iisp pulse

Winter 11 Issue7

Institute of Information Security Professionals

IN THIS ISSUE:

INFORMATION STEWARDSHIP IN THE CLOUD

SECURITY RISK MANAGEMENT 3.0

NETWORK FORENSICS IN CYBER DEFENCES

WELCOME MESSAGE FROM THE GENERAL MANAGER

Welcome to the winter edition of *Pulse*. At this time of year many of us are taking stock of the current year and making our plans for the next. For the Information Security profession, 2011 has seen some pretty significant events and initiatives that have raised the industry's profile. The articles included in this edition look at some of the issues that have been raised and developments within the Institute and our industry.

In the summer the UK Government demonstrated its commitment and investment in information assurance by announcing its certification scheme for IA professionals based on the Skills Framework to measure competency. We are obviously delighted (along with our consortium partners CREST and RHUL) to be appointed as one of the three bodies that will be able to issue the CESG Certified Professional (CCP) Mark next year and very proud that the scheme is based on our framework.

Within the Institute we launched our Academic Partner programme which supports our commitment to working with academia. The programme aims to formalise and strengthen existing ties and to promote the profession to staff and students. Details of the programme are included on page 16. In addition, we have included an article from Simon Walker who was one of the winners from last year's Cyber Security challenge. We have always been pleased to support the competition as it vital that we continue to attract talented individuals into the industry.

The Institute is also a partner of the Cloud Stewardship Economics project, and Simon Shiu and David Pym share some of their work. The project forms part of a wider UK Technology Strategy Board programme and there will be an opportunity for members to be involved next year.

Finally, in terms of the Institute and its strategic direction, we had our fifth AGM in November and welcomed three new members to our Board. The Board has been reviewing our vision and strategy as the Institute continues to mature. Our chairman Dr. Alastair MacWillson presented this vision at the AGM and it is also shared in this edition.

Amanda Finch
General Manager, IISP

A NOTE FROM THE EDITOR

It has been an unprecedented year for information security and an unprecedented year for the Institute. Never before has the industry had so much mainstream media exposure.

IISP membership numbers continue to grow and we should reach 300 Full Members by the end of the year. We have also had strong development in a number of new and current programmes some of which are featured in this edition.

In 2011 *Pulse* magazine expanded by 20% and this edition welcomes support from one of our large Corporate members for the first time. In 2012 we are pleased to announce that Pulse will move from three editions per year to four quarterly editions arriving in mailboxes at the same time every year – so you know when to look out for it. Expect to see it in March, June, September and November.

As ever, if you would like to contribute to the magazine via articles, letters, or general comments, please do not hesitate to get in touch – julian@instisp.com.

It is after all, YOUR magazine, and YOUR Institute.

Julian Wadley
Editor, IISP Pulse

INSIDE THIS ISSUE ...

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.

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.

THE CHAIRMAN'S OUTLOOK

Dr Alastair MacWillson, the IISP's Chairman, shares his thoughts on the initiatives required to grow and develop the Institute.

Our AGM was on Monday 7th November 2011 in London and for those of you who were not able to attend (turn-out was excellent), we had a lively meeting with the routine business of finances, status reports, voting, and the confirmation of co-opted Board members (me) and the appointment of new Board members. We closed off with two excellent talks by Jonathan Hoyle CBE, Director General for Information Security and Assurance at GCHQ and Dr John I Meakin, Chief Information Security Officer at BP. For the Chairman's Outlook, I had the opportunity to provide a short presentation on the work I have been doing since assuming the role of Chairman, taking a hard look at our objectives and strategy.

This article is intended to give those of you that were not at the AGM a short summary of my presentation.

REVISITING THE INSTITUTE'S OBJECTIVES AND STRATEGY

I was appointed Chairman of the Institute in May this year and over the past seven months have been taking a hard look at our core business, our purpose, what we have to offer, and where we sit against others. I have consulted with a wide number of members, both individual and corporate, non-members, the Board, founder members, the Accreditation Committee and the Secretariat, to establish views on our status, direction, purpose, organisation and vision. I did this as I wanted to formulate my own perspective of the Institute – which I have now done.

There has been a lot of great thinking, tremendous effort and the best intentions getting the IISP to where it is today. The organisation is well established with a healthy and growing membership, solid processes, an excellent, but underpowered secretariat, and an amazing team of volunteers (Assessors, Interviewers, Accreditation Committee and Board members) that are simply the life blood of the organisation.

We can certainly carry on as we are, but my concern is that, in doing so, we will not meet member expectations, and early promises made, and we will not be in a position to address the real opportunity, to establish an Institute that can really define and help shape the information security profession.

From the feedback, it is clear to me that the Institute will serve the membership well if we can fulfil the following key strategic objectives:

➩ *Bridging the gap between education, practice and research;*
➩ *Giving practitioners the professional development and career support they deserve ;*
➩ *Informing public policy on how security can contribute to society, protect infrastructures and data, and enable innovation;*
➩ *Ensuring everyone benefits from greater awareness ;*
➩ *Championing the global security profession.*

I believe we are heading in the right direction to achieve these objectives, but progress is slow; we have not achieved the visibility we hoped for, and we lack the recognition we need to become a respected voice in the industry. Clearly, these things take time and you don't get recognition and respect by asking for it – you have to earn it!

So how do we go about that? I have put together a consultation document which sets out eight areas that we need to work on to achieve our growth and development ambitions. These have been discussed at Board level and we have agreed to develop these ideas into initiatives which we can then take forward. The initiative areas are:

➩ *Reinforce the vision;*
➩ *Create a richer membership award structure;*
➩ *Explore Royal Charter status;*
➩ *Build critical marketing capabilities;*
➩ *Build an international presence;*
➩ *Explore selective 'mutually beneficial' alliances;*
➩ *Enhance the secretariat and organisational support;*
➩ *Focus on membership growth.*

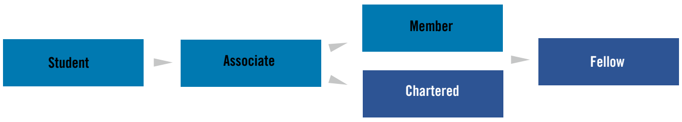
Unfortunately, given the limited space that I have for this article, it is not possible for me to expand upon all of these points, so for now I will focus on the following three key areas:

CREATING A RICHER MEMBERSHIP AWARD STRUCTURE AND EXPLORING ROYAL CHARTER STATUS

For me, one of the most exciting ideas from the strategy review is a proposal to extend the Institute's award structure. In fact, from the feedback I was given, this is also a hot topic with many of the membership. The Board believes that Full Membership is, and should continue to be, the award level that defines our vision for professionalism, in terms of skills and experience, while maintaining inclusivity across the profession.

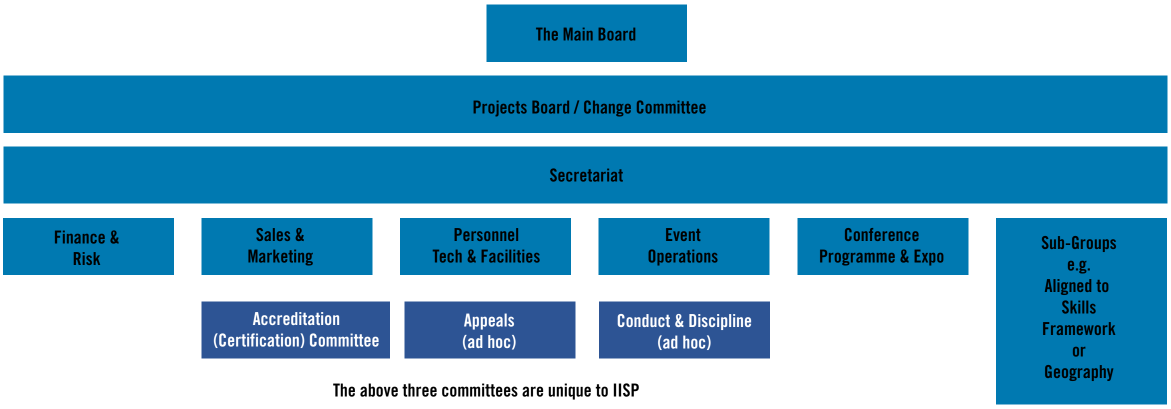
However, for us to have a legitimate 'licence to practice', chartered status would reinforce the significance of full membership, and would establish a gold standard, helping to elevate IISP membership above that of other organisations. With this in mind, we are seriously exploring the idea of obtaining a Royal Charter for the Institute.

