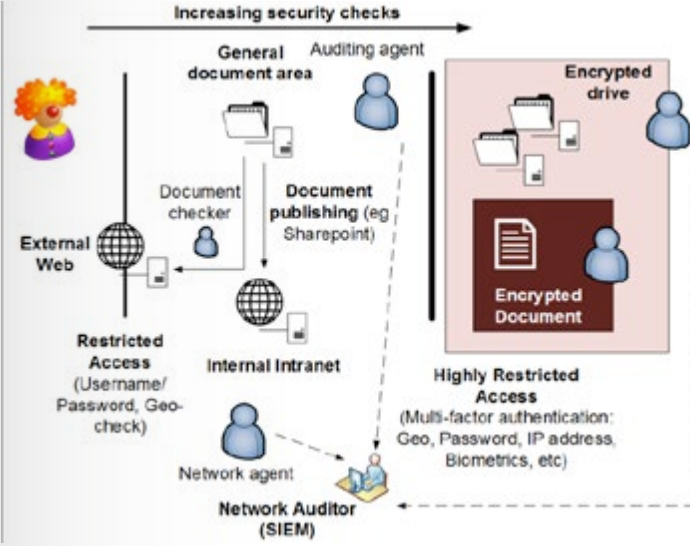


Figure 3: Secure architecture

Okay ... it's people who make mistakes ...

The processes involved in data loss prevention should focus on checking when employees make mistakes, and should make continual checks for data leakage. A lack of training and giving someone too many rights are often weak points in the process. A recent Thales survey on encryption highlighted too that the main reason for companies encrypted was not to protect against hackers or malicious insiders, it was “To guard against employee mistakes” (Figure 4).

So when setting up the system, users need the minimum of rights of access to anything sensitive, and sensitive documents must be stored in places away from less sensitive documents. A location lock-down is also important on accesses, especially if this can be embedded into the document. To allow a document such as a terrorism response plan to move onto a Web site, without authorisation or checks along the way, and even checks when the document arrives on the Web site, beggars belief.

Along with this the perception is that documents will be leaked by external hackers, but in most cases data leakage involves an insider in the organisation, or a trusted contractor, so all the controls on the firewall and external restrictions, will not stop and insider from gaining access to documents behind the firewall.

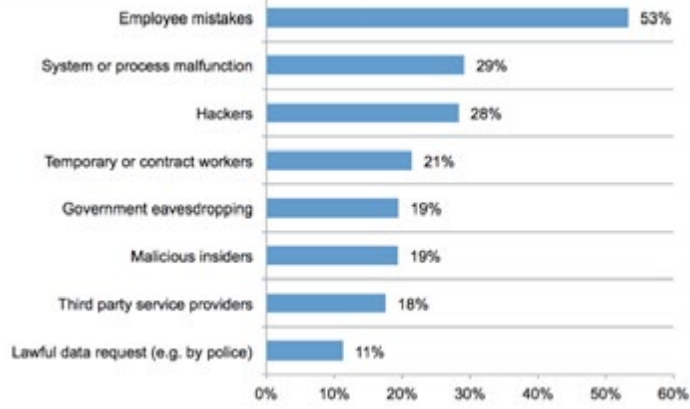


Figure 4: Why encrypt? ... people!

Conclusions

Data loss prevention is likely to become one of the hottest topics around, and adversaries just seem to be able to target companies and agencies, and gain access to their sensitive data. While most have focused on commercial companies, it is likely that government departments will become a target, especially around a strong commercial drive in selling sensitive data, and with the rise of hacktivism.

Our methods are often still based on having physical access to a paper version of a document, but as long as there's a network connection to a document (or through a physical storage device) there is a way that there can be access to it. So just marking a document as “Secret” is not going to stop someone from copying it.



# Pen Test 101



## Context Information Security sheds light on the world of penetration testing and explains why more companies and organisations see it as a key part of their cyber security strategy

The main aim of penetration testing is to identify technical vulnerabilities in IT and communications systems that could leave your organisation open to attack should they be exploited by a potential threat actor – from a disgruntled employee or casual hacker to a state sponsored cybercriminal. Once identified, these weak points within a network infrastructure, application or even business logic can be remediated to strengthen your overall security posture.