Possible Extended Award Route



Sub-Committee Structure

To deliver its vision the Board needs to more widely distribute accountability and responsibility more effectively across its Board members, rather than take on the majority of issues collectively.



The Main Board

Projects Board / Change Committee

Secretariat

Finance & Risk

Sales & Marketing

Personnel Tech & Facilities

Event Operations

Conference Programme & Expo

Sub-Groups e.g. Aligned to Skills Framework or Geography

Accreditation (Certification) Committee

Appeals (ad hoc)

Conduct & Discipline (ad hoc)

The above three committees are unique to IISP

We would also like to examine the idea of introducing a prestigious Fellowship (by achievement) to attract leaders and luminaries who have made a truly outstanding contribution to security or the profession. I believe a Fellowship award would inspire other members, would give us unprecedented external recognition and, importantly, would provide a pool of 'experts' who could act as the voice of the Institute and could drive and present an annual conference of real merit.

ENHANCING THE SECRETARIAT AND IMPROVING ORGANISATIONAL SUPPORT

As with all start-ups, we have matured to the point where we have outgrown our accommodation, our IT support systems are straining under the load, our policies and processes need to catch up with the way we work, and we don't have enough staff to run the day-to-day activities and make the changes we need to evolve and grow. Behind the scenes, changes in these areas have been happening under the stewardship of Amanda Finch and we are making great progress.

That said, to really move the Institute forward, and to execute the various initiatives and ideas we have, will require more time, energy and commitment, than we have resources for. To overcome this, we envisage that individual Board members will sponsor one or more initiatives and will form a sub-committee of willing volunteers from the membership to make it happen. You will hear more about this, and see specific requests for help from Alan Stockey and I, in the next monthly newsletter. **This will be your opportunity to get involved!**

FOCUSSING ON GROWING THE MEMBERSHIP

Our vision and ambitions simply will not be achieved if we fail to retain and grow the membership beyond current levels. Aside from the many things we need to do, I would like the Board to have laser focus on what we can do to grow both individual and corporate member numbers. This will mean a new emphasis on marketing, continuing the focus on professional development, and consideration on how we add value to all members. I believe the strategy I have been outlining will go a long way to making membership more attractive and professionally and personally compelling. We need your support and continued commitment to make that happen. By the way, if each of you commits to bring in one new member we will be in good shape for 2012!

Finally, expect to hear more from me on this topic. I pledge to keep you informed about how these ideas (they are not commitments yet!) develop and on the progress we are making in achieving our objectives.

If you agree, disagree or want to help, please let me know.

Best regards,
Alastair

THE AUTHOR

Alastair has been the Chairman of the IISP Accreditation Board for five years and has recently been appointed as the IISP Chairman. In his day job, he is the Global Managing Director of the Security Practice, at Accenture. He is passionate about raising awareness on insecurity, improving the effectiveness of security, and giving the security profession better visibility and new directions.

INFORMATION STEWARDSHIP IN THE CLOUD

We report on an exciting research project that will generate new ways of thinking about cloud risk and security, and develop pragmatic decision-support tools for cloud stewardship.

FROM SECURITY TO STEWARDSHIP

Managing information risk is a complex task that must continually adapt to business and technology changes. We argue that cloud computing presents a significant step change, and so implies a big change for the enterprise risk and security management lifecycle.

The challenge for enterprises is how to understand the options that are available to them when considering obtaining services from the cloud and, in particular, how to judge the risks involved in consuming cloud services. These problems are somewhat more complex than similar ones that arise when considering outsourcing where, typically, the customer is able to dictate terms and conditions. In contrast, the large scales of the operations of cloud providers, together with the associated cost-structures, mean that the vendors and the marketplace can be expected to dictate (standard, one-size-fits-all) security service levels. Moreover, concerns develop from the traditional security concerns of confidentiality, integrity, and availability, to whether agents, brokers, and other service providers and integrators will act appropriately as stewards,[1] to whether operations and assurance will work across supply chains, and to whether the whole system – which will contain a multitude of such relationships, potentially all influencing one another – will be sustainable and resilient.

It is not just cloud consumers that will be concerned. Each firm in the ecosystem will be vulnerable to any changes that happen not only within that environment, but also externally. For example, how exposed will they be to high-impact security incidents that affect multiple supply chains? Or to skill shortages and liquidity changes that affect multiple groups in different ways? Is there a danger that some 'shocks' will permanently damage the ecosystem upon which they rely?

We are seeking to help cloud stakeholders understand the options they have to improve stewardship outcomes. How should regulators impose rules and regulations? How much influence does a single consumer have? How does this change if they act as a group? How much transparency into operations should be demanded by consumers and offered by providers? How should all the stakeholders act to deal with factors exogenous to the market, such as, the state of the economy, business trends and technology changes, or shifts of human skills?

Specifically, we aim to provide effective ways for stakeholders to explore their assumptions about the value and uncertainty associated with engaging with cloud ecosystems.

STEWARDSHIP IN THE CLOUD ECOSYSTEM

To simplify our discussion and analysis we distinguish three types of firms in cloud ecosystem: cloud consumers, cloud service providers, and cloud platform providers. Cloud consumers represent large and small enterprises that are making a transition from reliance on internal IT departments to consuming cloud services. Cloud platforms represent a bundling of platform- and infrastructure-as-a-service offerings.[2] Cloud service providers represent software providers that are able to leverage (and are conditioned by) platforms to offer software-as-a-service with particular agility, cost, and security profiles. Figure 1 shows these basic components in the context of exogenous factors such as attacks, regulation, and financial conditions.

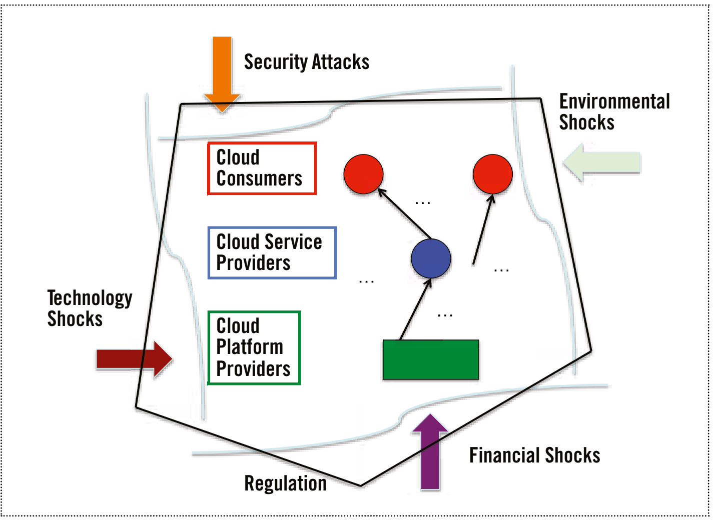


Figure 1: The cloud ecosystem

Stewardship concerns arise from all components in this framework. That is, all the cloud stakeholders will be concerned with whether firms in their supply chain are meeting stewardship commitments and expectations, and that they understand and can meet their own stewardship obligations. For example, how are firms incentivized to keep my information confidential, and will the ecosystem support my needs for federated surveillance.

Equally, they will all (perhaps implicitly, and certainly regulators and policy-makers) be concerned with the structure of the overall ecosystem, as conditioned by regulation and incentives, and as affected by potential shocks. Specifically, responsible stakeholders – that is, the good stewards of the ecosystem – will seek to ensure that they can expect the ecosystem to be sustainable, to be resilient, and to deliver good stewardship outcomes not only for themselves but also for the wider ecosystem community. For example, will the ecosystem be resilient to the failure of a few providers, and will regulation destroy the agility benefits upon which key consumers rely? Figure 2 shows some of the typical fast and slow dynamics of change to which the ecosystem must be, respectively, resilient and sustainable.

The dynamics of the evolution of the ecosystem will be affected by how easy it is for companies to switch between different cloud service providers. Where moving supplier is hard, companies will be more reluctant to adopt cloud and need better up-front risk and stewardship planning. The lock-in effect will also determine how service providers respond (if at all) to competition within the ecosystem and to exogenous shocks.