There are lots of analogies that work here, but amongst the most illustrative is that of the fire drill. Everyone knows they need to leave the building if the fire alarm goes off, and thanks to installed signage they even know the safest route to follow. A fire drill which simulates the real thing might reveal that a door is routinely locked, an exit blocked or fire extinguishers that are either missing or non-functional. Now think of your network as a building with flammable materials lying around and a faulty extinguisher as vulnerabilities and a man with a match as the threat. A penetration test provides that same kind of real world attack experience by mapping vulnerabilities, exposing gaps in security policy and process and ultimately managing risk. It would advise against storing large quantities of oil in an unsafe environment, point out that policy was being breached regarding extinguisher maintenance and suggest better methods of preventing arsonists from gaining access.

## Size doesn't matter

While pen testing is often thought of as being something only large enterprises need, and have the budget for, the truth is that small and medium-sized business are firmly in the cybercrime cross-hairs. In fact, recent research from Symantec<sup>1</sup> suggests 60 per cent of attacks are aimed at the SMB sector. When it comes to being targeted by the bad guys, size really doesn't matter: every organisation is at risk. As for budgets, you shouldn't be asking whether you can afford a penetration test but rather whether you can afford to be breached. Breach costs can be financially devastating by the time you've rolled forensic investigations, incident mitigation and reputational damage into the total. According to the Department for Business, Innovation & Skills<sup>2</sup> a breach can cost the SMB as much as £310,800 while for big business that rises to a starting point of £1.46 million. More recently, cyber criminals are also looking to directly monetise hacking through the likes of ransomware and Carbanak, used to steal money from banks. So, where the impact used to be in terms of ICO fines or loss of reputation and business, there is more likely to be a direct financial impact.

## DIY disasters

You may be thinking, what with the number of readily available automated vulnerability scanning tools out there, why you can't pen test yourself? In some cases, such as an organisation applying for accreditation or certification there will be a requirement to obtain penetration testing from an independent third party, but even if you were just looking to self-assess your security posture there are still plenty of good reasons not to do it. The main one would come down to skill sets as the person responsible for the testing

may not have the necessary technical knowledge to carry out the various aspects of a penetration test. For example, they may need to perform a web application test, an internal infrastructure test and a Citrix review for which an external company would be in a position to provide experienced and capable consultants for each. Another benefit of using an external provider is what they provide to the organisation in terms of exposure. A self-test may not provide a realistic picture, as an internal employee could bring additional access or knowledge about their own infrastructure that could skew test results. The fact that an external provider will be unbiased and independent really cannot be stressed enough, as these are vital requirements for a meaningful penetration test.

The skewed perspective through existing infrastructure knowledge may be relatively obvious, but the danger of subconscious bias if reporting to your own senior management less so. An external contractor will be free from both.

## Manual dexterity

When it comes down to the use of automated vulnerability scanning tools, these actually do have their place and could help an organisation improve its security posture if identified issues were properly remediated. However, a vulnerability scan can only go so far. Anything more complicated than simple scans of infrastructure and web applications can lead to a lot of false positives. In addition, any issues will need to be manually reviewed to ensure they are legitimate issues. This can easily become unmanageable, and when you throw in complex systems and applications, it becomes impossible as simple vulnerability scanners will not identify vulnerabilities within business logic or complex multi-stage transactions. Automated scanning has its place but should only be used in conjunction with a more robust and manual penetration test approach.

## The small matter of trust

Something that might be of concern, given the nature of the access being handed over to a pen testing team, is the not so small matter of trust. It's vital to ensure that any organisation carrying out penetration testing, and engaging an external company to provide that service, should be satisfied regarding appropriate qualifications. There are numerous certifications out there that can provide a level of assurance that the consultant is appropriately skilled and has the requisite knowledge. At Context, we aim for our consultants to acquire CREST related qualifications such as CREST Registered Tester (CRT), and Crest Certified Tester (CCT) which are technical qualifications that require a high level of knowledge and technical ability to be able to complete. Any external consultants will also require the necessary security clearances - at least Security Check (SC) level - if accessing protectively marked

information and assets. Tick the certification and clearance check boxes and you can be happy with a high degree of assurance that your pen testing partners are competent, trustworthy and appropriately skilled.