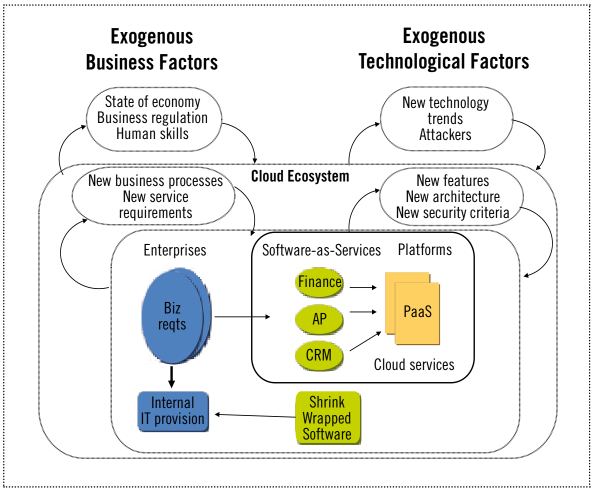


Figure 2: Fast and slow dynamics of the cloud ecosystem

MODELLING FOR POLICY AND STRATEGY

In our analysis of this ecosystem, we draw quite significantly on research carried out on ecological ecosystems.[3] The ecological ecosystem consists of various organisms that exist in a habitat or a series of linked habitats. The ecosystem will be affected by the way in which the organisms interact (because of their biology) as well as external influences such as the weather, fires, or pollution. In studying an ecosystem and its dynamic behaviours, we can start to see how resilient it is to different shocks and so start to manage it in a sustainable way. Analysing cloud-based services ecosystems from such a perspective leads us to develop helpful stewardship concepts.

Instead of organisms in various habitats, we have an ecosystem of cloud stakeholders. Instead of the interaction between these entities being driven from their biology, it is driven by their need to maximise (or at least satisfice) their utility, so influencing their policies and decisions. This utility will usually be implicit in each company's decision making, but will drive a customer's choice of services, as well as the terms and conditions offered by the service and platform providers.

We have developed a series of economic and mathematical models that explore numerous aspects of the emerging cloud ecosystem. Based on these models, we have developed one rich system model that has (hundreds of) firms consuming IT, (hundreds of) firms offering services, and several platform providers offering IT resource capacity. Unlike our preceding models, which have been based on empirical studies or well-established economic methods, this model is designed to allow security professionals (and other stakeholders) to visualise and explore the implications of exogenous and endogenous factors on cloud stewardship.

The system model can be executed to simulate a range of phenomena: consuming firms' switching from internal IT to the cloud, or changing service providers; new service providers entering the market with different cost and security properties; and new platforms offering different conditions for the service providers. The behaviour of each

THE AUTHORS

Professor David J. Pym is 6th Century Chair in Logic and SICSA Professor of Computing Science, University of Aberdeen

Dr. Simon Shiu (M.Inst. ISP) is a senior research manager at HP Labs Bristol

firm is conditioned by utility functions that govern, for example, whether they will prefer a secure but restricted service to a cheap and flexible one.

There are a number of parameters so that we can explore. For example, the average difference in outcomes for firms with different stewardship priorities, or the relative success of different policies and attributes of platforms and providers. Soon we hope to be able to explore and illustrate resilience of this ecosystem to shocks such as massive and swift reductions in available (financial) capital, or the impact of major (ecosystem-wide) security failures.

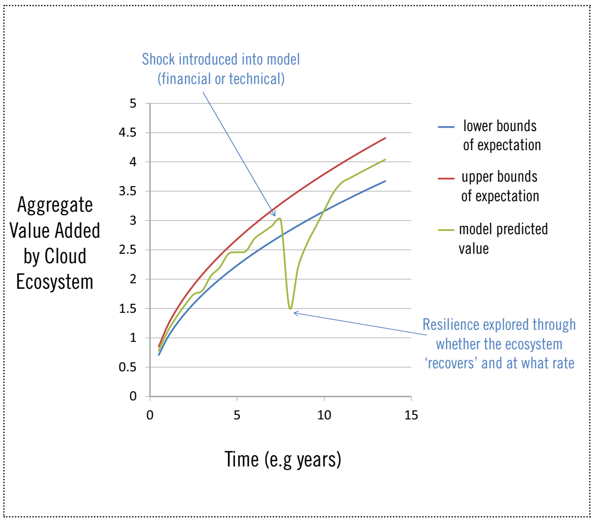


Figure 3: Illustrating how sustainability and resilience will be explored

Figure 3 shows a typical target output of a simulation based on the model. Clearly, much will depend on how the model defines (and stakeholders interpret) 'value added by the ecosystem'. The point is to explore and discuss the conditions that will lead to shocks – for example, an economic shock such as a 'credit crunch', a highly intrusive malware incursion, or a radical shift in infrastructure technology – and what attributes are important for resilience, recovery and, ultimately, sustainability.

The model has been developed as part of the UK Technology Strategy Board-funded 'Cloud Stewardship Economics' project. This project, led by HP Labs' Cloud and Security Lab, brings together companies (Sapphire, Validsoft, Marmalade Box), mathematicians and economists from the Universities of Aberdeen and Bath, Lloyd's of London, and the IISP. In this project, we have performed a series of empirical studies of how it is that certain enterprises are consuming cloud services, and how they manage stewardship concerns. We have used these studies to develop a series of economic models, including a switching model, that uses real option theory to help firms re-use all the financial modelling (taking into account the time value of money) associated with valuing different states and handling uncertainty, in the context of whether and when to 'switch' from internal IT to cloud computing. We have also developed models of macro-migration behaviour and the expected benefits of on-demand services, which we have used to inform and calibrate our system model.

ENGAGING THE PROFESSION

We plan to use this model to support scenario-planning workshops with security professionals and other stakeholders in order to generate new ways of thinking about cloud risk and security. We also plan to develop pragmatic decision-support tools for cloud stewardship.

We still need to develop our models, and our modeling infrastructure, to support real-time simulation that allows clients to explore the influence of parameters that are endogenous and exogenous to the cloud market. We will also make further efforts on refining and encompassing ongoing conceptual and economic research on cloud stewardship. Our next step is to take our current model and scenario plans and run a workshop with the IISP members in the spring of 2012.

Simon and David will be talking about this project at the London Branch meeting on December 8th 2011 at Accenture.
Please see www.instisp.org for more information.

Footnotes:

[1] Stewardship can be considered to be the maintenance of effective institutions to facilitate or encourage activities that are deemed important.

[2] This ignores many of the drivers involved in creating services that exploit large scale security and easy to use 'platforms', but allows us to concentrate on interactions nearer the business layer.

[3] We have also been influenced by work on stewardship in financial reporting.

REGIONAL BRANCH UPDATE

A round-up of recent activities and plans for 2012 from our branches around the country.

TOP GUN – WAR OF THE ROSES

As you are reading this, the North East and North West Branches of the IISP will be battling it out as part of the 'War of the Roses' IISP Top Gun Workshop series (Tuesday 29th November).

Which branch won the battle of the North? Find out in the December IISP Bulletin.

NORTH EAST BRANCH

As mentioned above, the North East Branch has been busy preparing for their battle with the North West.

The Branch is keen to work with CLAS consultants in the North East area to help the IISP deliver the CESG Certified Professional Scheme, so if you are interested please contact ccp@instisp.com

In 2012, we will also be looking to establish stronger links with other branches in the area such as the BCS.

Mark Grover – *Chairperson*

NORTH WEST BRANCH

The work of the North West branch was well represented in National Computing Centre seminars on Bring Your Own Device. The seminar took the risk assessment and considered how to organise the mitigating controls into a coherent policy. The conclusion was to make a commitment to do things correctly. Measure twice and cut once. Select your security measures according to the risks you face. And write them down so you're less tempted to change them on the fly. If you're tempted then you've made a mistake with your risk assessment in the first place and your risk appetite has just increased to that of an Israel Bonds seller at the meeting of the Arab League.

Danny Dresner – *Chairperson*

SCOTTISH BRANCH

The information security industry in Scotland is busier than ever, with more projects in financial services, oil and gas, public sector, manufacturing, logistics and retail. In the Scottish branch we hope to reschedule the talk by the anti-terrorism squad of Lothian and Borders Police before the end of the year, but would also like to get a pipeline of speakers sorted out. For this to work we need you to help identify topics and volunteer or help us get in touch with speakers.

Rory Alsop – *Chairperson*

LONDON BRANCH

The London Branch will convene for the last time before Christmas on Thursday 8th December.

Simon Shiu from HP Labs will discuss the Cloud Stewardship Economics programme, while IISP Chairman and Global Managing Partner of the Security Practice at Accenture, Dr Alastair MacWillson, will talk about his proposed visions and strategies for the Institute.

IISP Chief Operations Officer, Triona Tierney, will also provide an update on the CESG Certified Professional certification scheme.

The next instalment of the London lecture series will occur in early February.

Ryan Rubin – *Chairperson*

SOUTH WEST BRANCH

The autumn schedule for the South West Branch has seen two very well received talks, each focusing upon topical threats that require attention.

The first talk, on 10 October, was entitled 'Web 2.0 Applications - Do they help your Business?' by Paul McKay from Bond Pearce LLP. The presentation examined how social networking services such as Twitter, Facebook, and LinkedIn are now being used within the corporate world, and considered the benefits and risks that this can represent for the organisations concerned.

On 1 November, we saw a presentation from Alan Cottom, solutions architect with Stonesoft, entitled 'Advanced Evasion Techniques (AET): Are they being used to bypass your security?'. The talk explained the threat posed by AETs, and demonstrated their potential to bypass existing intrusion detection and prevention tools.

Both talks were hosted at Plymouth University as joint events with the South West branch of the BCS. Links to the talks themselves are available on the IISP website.

Steven Furnell – *Chairperson*

NORTHERN IRELAND BRANCH

It was with regret that the meeting in September was cancelled.

The Branch has two volunteers keen to be either Interviewers or Assessors for IISP membership and will soon attend training with the intention of increasing membership in Ireland (North and the Republic).

As always, please keep me informed of any topics that you would like discussed at a future meeting.

Roger Millar – *Co-chairperson*

THE ROLE OF NETWORK FORENSICS IN CYBER DEFENCES

David Bird and Brian Mallinson discuss whether digital forensics be extended beyond a niche discipline and prove useful as an arm of tactical cyber defence.

Experience tells us that the compromise or loss of information can cause untold reputational damage that, in turn, may inevitably affect the financial bottom line. Information security (Infosec) and information assurance efforts over recent times have been striving to narrow the attack vectors open to nefarious threat actors stretching out their tentacles of intent from the 'wild'. We have seen from recent government and press announcements that cyber security is now at the forefront of our consciousness. We are more at risk from global information warfare capabilities than we have ever been and organisations should now be more attuned to the need for boundary defences in the cyber context.

...wouldn't it be advantageous to have the evidence as proof rather than using traditional forensics hindsight?

THE NEED FOR PROTECTIVE MONITORING FRAMEWORKS

Today, organisations must operate as safely as possible in the knowledge that at some undefined moment unknown vulnerabilities may be identified, or unauthorised changes undertaken, within their IT environments that can be the root cause of potential security incidents. The paper by Z. Chen et al (2006), *An Inline Detection and Prevention Framework for Distributed Denial of Service Attacks,* republished by Oxford University Press in 2007 has investigated defence mechanisms for the identification and classification of Distributed Denial of Service (DDoS) attacks and it reinforces the importance of protective monitoring frameworks. This is especially important when we consider the following topical areas that were raised at the Infosec 2010 event at Earls Court, which proves that such capabilities should in no way be undervalued:

- ⇨ *The 'insider threat' is still a concern because users are oblivious to the risks and this is not adequately addressed through security training;*
- ⇨ *There is an increased trend in malware-based incursions through malware obfuscation;*
- ⇨ *Pay-as-you-go DDOS attacks as a 'service' is a reality.*

So the threat is there whether it is based on externally or internally initiated actions. Where does that leave us when we know network assaults have the capability to successfully penetrate even stateful firewalls? If all else fails, it would seem that computer forensics has become a last bastion of defence, where techniques are used to try and fathom out how an incident may have occurred, what data, if any has been leaked, lost, or damaged and by whom; whether it be by data exfiltration, accidental release or through deliberate actions.

Obviously this would not be the preferred approach for most organisations because it would invoke the need for dead computer forensics techniques to acquire derived evidence – traditionally causing the isolation of servers for forensics imaging activities and the safe storage of server disks for evidential purposes – thus causing downtime costs, availability issues and the time consuming need to restore data from backup to continue normal operations.

WHY NETWORK FORENSICS?

Let us alter our perspective slightly and redefine computer forensics, which is commonly understood as a discipline that applies to computer investigations in order to facilitate the gathering of forensically sound electronic evidence. It is widely accepted that all actions in ICT environments leave a digital trace of some kind or other – whether in system logs, erased files on disk, time stamps of modified files and the like – the key is how to find such electronic evidence and use it effectively to prove that a suspected security incident or crime has actually taken place.

Although it can be argued that protective or configuration monitoring implementations provide alerts of unauthorised events in near real-time, more often than not security breaches are not necessarily always identified until weeks or months after-the-fact due to the sheer volume of logs that need to be analysed. But wouldn't it be more palatable for organisations, who value their data's confidentiality, integrity and availability, to be able to track attackers and differentiate the methods employed by them to undertake unauthorised internal network activities? And wouldn't it be advantageous to have the evidence as proof rather than using traditional forensics hindsight?

Network forensics techniques are an answer to this problem. Outside the true definition of the computer forensics remit, it is feasible that data can be captured in transit and analysed off-line in order to complement Security Incident and Event Management methods; that is, not necessarily be enacted post-incident but be actively employed as another sensor as an extension of protective monitoring.

How could this be done? Through solutions that employ network forensics capabilities, volatile data transiting organisational networks can either be netted using the 'catch-it-as-you-can' technique or filtered to discern relevant data for extraction using the 'stop-look-listen' methodology. 'Stop-look-listen' is more a selective packet inspection approach, requiring high-powered processing to avoid latency, within its data extraction process and would be more appropriate because 'catch-it-as-you can' presents privacy issues when transient data is cached in bulk.

However, in either case, to a greater or lesser extent depending on the approach, network traffic is cached into storage for evidence preservation and would also need to be replicated; with the data replication being the associated source for the off-line analysis using forensics-based analysis methods and not the raw data cache itself. But caution is required because this process will still have to be compliant with the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations of 2000 and the collected data would also need to be prescriptively captured within the bounds of necessity and proportionality for legislative compliance. If deemed to be evidential through analysis, the stored data cache would also need to be securely archived using an ascribed chain-of-custody and isolated from the solution's replicated data in order to minimise contamination for further lawful purposes.

BRIDGING THE GAP

In essence digital forensics techniques can offer additional options to operational security, which actually provide creditable capabilities to bridge the gap somewhere between intrusion detection and a fully-fledged investigation – the latter being a place where it can be argued that most organisations do not want to be. As a protective monitoring enhancer, the less intrusive network forensics 'stop-look-listen' technology coupled with digital forensics analysis could be used to identify efforts to circumvent an organisation's network-borne technical security and the resultant actionable information could then be cross referenced in conjunction with other intrusion detection efforts to provide a richer digital counter-insurgency effort.

A deployed network forensics capability, and the supporting team, would enable more informed data compilation, the generation of better and more effective trend analyses – as dubious activities are categorised over protracted periods of time – to supplement and enhance current intrusion detection solutions. Assisted by the use of visualisation tools, this facet could be used to gather real evidence and trigger remedial actions in order to quash weaknesses closer to when they unfold as electronic defences are permeated, rather than wait until after a time-consuming retrospective investigation has been conducted. Of course more automation of the data analysis process would be desirable, but this will only come with more investment in the field and through a greater uptake of such technology.

SUMMARY

In summary, various technologies have been implemented by organisations in the past providing veritable layers of protection in order to limit the risks posed by external threats. The computer forensics tradecraft has traditionally been viewed as a specialised discipline and defined by its role in post-incident security breach investigations, the preservation of evidence and its lawful submission for disciplinary, civil or criminal proceedings.

However, digital forensics techniques could now be deployed offering more to Operational Security Management than is the case currently and be employed as an enabler to further mitigate risks associated with our interconnected world. Rather than an organisation having to unwittingly react after-the-fact on the diagnosis of a suspected security breach caused by unauthorised changes, malicious or erroneous intent with respect to network traffic ingress/egress, network forensics could assist current intrusion detection capabilities.

By leaning towards discriminatory data capture using 'stop-look-listen', and through the use of digital forensics analysis expertise, better unauthorised network activity trend information can be collated, aiding remediation for intrusion prevention modus operandi. Network forensics can therefore provide a more informed perspective for protective monitoring, vulnerability rectification and, if appropriate, prosecution based on collated evidence within the bounds of the law.

More investment would provide faster computational ability for in-flight data collation and on-the-fly data analysis, and therefore establish greater transparency in the production of actionable results from the process. This tactic would proactively assist organisations in the safeguarding of information and could head off financial and reputational damage that may be inflicted once a security breach has been identified. Thus for its part, if used appropriately and with more adoption and technological advancement, network forensics could help provide a more thorough cyber defence within the context of today's information age.