## Legally speaking

From the legal perspective, any company carrying out pen testing could be in contravention of the Computer Misuse Act. Penetration testing is also known as ethical hacking, which provides a hint as to why, so relevant authorisation must be given by the organisation being tested. Where the Data Protection Act is concerned, a penetration test may involve access to corporate data and information; so the organisation also needs to ensure that the testing company is handling any data appropriately and securely. At Context, we conform to relevant standards ISO9001 and ISO27001, which gives the organisation assurance that any issues can be avoided.

## Report and remediate

You should also bear in mind that a successful penetration test does not end after the penetrating has been done; in order to deliver value to your business it has to also assess the impact of any issues found. A properly conducted pen test by a team of certified professionals will result in a comprehensive and focussed report; far more so than any automated process could hope to achieve. This is important, because the success of the testing should be measured less in what has been found and more in how those weaknesses can be mitigated.

By providing clarity through detailed reports stating the technical impact and ease of exploitation, you can better understand the risk and so be in a better position to implement the most appropriate and proportionate mitigation methods.

With network breach and data loss headlines appearing day-in, day-out, they threat to businesses is not going away. And whereas penetration testing was once seen as something only government departments, major corporations and financial institutions undertook, it is now seen as an essential part of information security strategies for companies of all types and sizes.

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

<sup>1</sup> [www4.symantec.com/mktginfo/whitepaper/ISTR/21347931\\_GA-internet-security-threat-report-volume-20-2015-appendices.pdf](http://www4.symantec.com/mktginfo/whitepaper/ISTR/21347931_GA-internet-security-threat-report-volume-20-2015-appendices.pdf)

<sup>2</sup> [www.gov.uk/government/news/government-urges-business-to-take-action-as-cost-of-cyber-security-breaches-doubles](http://www.gov.uk/government/news/government-urges-business-to-take-action-as-cost-of-cyber-security-breaches-doubles)





**Alex Baxendale**  
**Company:**  
CGI  
**Job Title:**  
**Managing Security Architect**

Atstake (previously Lopht of Lophtcrack fame) which taught me to see security from an aggressor's perspective and has proved invaluable insight into my current role.

Fortunately (it did not feel like it at the time) I was made redundant from Atstake in 2003 but was soon offered a job in the Enterprise Architecture group at Northrop Grumman, courtesy of an Astake Director. This was a revelation as I moved over into true security delivery role for the first time at a major systems integrator and resulted in my current career path. It also led to my re-introduction to CESG via the CLAS scheme, then ITPC and ultimately the IISP.

After a couple of years I was head hunted by CGI and ended up working for my current boss, whom ironically was my boss at Admiral PLC. So I have arguably ended up back where I started (almost home) but much the wiser and with some great experiences along the way. Since re-joining CGI I have worked on a variety of bids and programmes as the Lead Security Architect, ending up in my current role as the CGI Lead Security Architect on the UK National Programme.

**Your reflections on 10 years of The IISP**

A decade, truly! How time flies when you're having fun. I can proudly state that I was a founder member, and have seen the IISP grow from what felt like a small club to a professional institute of some stature. Along the way we have experienced some ups and downs, some great events, but also a lack of clarity over CCP evolution, multiple changes to HMG schemes and the challenges of handling a rapid membership expansion in a not for profit organisation. Still that's part and parcel of what makes the IISP special. It's run by us for us.

**Short career biography:**

I joined Admiral PLC (which is now CGI) in 1995 as a provisional trainee evaluator under the ITSEC scheme working my way up over 5 years to the post of Lead evaluator and CLEF Training Manager. This provided a strong foundation in security principles and security assurance. I started providing ITSEC consultancy in 1998, helping parties whom were going through ITSEC evaluation, and this led to my becoming increasingly involved in broader security consultancy and security testing, including penetration testing. This resulted in my departure from Admiral in 2000 to join a couple of small penetration testing consultancies, including

**Professional:**

**What was your first role in information security and how did it come about?**

On completion of my PHD in 1997 I applied for a Database Administrator job in Plymouth based on a paper advert. I was summarily rejected for this role, but then had a call from the recruitment agents that placed the advert asking if I had ever heard of Admiral PLC (now CGI) an IT Consultancy. At the interview the opening line was 'why do you want a career in security' I cannot recall what I said but three weeks later I was a provisional Trainee ITSEC evaluator in the Admiral Commercial Evaluation Facility (CLEF). So by chance really!

**What has been your biggest professional achievement to date and why?**

To date, probably helping to win the UK National Programme for CGI. As the bid security lead I made a significant contribution to our proposal and helped formulate our core solution design. Very stressful, but very rewarding. Especially as we were up against the heavy weights competitors. Soon to be replaced with the successful delivery of Smart Meters into operation, I trust!

**What are the biggest challenges in your current role?**

I was tempted to talk here about the nature of my role and the complexities of the programme, the breadth of the role, commercial pressures and the challenges of delivery etc. The real challenge however is security culture. Security is a sliver that weaves through all aspects of a large delivery programme, yet is often seen as an obstacle. If everyone understands the importance of security and its basic principles, to understand that doing it right from the start is easier and to have a desire to contribute in their own way then this makes a massive difference.

**What is your best advice to anyone entering a career in infosecurity?**

Security is really a state of mind. It's seeing the world from a particular perspective, while understanding the broader picture. It is also predicated on Trust. My advice would be to focus on your day job, but try to immerse yourself in the broader field of information security. Seek out every opportunity to expand your understanding of the core principles of security and their application including the why, what, how, where and when aspects. Listen to your more experienced colleagues; participate in security forums, read widely, join an institute or two, basically be open minded and engage. It's a world of opportunity and diversity.

**Where do you see yourself in 5 years?**

I am a people centric techie at heart and there I wish to remain. That said I am more interested in the journey than the destination. So it's all about the challenge of interesting work, working with great colleagues while delivering value that excites me. So in 5 years time I hope to be a performing similar work but with an increased IISP engagement, including Lead IA Architect and IISP Chartered Status. CGI is also getting heavily engaged in the education sector and I hope to be part of that.

**Why is it important to be a member of the IISP**

Security is becoming increasingly professionalised, because it is fundamentally based on trust while the needs of compliance drive standards in all aspects of the security space. So on that argument alone belonging to a leading professional institute is in itself an increasingly important element of career development. Professionalization is not however about having a badge, it's about driving forward best practices, standards and industry capability and working within the community to raise awareness. The IISP provides a great forum for engagement, to help you make a difference and to enable others to help you.

**Personal:**

**What has been your biggest personal achievement to date and why?**

Erm, Probably having tea with Prince Charles and my Headmaster, when I was a young lad. To talk about the school aeroplane we built. Ironic as I am a republican at heart, although I have to say I quite liked him.

**If you could have dinner with anyone, past or present, who would it be and why?**

Delia Smith, a) because I am sure she would cook a smashing meal and b) because I am an ardent Norwich City fan and I would relish the opportunity to thank her in person for all she has done for the club. We may be struggling right now, but there are not many clubs in this day and age with a heart like Delia's at its core.







**Paul Irwin**  
**Company:** QinetiQ  
**Job Title:** Principal, Consultant

**Short career biography:**

I have 22 years’ experience as an IA professional establishing and driving technical information security and assurance in the Defence, Telecommunications, and HMG arena. My career has included IA delivery, team leadership, technical and assignment management and business development.

My earlier roles included 6½ years in the Defence Sector as the IT & Security Manager at a List X organisation and 2 years in the Telecommunications Sector as a Senior Consultant for a CNI provider.

I have been in my current post for 13½ years since joining QinetiQ in 2002. As Principal Consultant in the Advanced Cyber Threat

(ACT) practice I am responsible for managing and leading a multi-disciplinary team of IA professionals, developing and implementing compelling Cyber Consultancy propositions that deliver high-value services to clients, and the successful delivery of client-focussed assignments to a wide range of MOD, HMG, CNI and Commercial clients.

Your reflections on 10 years of The IISP (100 words or less)

It has been interesting and encouraging to see the institute emerge from the grass roots of IA, grow into a recognised centre of excellence and continue to mature into the leading UK and International body for IA professionalism.