THE AUTHORS

David Bird is a senior CLAS consultant and Associate member of the IISP

Brian Mallinson is an established computer forensics practitioner

THE NEED FOR SECURITY RISK MANAGEMENT 3.0

With the explosion of consumer devices in the workplace, increased demand to access information anytime, anywhere combined with a young workforce and an ever-changing threat landscape, are our traditional security risk management practices agile enough to cope with tomorrow's challenges?

In the last decade we have witnessed a significant change in the field of information security. Software vendors are delivering more secure systems but struggling to keep up with increasingly innovative, motivated and organised attackers. Despite the use of maturing countermeasures and safeguards, attackers have now changed their strategy towards weaker targets such as the end users. Industry standards, government regulation and highly publicised security breaches are among the many factors that have increased demand for an Information Security Risk Manager role.

THE CURRENT THREAT LANDSCAPE

Security risks still plague all businesses, large and small. Insider threats are high on the agenda for fraudsters and are often the easiest way to gain unauthorised access to information. Employees continue to leak data intentionally or unintentionally due to increased use of removable media, mobile devices, remote working and use of the web and/or social media.

Increased reliance on third party suppliers supporting business activities opens organisations up to wider exposure beyond corporate boundaries. Despite the rapid adoption of web-based applications using web 2.0 technology by consumers, software developers still struggle to remove the most basic web application security threats such as SQL injection from their applications. Young employees entering the organisation are less intimidated by technology and have grown up sharing information and ideas, and collaborating with friends online – they expect to continue carrying out these activities within the workplace despite potential corporate risk exposure.

Finally, there are the advanced persistent threats from foreign governments and/or competitors seeking to gain Intellectual Property or cause business disruption in order to gain competitive advantage.

Employees continue to leak data intentionally or unintentionally due to increased use of removable media, mobile devices, remote working and use of the web and/or social media.

THE NEED TO TAKE CONTROL

Demands on Information Security Risk Managers are growing out of control. Many information security functions are overwhelmed by a mountain of tasks for managing information security risk across the organisation and have to balance the following priorities:

- *Keeping on top of the information security threat landscape in a world of new technologies, applications and business services;*
- *Keeping the business safe from these threats while allowing it to take advantage of new opportunities as it continues to grow (e.g. cloud computing, home working, third party outsourcing);*
- *Maintaining a level of security controls in-line with legal and regulatory requirements;*
- *Performing the business-as-usual activities of defining and often policing security policies;*
- *Responding to security incidents – often in crisis mode after a breach has occurred.*

To manage emerging security threats, the information security industry continues to use security mitigation techniques developed to deal with past threats and not necessarily the changing and rapid threats of today. In our industry, we don't seem to retire security technologies, though obviously some approaches, such as public key encryption algorithms have stood the test of time. Is there a need to revisit the effectiveness of other technologies and practices – anti-virus, intrusion detection, frequency of password changes, use of passwords as a primary authentication mechanism etc.?

COMMON DEPARTMENT RISKS

Security departments are also exposed to their own challenges which will impact upon their effectiveness and efficiency to protect information assets and achieve security goals for the business. These challenges include:

- *Managing the demand for information risk management services;*
- *Extracting valuable information from the variety of information sources collecting data;*
- *Stepping away from fire fighting to a more controlled and sustainable state;*
- *Managing stakeholder expectations effectively;*
- *Extracting value out of existing investments;*
- *Leveraging point solutions to support strategic initiatives;*
- *Keeping on top of emerging threats to the organisation;*
- *Being bypassed by the business who do not want to hear no for an answer;*
- *Lacking internal resource to meet demand;*
- *Lacking transparency on progress which makes it harder for the department to justify its existence and add value to the organisation;*
- *Complying with increasing amounts of regulation which may divert focus;*
- *Reacting fast enough during security incidents;*
- *Retaining specialist staff required for specific services – key management, incident management, security testing.*

COMMON INFORMATION SECURITY MYTHS

The situation is not helped by the following myths which mask management's perception of information security within the business:

- *It is possible to be 100% secure – this sets an unachievable task for those in information security;*
- *The security manager is responsible for the security of the organisation – everyone is responsible and accountable for security in some way;*
- *We have technical security controls (firewalls, AV, IDS, DLP) therefore we are secure. – an holistic approach to security is required beyond IT;*
- *We are certified to ISO-2700x or PCI DSS therefore we are secure – compliance is a journey and not an end destination;*
- *If we appoint a security manager our job is done – this is only the beginning of the journey;*
- *Security is still perceived as a blocker not an enabler – sometimes the department still has to say no to manage business risk effectively.*

WHAT IS OUT THERE TO HELP?

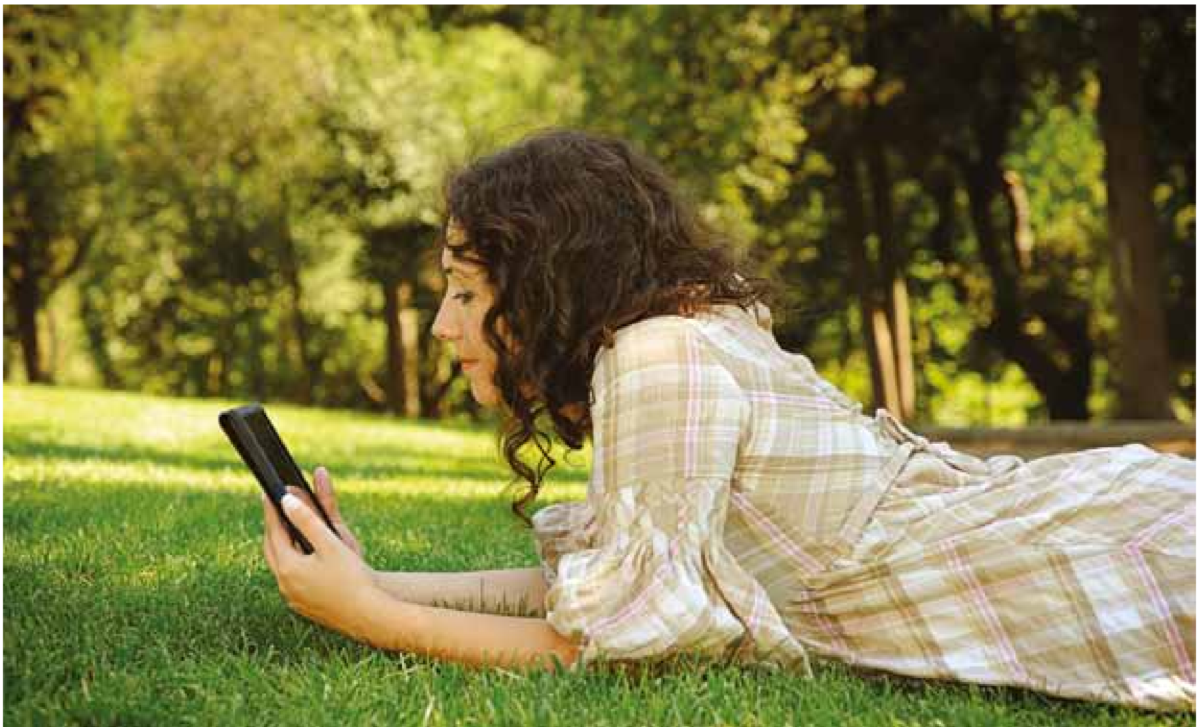
Security standards such as ISO-2700x and PCI DSS provide a wealth of guidance and insights into how organisations can manage information security risk more effectively. Many of these standards are further maturing and gaining wider acceptance internationally. However, these often require mature security organisations to be implemented (and thus can be too much of an overhead for smaller organisations or those will small security budgets) and can take significant time and resources to embed within large complex organisations. Information Security Risk Managers need to take a more agile approach and pragmatic view on adopting good practices, and move towards these standards at a rate that meets the organisation's appetite for risk. Unfortunately, unless the organisation is forced to comply with requirements for marketing or legal/ regulatory reasons, there is often no clear driver to fully embrace these standards.

STEPS TO REGAIN CONTROL

To manage security risks effectively, Information Security Risk Officers need to build the following into their information security transformation plan in order to reach a sustainable and controlled state:

- *Establish a clear security strategy and boundaries for the security function to operate within;*
- *Engage with key stakeholders across the organisation to drive sustainable change;*
- *Establish a security services catalogue and communicate this to manage stakeholder expectations;*
- *Separate 'business-as-usual' operational activities from 'project / programme' activities, both are important and need adequate resource allocation;*
- *Establish a reporting process which links security improvement metrics to organisational Key Performance Indicators (KPIs);*
- *Raise awareness throughout the organisation to change security culture and perspectives;*
- *Partner with other risk management functions including business continuity, physical security and operational risk to establish a common risk language to engage the business with, and leverage and share resources;*
- *Simplify security policies for all to understand – define policies that are tailored for the users reading them;*
- *Maximise existing security investment – make the most of the security and risk tools already purchased by the organisation;*
- *Develop depth in repeatable security processes such as: joiners, movers, leavers, project engagement, compliance readiness and attestation, logical access management (LAM), software development lifecycle.*

By carrying out these activities, Information Security Risk Officers can gain some much needed time to focus on what matters the most within the organisation and harness available resources effectively to deal with the onslaught of increasing threats to their organisation. In doing so, they can help the organisation to proactively reduce key security risks using safeguards aligned to their corporate business risk appetite.



THE AUTHOR

Ryan Rubin, of Protiviti, is Chairperson of the IISP London Branch.

Cyber Security Challenge UK

CYBER SECURITY CHALLENGE – AN INSIDERS'S VIEW

Simon Walker describes how participating in the Cyber Security Challenge helped to launch his security career.

'UK SEEKS NEXT GENERATION OF CYBER SECURITY SPECIALISTS'.

Those were the words proclaimed on the BBC website in July 2010. The BBC article was referring to the Cyber Security Challenge, a new initiative backed by both the government and major businesses to reduce the shortage in skilled information security professionals. Those words are also the reason I have the opportunity to write this article.

For the past fifteen years, I have been working as an IT consultant specialising in a large ERP software solution. For even longer than that, I have had an interest in computer security. My interest started at university in the 1990's, during which time the World Wide Web was starting to grow out of the existing military and academic networks. At that time, most of the security research seemed to be centred around buffer overflows and weaknesses in common protocols such as SMTP (for email) and TCP/IP (for the internet). General security information was hard to find but there was already an 'underground' movement in which new research and exploits were being shared. During those three years, I learned much about vulnerabilities of the popular operating systems and software. Alas, university was soon at an end and computer security jobs seemed to remain the domain of the graduated computer scientists, so I looked for a different career choice.

Figuring that the world would always need accountants, I started to train as a management accountant in a large retail company. With my newly found understanding of computers, I quickly gained knowledge of the existing finance system and was seconded to work on the implementation of a new one. Within a year of the go-live, I had left the company to become a consultant instead. The benefits of consulting would give me exposure to a variety of operating systems, databases and the complete software lifecycle. With so much to learn at work, my security research was limited to securing my own servers at home and reading security mailing lists such as bugtraq and full-disclosure, but I still had the idea that one day I would move in to a security-related career. With that in mind, I looked at certifications that I could study in my own time to boost my chances. This was the point at which I hit the 'chicken and egg' scenario of lack of experience versus lack of qualifications. There did not seem to be associate programmes in any of the security institutes and professional bodies that would allow someone outside of the industry to start a new career. With my path apparently blocked, I carried on with my consulting for several years until I read that BBC website article.

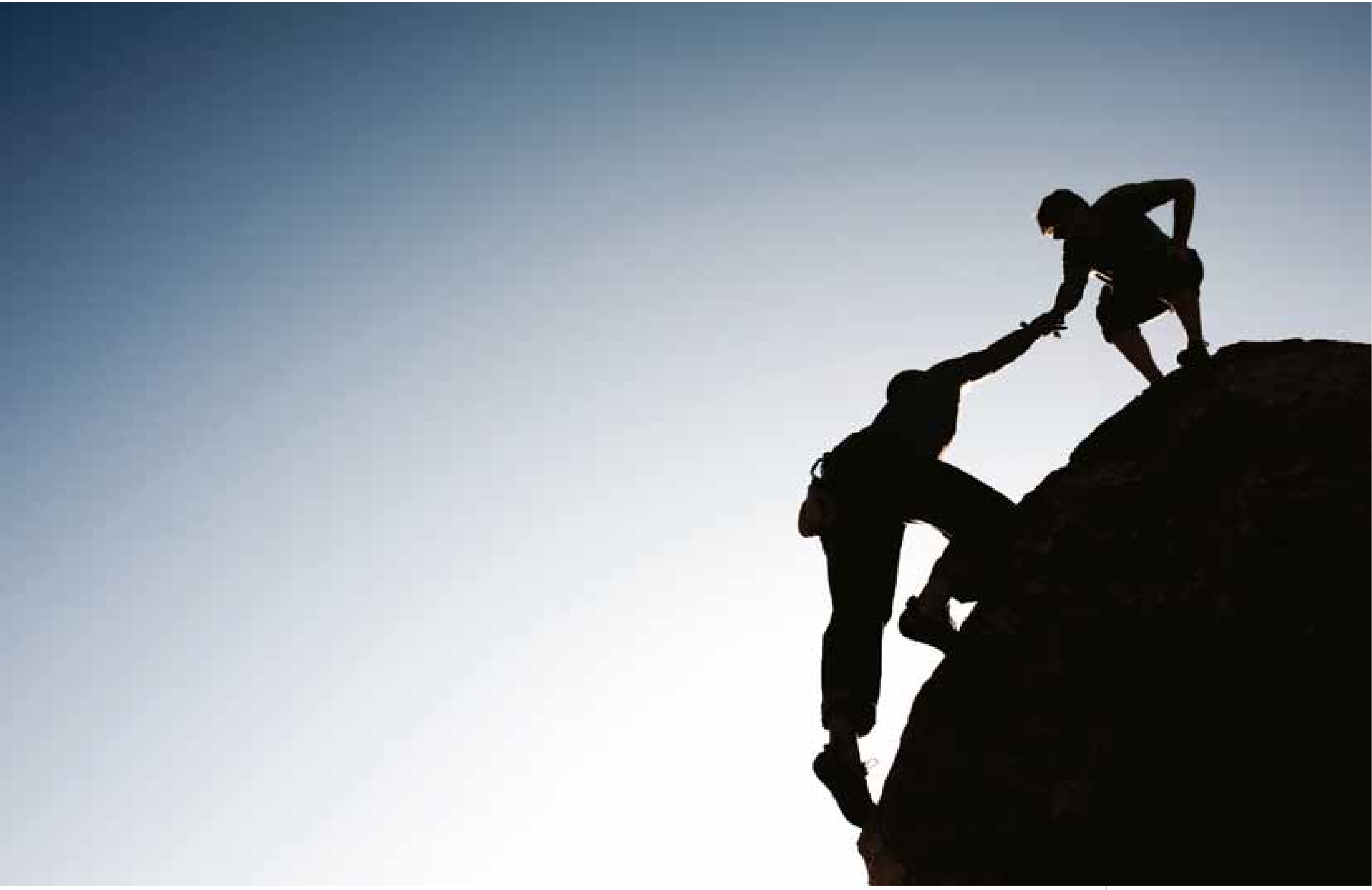
The Challenge and the IISP are now providing the support that was so lacking when I was looking to start my security career

GETTING STARTED ON THE CHALLENGE

At first, the Cyber Security Challenge Treasure Hunt sounded like a bit of fun. I thought I knew a little about cyber security so it was a good way to measure my abilities, or lack thereof. The first round was split in to three multiple-choice answer parts: a general computing section, a security section and a more practical security simulation. After a couple of hours, I submitted my answers and waited for the score. With the competition taking place over several weeks, a leader board was made available on the Challenge website with the top 25 going through to the next round. With a little surprise (and a self-indulgent smile!), I found myself in about tenth place. The next couple of weeks were tense with more results being posted and my score slowly slipping down the board. However, I was soon to be greeted with a congratulations email and a place in the next round, ominously titled 'Head to Head'.

THE 'EXAMINATION'

Roll forward to early 2011 and the top scorers were at Sophos headquarters. We were nervously sitting in the reception area not knowing what to expect (although in hindsight the work that Sophos undertakes should have provided a big clue). For this round, we were given ten virtual machines that had samples of real life malware installed. The task was to find the malware, describe what it was and how it infected the system, all against a strict time deadline. Feeling every bit like an examination, time pressure was the issue, with too long spent on the early samples, leaving little time for the latter ones. At the end of the test there was a debriefing with a Sophos expert, giving an analysis of the answers. Like most of the other competitors, I was feeling a little deflated with the thought that I had missed many of the required details. Finally, there was the countdown of the scores, with the top few going through to the Masterclass final. To say I was a little surprised is an understatement when it was announced



that I was in first place. At this point, I knew I was going to get an impressive prize from the list that the sponsors had put forward and it was onwards to the Masterclass final.