The Institute has steadily and progressively established itself as a recognised force for good and has attracted the attention, support and commitment of individuals and organisations dedicated to professionalising IA and driving its recognition as a discipline that supports the protection and promotion of information security in a digital world.

**Professional:**

**What was your first role in information security and how did it come about?**

My first role was as an IT Security Engineer at a List X organisation, which came about following a work placement I had with that organisation during a higher education course.

**At what point did you realise you wanted a career in infosecurity?**

At the risk of showing my age, it was following the introduction of the very early desktop computers into the workplace, well before the widespread use of the Internet. I realised that I was more interested in the computers and their security than what we were actually using them for!

**What has been your biggest professional achievement to date and why?**

Attaining Certification as a CCP Lead. I consider the recognition resulting from the rigorous assessment process to be invaluable and a source of enormous personal achievement.

**What are the biggest challenges in your current role?**

Keeping up to date with information security subject matter as it continues to rapidly evolve and respond to meet the myriad of constantly changing demands and challenges posed by emerging technologies, threats and attack vectors.

**What is your best advice to anyone entering a career in infosecurity?**

Get yourself a solid grounding in a technical IT discipline before specialising in security and information assurance. The knowledge and experience you gain from that technical background will be invaluable in supporting your infosec career as it develops and matures.

**Why is it important to be a member of the IISP**

The IISP is the recognised leading UK and international Professional Body dedicated to the information assurance profession. Members benefit hugely from the personal professional recognition afforded to them through IISP membership and CCP, and from the Institute’s crucial role in advancing the professionalism of the industry as a whole.

**How long have you been involved with the IISP and what is your current role?**

I have been involved with the IISP from its inception and outset, before the Institute was known as the IISP. On behalf of the IISP I am an Assessor and Interviewer for IISP membership applicants and for candidates seeking certification under the CCP scheme. Outside of the IISP, I am a Principal Consultant within the Advanced Cyber Threat (ACT) business of a leading security consultancy.

**What surprised you the most when you started working in this field?**

Rather than expressing surprise, I would express satisfaction at the unforeseen breadth, depth and variety of interesting, challenging and rewarding assignments that I have worked on which have sought and benefited from information security and assurance input.

**Personal:**

**Sweet or savoury**

Savoury.

**What is your ideal holiday destination?**

Anywhere warmer and drier than here.

# CESG Cyber Service Consultancy – What’s In A Name?



**Matt (Bod) Horan**  
**LCCP, CISM, CISA, CITP, M.Inst.ISP,**  
**Director C3IA Solutions Ltd**

Within a month of the Crown Commercial Service (CCS) going live and advertising the services of the newly crowned Cyber Security Consultancy (CSC) companies, it was a pleasant surprise to receive 3 approaches from customers specifically looking for the services of such a newly qualified company. For these customers the message has clearly got through that CLAS was no longer the answer to a cyber security requirement and that a structured, quality assured and governed approach to risk assessment and management was the way ahead and that a framework existed through which it could be procured.

This situation marks a milestone in what has been a long journey, starting in 2014, from what could be cynically described as an RMADS based, accreditation ruled, CLAS enabled security management approach. This has been changed to the implementation of a risk-owner managed and business focussed approach to risk assessment and management. But it is just a milestone and the journey is far from over. Where we find ourselves now is in a procedural hiatus, developing sets of documents for risk management and accreditation, through the work of individual or small teams of experienced and CESG Certified Professionals on behalf of business owners that have not quite got the message that risk management is their responsibility. So it’s early days.

For many CESG Certified Professionals, the vast majority of whom will continue to be the bedrock of the delivery of risk assessment, management and related services, this change has been turbulent. There is no clear pattern to how the ex-CLAS Certified Professionals are aligning themselves in response to the arrival of these new schemes. Nor does there seem to have been a tsunami of SMEs and larger companies racing to achieve CESG CSC status. This may be because despite the initial success of the CSC, there remain numerous frameworks and procurement

channels through which their services can be contracted, including Digital Outcomes, G-Cloud, R-Cloud, FATS, OJEU and prime-subcontract to name a few. Even though terms and policies have been updated, plenty of customers are slow to move away from the old terminology and concepts, calling for the services of a CLAS consultant and referring to the old Impact Level statements to define the systems to be Accredited or assessed. From my perspective it seems this situation may be slow to change, unless a more proactive communication plan is initiated and/or replacement processes proposed from CESG.