THE MASTERCLASS FINAL

The final was hosted at HP Labs in Bristol a few months later. The format this time was changed to a team competition. One part of the challenge was to pitch a new IT security policy to a fictitious board of C-level executives, played by Challenge members. Another part was to defend a network against a series of cyber attacks in a virtual simulation. Both of these are very much real world challenges that employees could face in their information security careers. The network defence simulation was fast and frenetic, with multiple devices to monitor and intrusions to report. I learned that the same type of simulation is being used to train future cyber warfare personnel in the USA. The IT security pitch was no less stressful, with the executives questioning every decision made and probing for weaknesses in the policy design. The finale of the event was a dinner and awards ceremony. I had the pleasure of sitting next to Baroness Neville-Jones and even managed to join in a discussion on government cyber policy! I was not crowned the overall Cyber Security Champion (that honour went to Dan Summers) but I did receive my main prize as winner of the Treasure Hunt – a three-month internship at PwC.

THE PRIZE-WINNING PACKAGE

The length of the internship at PwC meant that my current employment would have to end and I admit to having a few sleepless nights thinking about the risk of moving in to a new career. However, in May I joined the Threat and Vulnerability Management team at PwC as in intern (albeit an old one!). The team specialises in penetration testing, which I considered a rather technical, but glamorous, endeavour. I was able to spend time with several of the team learning the different aspects of testing and also shadow team members as they worked on client sites. The whole experience was extremely valuable and gave me a clearer understanding of the work involved. Penetration testing does have its glamorous side but there are also the reporting and client relationship aspects to the role as well. As part of my prize-winning package, I was also given free entry to the CREST registered tester exam. I managed to pass this exam, which I hoped would give me a better chance of securing a permanent place in the team. The director of the team described the internship as 'one long job interview'. With the three months nearing completion, I was given the news that I had been waiting for. PwC were offering a permanent contract and it did not take me long to gratefully accept it.

Since then I have continued my journey in to the information security world. With PwC being such a large organisation, I have gained an appreciation of other areas of security that I had never even considered, such as governance, audit, data assurance, and even crisis management. Being successful in the Challenge has also brought some additional benefits, such as attending media events, including an invitation to talk at the IISP Graduate Development Programme in August.

As for the Challenge, this year there are even more sponsors and competitions available. The Challenge website has also been refreshed, with the IISP providing information on career paths, jobs and qualifications. The Challenge and the IISP are now providing the support that was so lacking when I was looking to start my security career. For my part, I can only say that the Challenge has been a great success.

THE AUTHOR

Simon Walker is a Senior Associate in Threat and Vulnerability Management at PricewaterhouseCoopers and in August spoke at the IISP Graduate Development Programme meeting.

YOUR INSTITUTE

THE 2011 ANNUAL GENERAL MEETING

The Institute's 5th Annual General Meeting was held at PwC's Embankment headquarters in London on the evening of Monday 7th November 2011.

The IISP Board and the Secretariat were joined by nearly 100 IISP members, many of whom had the opportunity to vote in the Board elections as Full Members.

Nine candidates stood for six positions on the Board, with three new Board members elected – David Alexander, Andrea Simmons and Piers Wilson – while current Board members – Alastair MacWillson (Chairman), Nick Seaver (Treasurer) and Alan Stockey were re-elected.

Alastair MacWillson presented his objectives and strategy for the Institute going forward – available at www.instisp.org – while Nick Seaver provided the Treasurer's report.

The AGM preceded two prominent keynote speakers: Jonathan Hoyle, Director General for Information Security and Assurance at GCHQ and Dr. John I Meakin, Chief Information Security Officer at BP.

Hoyle highlighted the role that professionalism in information security would play in enhancing the UK's economic prosperity, while Meakin announced that BP had integrated the IISP certification process into their IT professional skills and Licence to Work processes.

Special thanks to our speakers, PwC for kindly providing the venue, and Ultima Risk Management and Qinetiq for sponsoring the catering.

ACADEMIC PARTNERS

The IISP is delighted to announce the launch of Academic Partner status. Open to those universities offering courses in information security-related topics, the following four universities have successfully applied for Academic Partner status:

- ⇨ *City University;*
- ⇨ *Oxford University;*
- ⇨ *Plymouth University;*
- ⇨ *Royal Holloway University of London.*

About the Programme

Academic Partnership provides an opportunity for the IISP and academic institutions to collaborate and ensure the effective promotion of information security professionalism to staff and students. The award of Academic Partner status aims to recognise the significant base of security-related expertise and activity that exists within academic institutions, and to encourage and enable a dialogue between academia and the wider community of security practitioners.

If you would like further information regarding this programme please contact julian@instisp.com; alternatively you can download the application form at www.instisp.com/academic.

CESG Certified Professional
IACF: v1.1

THE IISP CESG CERTIFIED PROFESSIONAL SCHEME

As part of the Government's investment in cyber security, the IISP consortium has been appointed by CESG to provide certification for UK Government's Information Assurance (IA) professionals. This appointment grants a licence to issue the CESG Certified Professional (CCP) Mark as part of a certification scheme driven by CESG.

The certification process is designed to increase levels of professionalism in Information Assurance and uses the established IISP Skills Framework to define the competencies, knowledge and skills required for specialist IA roles. Developed through public and private sector collaboration by world-renowned academics and security experts, the IISP Skills Framework has been adopted by GCHQ as the basis for its CESG Certified Professional specification.

This certification builds on the IISP's existing competency-based membership programmes, so not only will an individual be certified, but their areas of specialism will be recognised, offering the individual and their customers' greater confidence that an individual has the right skills and experience for a role.

The consortium comprises three organisations, all of whom have gained significant reputation within the IA profession: the IISP, who will certify competency against the skills framework, in line with existing Associate and Full Member processes; the Council of Registered Ethical Security Testers (CREST) who will provide robust examinations for the more technical roles, and Royal Holloway's Information Security Group (RHUL), adding their considerable experience and expertise in setting rigorous and consistent assessment processes.

Certified roles

This certification will develop further, and the initial roles identified are detailed below. All roles have three levels of certification, at practitioner level, at senior practitioner level and at lead level, thereby helping those working in IA to identify a career path.

The roles are:

- ⇨ *Accreditor;*
- ⇨ *IA Auditor;*
- ⇨ *Communications Security Officer/Crypto Custodian;*
- ⇨ *IT Security Officer;*
- ⇨ *Security & Information Risk Advisor;*
- ⇨ *Security Architect.*

The CCP roles broadly map into the IISP membership levels at:

- ⇨ *Practitioner – Associate Member (A.Inst.ISP);*
- ⇨ *Senior Practitioner and Lead – Full Member (M.Inst.ISP).*

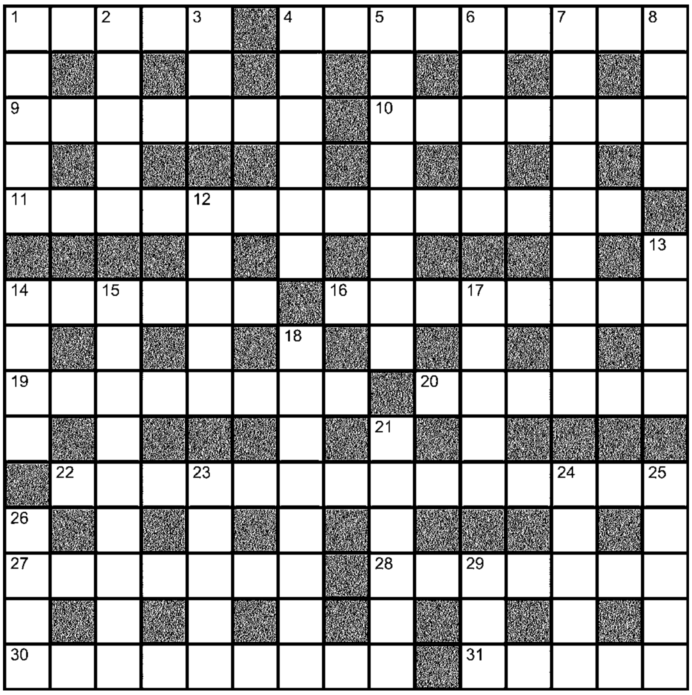
This means that an individual can attain both IISP membership and CCP certification with a single application.