This change is, however, coming. For example, the new approach to risk management and accreditation that has been developed by the Home Office National Police Information Risk Management Team is bringing a new baseline to best practice on the Public Service Network in Policing (PSNP). Local Government and Police and Crime Commissioner led initiatives alone are driving the need for business leaders to consider the utility and security of their information assets in tandem. Customers are getting the message that they should be seeking certified services and that a framework approach has facilitated their access.


So by choosing to become a CSC provider C3IA has been required to demonstrate, based on evidence that its IA practice and processes, both as a company and at individual leadership level, are of the appropriate quality to provide consultation in such scenarios. No doubt some of the larger companies feel that they have been doing this for some time, and this may be true, but for an SME like C3IA it has been a healthy (although not easy) process. As a result of the certification process and qualification, our communication and engagement with CESG has been both proactive and productive. C3IA feels it is well placed to respond to new initiatives. It has also provided a very clear path to certification for a wider set of IA service categories when the current set of 3 (Risk Assessment, Risk Management and Architecture) expand. Finally with the formation of the National Cyber Security Centre and a new relationship with industry being planned we are well placed to engage in workshops and discussions that are normally reserved for the larger consultancy brands.

So how is life post certification? Shaping up nicely thank you.



## IISP Scotland Branch Meeting


**When:** Wednesday 8th June 2016  
**Where:** Waxy O'Connor's, Glasgow

The third Scottish branch meeting is coming up you can register can keep up to date with the agenda for the evening [here](#): 

## IISP Thames Valley Branch Meeting

**When:** Tuesday 28th June  
**Where:** CGI, Green Park, Reading

The IISP would like to invite you to the inaugural Thames Valley branch meeting. The event is kindly hosted by CGI who will provide a talk on the evening with a second talk coming from IISP Chairman, Alastair MacWillson. The evening will also provide attendees with the chance to network with members from the area. Come along to have your voice heard on how you would like the branch run and what topics you would like to see discussed at future meetings.


**Register here:** 

## ADP Midlands #2: Service Continuity

**When:** Monday 13th June 2016  
**Where:** Capgemini, Birmingham

This second Associate Development Programme (ADP) event in the Midlands will be centered on Disaster Recovery. The facilitator on the evening will explore 'not making a drama out of a crisis Business Continuity'.

A reminder that this programme is open to graduates and new joiners employed by IISP Corporate Members only.

**Register here:** 

## CCP Briefing Round 2

**When:** Monday 20th June 2016  
**Where:** Deloitte, Leeds

After successfully touring our CCP Briefings in London, Cheltenham & Manchester we are about to embark on the second round. We can now announce that the first event will be taking place on Monday 20th June and will be kindly hosted by Deloitte in Leeds. The event will feature a presentation from Mike Nash on the 27000 series.

IISP CCP Briefings are an exclusive benefit for IISP members holding CCP gained through the Institute, so in order to attend you must have gained CCP certification through the IISP. The aim of the events is to address topical issues and give an update on the scheme and recent changes.

**Register here:** 

## Cyber Security Challenge

Could you represent the UK in a European Cyber competition?

Would you like to represent the UK in Germany? Are you between 14 and 30 years old and not currently working in the Cyber Security Industry? Do you love working with computers, networks and solving CTF challenges? The European Cyber Security Challenge could be for you!

Signups for the European competition will launch on April 11th 2016 and we need you!

This year will see the second European Cyber Security Challenge, bringing together the best talent from across Spain, Romania, Germany, Austria, Switzerland and the UK, to compete for the ultimate title of European Champions.

Cyber Security Challenge UK will be sending a team of juniors (age 14-20) and one of seniors (age 20-30) to compete in the competition in Dusseldorf from 7-12 November 2016. The competition will give participants an opportunity to prove their ability within web and mobile security, crypto puzzles, reverse engineering and forensics; using their skills throughout the challenges to take them as far as they can go.

**If you think you're up to the task, then you'll need to play our qualifying games, delivered in association with Hacking-Lab, by Saturday 28th May.**

**For more information – please contact Debbie Tunstall on [dtunstall@cybersecuritychallenge.org.uk](mailto:dtunstall@cybersecuritychallenge.org.uk)**

## Cyber Security for Financial Sector

**When:** 1st-3rd June 2016  
**Where:** Frankfurt, Germany

Global Forum on Cyber Security for Financial Sector will serve the attendees as a platform to gain a cost-reducing advantage from a shared proven know-how of experts through practical business-friendly networking in the Financial Sector; including banks, investment funds, insurance companies, credit card companies and stock brokerages.

**Register here:** 

## Infosecurity Europe

**When:** 7th-9th June 2016  
**Where:** Olympia, London


Everyone & everything you need to know about information security Infosecurity Europe on 7-9 June 2016 in Olympia London is region's number one information security event featuring Europe's largest and most comprehensive conference programme, and over 315 exhibitors showcasing the most diverse range of products and services to 12,000 visitors.

This year's theme is a rich and complex evolving challenge which infosecurity professionals of all types are facing every day.

From connections and collaborations with multiple partners and suppliers, to increased technological connectivity and the IoT, to connected, always-on, tech savvy employees and customers - organisations are more connected than ever before as they strive for efficiency and speed to market. The resulting myriad of new threats, vulnerabilities and risks are ripe for exploitation by increasingly sophisticated cybercriminals who themselves connect and collaborate. The Conference Programme will look at the challenges of securing the connected enterprise and provide strategic and practical advice on how to address them.

Choose from over 160+ hours of high-quality conference sessions in our free to attend conference programme, bringing 260+ international thought-leaders.

Confirmed speakers include: The Right Honourable Lord Hague of Richmond, Levison Wood, Explorer & Writer, Mikko Hypponen, Security Researcher, Bruce Schneier, Security Technologist, Troels Oerting, Group CISO, Barclays, Cory Scott, Director of Information Security, LinkedIn, Lee Barney, Head of Information Security, Marks & Spencer, Jaya Baloo, CISO, KPN Telecom, Gaynor Rich, Director Information Security Risk & Governance, Unilever, Dean Atkinson, Head of Cyber Security Operations, Thomas Cook Group, James Lyne, Security Researcher, Rik Ferguson, Advisor, Europol and Security Researcher, Hem Pant, CISO, ING Wholesale Bank, Arnaud Wiehe, Chief Information Security Officer, TNT Express, Steve P. Williamson, Director, Governance, Risk and Compliance, GlaxoSmithKline, Will Harvey, Head of Assurance and Head of Security Profession, HMRC and many more industry luminaries.

**Register here:** 

## The Cyber Security Summit

**When:** 22nd June 2016  
**Where:** 43 Crutched Friars, London

The threat we face from cyber is unendingly evolving, expanding and diverging. With evermore systems and devices going online and becoming connected, the financial, political and physical damage caused by a potential breach has never been higher.


The UK Government has acted by investing £1.9bn by 2020 in Cyber Security and with the new National Cyber Security Strategy being published in 2016, join this free-to-attend summit to discover the latest developments, strategies and technologies available to defend your organisation online.

**Register here:** 

## Cyber Security in Healthcare 2016

**When:** 28th September 2016  
**Where:** Olympia, London

Cyber Security in Healthcare gives one of the most debated areas of discussion its own platform, examining in even more detail how effective Information Governance and Cyber Resilience is now at the heart of any digital system and an immediate consideration for any institution responsible for sensitive patient information.

**Register here:** 

## RANT Conference '16

**When:** 3rd November 2016  
**Where:** etc. Venues, London

The fourth annual RANT Conference will once again take on the slightly alternative format and provide an entertaining and educational networking and open discussion focused event for 300 senior end user information security professionals.

**Register here:** 





**London Office**

CAN Mezzanine  
32-36 Loman Street  
London SE1 0EH

**Evesham Office**

Basepoint Business Centre  
Crab Apple Way  
Evesham  
Worcestershire  
WR11 1GP

Website: [www.iisp.org](http://www.iisp.org)