ITPC holders

Those individuals that currently hold the ITPC certification, and for whom CPD points are up-to-date, have already demonstrated competence against many of the skills required.

The IISP scheme will recognise the ITPC competency profile, and candidates who hold the ITPC will only need to demonstrate competency against the delta between the role applied for and the ITPC profile.

CRYPTIC CROSSWORD by DREX



Across

1 Sandwich – like an end? (5)
4 Run a tally encrypted – of course (9)
9 Obstruct attack (7)
10 Suit the human period, right? (7)
11 Drunken heretics buy car – a possible cause of reputational damage (8,6)
14 Imaginative author with convulsive twitch (6)
16 Gesture in cyberspace? Point with fear and anger, for example (8)
19 Grand handouts everywhere (8)
20 US magazine cut identification to deny access (6)
22 Assessment of risk's consequences troubled a talismanic spy (6,8)
27 One of eight arms on a freak (7)
28 Come on, lunatic! Monkey tail has been struggling for a few years now (7)
30 Management of risks – goody intended I hear (9)
31 On that point, you are about right (5)

Down

1 Common connections for communications and people transporters (5)
2 Restorative relative key (5)
3 Lad turned up-side-down hooligan (3)
4 Reverse Chester-le-Street wicket (6)
5 Confused bimbo met exploding ticker (4,4)
6 Fruit – not top class (5)
7 5 in cyberspace perhaps reason with a lot of money (5,4)
8 Measure quad (4)
12 Arrests amongst hellfire insurrections (5)
13 Thought profoundly decapitated and victimised (4)
14 What denotes location of Unix file, secretary took home at first (4)
15 Cloud business (1-8)
17 Goblin recedes, first wearing ring (5)
18 Example made out of ancients (8)
21 What a viruses do to a computer, left out of turn (6)
23 Accept university following publicity (5)
24 Without fire, none found! (5)

HOW TO WIN THE PRIZE!

This issue's codeword is concealed within the crossword and can be solved by completing the numbered boxes below as you solve the cryptic clues.

27	10	4	22	14	29	2	16	4	19

If you discover the codeword, please email it to events@instisp.com.
Closing date is 12.00 on Friday 13th January 2012, and the winner will be drawn at random from correct entries at the time. A prize of £40 in Amazon vouchers is on offer to the winner. Good luck!

Last issue's codeword was 'applicable'. The winning entry was submitted by Richard Weatherill, who won the prize of £40 in Amazon vouchers. Congratulations, Richard.

LAST ISSUE'S SOLUTION

P	A	R	A	L	L	E	L	■	B	■	■	M	■	B
■	R	■	P	■	Y	■	O	V	E	R	T	A	K	E
S	T	O	P	■	M	■	G	■	T	■	■	G	■	G
■	E	■	R	E	P	R	I	M	A	N	D	I	N	G
■	R	■	E	■	H	■	C	■	■	■	I	■	■	A
Z	I	N	C	■	O	■	A	N	C	E	S	T	O	R
■	A	■	I	■	I	■	L	■	■	■	P	■	■	L
C	L	E	A	R	D	E	S	K	P	O	L	I	C	Y
H	■	■	T	■	■	■	E	■	R	■	A	■	R	■
E	C	L	I	P	T	I	C	■	O	■	C	H	I	P
R	■	■	V	■	■	■	U	■	T	■	E	■	P	■
U	N	D	E	R	P	E	R	F	O	R	M	■	P	■
B	■	A	■	■	I	■	I	■	C	■	E	E	L	S
I	N	T	E	R	N	E	T	■	O	■	N	■	E	■
C	■	A	■	■	G	■	Y	U	L	E	T	I	D	E

MORE FULL MEMBERS OF THE INSTITUTE – M.INST.ISP

We would like to congratulate the following IISP members who have, since the publication of the previous issue of *Pulse* in July, achieved the Institute's professional accreditation, M.Inst.ISP. Well done to you all!

Tracy Andrew
Gary Brophy
Peter Fischer

Tim Harwood
Peter Herdman
Roland Johnson

Ian McKinnon
Brian Morrison
Tony Seymour

LETTERS TO THE EDITOR

THE VALUE OF INFORMATION SHARING

Dear Sir,

I feel moved to respond to the letter from Steve Thomas in the Spring issue of *IISP Pulse*. Steve is absolutely right with regard to organisations' reluctance to share details of security breaches for some very well established reasons, self protection, impact on reputation, impact on share price etc. But it is worth remembering that even Blue Chip multi-nationals are just as vulnerable (maybe even more so) to security breaches, Sony being an obvious recent example.

So if companies of Sony's calibre are vulnerable, it is clear that companies and organisations across the board are too. Companies of all sizes need to understand that breaches can (and do) happen to anyone.

I worked in the information sharing arena at the Centre for the Protection of National Infrastructure (CPNI) for four years and, through CPNI's Information Exchanges, became well aware of the value of sharing information in a mutually trusted environment. Accounts of breaches and, equally importantly, success stories are shared in confidence across industries critical to the UK national infrastructure. Information Exchange members are then free to share these in anonymous and sanitised form within their own organisations.

CPNI's model has been extremely successful, the first two Information Exchanges (Finance and Telecoms) started in 2003 and since then the concept has proved incredibly powerful and CPNI now facilitates a total of thirteen separate exchanges.

Obviously CPNI's remit is to provide security advice to businesses and organisations serving the UK national infrastructure, so it may appear to be a 'closed shop' to many, but there is no reason why the information sharing model cannot be adopted by organisations operating outside the UK critical national infrastructure.

So, there are ways for companies to share and learn mutually once a culture of trust has been established and that really is the nub of the whole information sharing concept. Getting what are, in essence, a group of competitors to sit around a table and admit to and share their vulnerabilities with each other, does not necessarily happen overnight, but if there is a genuine will and desire to make the business more secure and companies are prepared to invest in information sharing in a trusted environment, then the benefits are considerable.

I wholeheartedly endorse Steve's plea for experiences and solutions to be shared, but would add there needs be a culture change around the whole concept of information sharing. As Steve says, there is a need to look beyond apportioning blame for security breaches and to look for lessons that can be learned and shared.

Mark Pattinson (IISP membership pending)
InfoSec Consultant
Stark Rogers

NATURAL PARTNERS?

Dear Sir,

The IISP has recently launched its Academic Partnership programme, which aims to nurture a culture of collaboration and information security professionalism between the IISP and staff and students of partner academic institutions. For the IISP, a relatively fledgling professional body, relationships with academic institutions should prove valuable in the promotion of services and attracting new memberships. These are entirely reasonable aims for an organisation seeking to establish itself as the 'voice of the Information Security Profession'. But what is in the deal for academic institutions engaged in information security education, such as my own, Royal Holloway? Should we aspire to become academic partners of the IISP?

Let me give you two good reasons why I think that we should.

The first is that we are in the same game. Information security is not a subject that students tend to study solely for entertainment or intellectual stimulation. While there are corners of the subject space where this might be true to an extent (cryptography springs immediately to my mind), the vast majority of information security students come to academic institutions in order to get a broad education in the fundamental issues that matter concerning the practice of information security. And the reason they want that knowledge is to obtain a decent job at the end of their course of study. In other words, if they are not already, they aspire to become information security professionals. The IISP aims to professionalise the industry and we train upcoming information security professionals. It is obvious that we should work on this project together.

The second is, simply, that it works. Royal Holloway has trained information security professionals for over thirty years and has run a leading masters programme in this area for twenty. During this time over 2,000 students have passed through the institution, the vast majority of who are now information security professionals. Do you think we did this on our own? From the outset, Royal Holloway's academic offerings in information security have been designed with the input of, taught with the assistance of, and reviewed using the expertise of the Information Security Profession. In order to keep our programmes relevant and informed, we have worked with a large community of information security professionals, of which the IISP is a welcome embodiment. Some of the benefits of the Academic Partnership programme are ones that we have been dining on for years, and we highly recommend them.

So that's why we recently completed our application form for the IISP Academic Partnership programme and look forward to a close ongoing relationship in the years to come.

Prof. Keith M. Martin
Director, Information Security Group
Royal Holloway, University of London

Europe's No.1
Information Security Event
SECURE THINKING
SECURE WORKING

83 VICTORIA STREET
LONDON SW1H OHW

TELEPHONE: +44 (0) 8456 123 828
WEBSITE: WWW.INSTISP.ORG