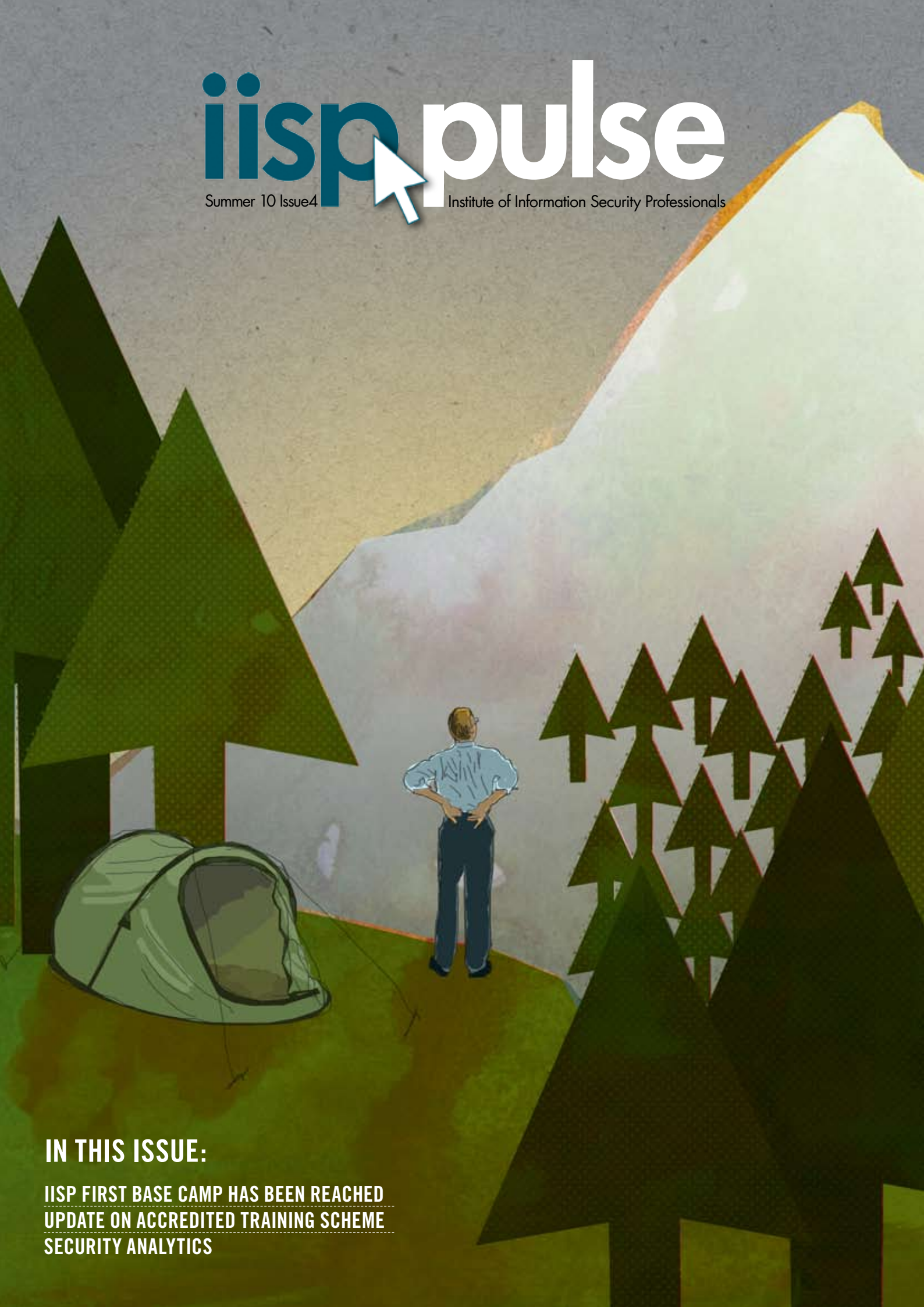
iisp pulse

Summer 10 Issue4

Institute of Information Security Professionals



IN THIS ISSUE:

The Institute of Information Security Professionals
Graduate Development Programme

HAVE YOU CONSIDERED A CAREER IN INFORMATION SECURITY?

Cybercrime, Identity Theft, Computer Hacking, Data Leakage, User Behaviour, Biometric Profiling, Encryption, Botnets, Cyberterrorism, Data Protection, Cloud Computing, Data Loss

Do you want a really challenging, interesting and varied career?

Our Graduate Development Programme helps you develop the skills to protect an organisation from all these threats and more. We are looking for high calibre graduates from a variety of backgrounds to join our Graduate Development Programme and kick-start their career with a top employer.

Join the IISP Graduate Development Programme and within 3 years you can kick-start a career in Information Security with a qualification recognised across the industry and by top employers.

For more information and to apply visit www.instisp.org/graduates or contact 08456 123828.

MESSAGE FROM THE CEO – ONWARDS AND UPWARDS

Welcome to *IISP Pulse*, Issue 4. The magazine was introduced last year as a key communications medium for members to ensure that everyone is aware of important activities at the Institute, and in which members can participate by submitting articles and papers on hot topics and industry initiatives.

The IISP continues to grow and develop, with the addition of two new Regional Branches in the last two months (Midlands and North East) and plans to form two more (Northern Ireland and South West) in the near future. So as we approach the figure of 250 members who have achieved full accreditation to M.Inst.ISP, I see the heartening signs of good health which tell me that the Institute has now achieved a solid foundation, and will (with continuing member contribution and support) grow and develop into the influential and definitive professional body which we all aspire it to be.

Further reinforcement comes from the CESG endorsement last year of the IISP Skills Framework as a common basis for the definition and mapping of Information Assurance (IA) skills for job roles in this discipline across the 'wider public service'.

There are many more activities in progress and in development which Paul Dorey outlines in his article on the following pages.

In line with this increased activity, the Institute is now moving to recruit a full-time, permanent CEO position, with a more operational focus. I am pleased to say that there has been keen interest in this role from the market and we are hopeful of finding a strong candidate who will lead the Institute on towards the next stage of its development. I feel privileged to have held the CEO position over the past two-and-a-quarter years, and to have worked with all of you to build the Institute to the position it now holds, and the platform for continued growth that this represents.

And there is much still to do – for example, the further promotion of the 'brand' of M.Inst.ISP in the eyes of recruiters and employers, as the distinctive competence-based mark of a professional in our field. We have made some progress, and some job adverts do quote A.Inst.ISP or M.Inst.ISP as preferred qualifications, but this requires reinforcement and development. There is also potential for the IISP to attract members from other industry sectors not currently represented, and indeed more representation from outside the UK as well.

As I move on to other roles and professional work, I will continue to help support and promote the Institute in rising to these further challenges in whatever way I can, and look forward to meeting many of you as we join our energies in building THE Institute of Information Security Professionals.

Gerry O'Neill
Chief Executive Officer, IISP

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.

FIRST BASE CAMP HAS BEEN REACHED

Paul Dorey, Chairman of the IISP, reviews the impressive growth of the Institute in its short history.

A few years ago when the founding group set the goal of building a completely new professional institute from scratch, we certainly received the views of a number of sceptics. 'Naïve' was perhaps the most memorable comment, coming from someone outside the UK who agreed with and admired the goals of the newly formed IISP but just did not believe that the necessary high standards were achievable:

- ⇨ *Could a membership organisation really get away with not 'grandfathering' in the first full members with automatic membership to achieve critical mass?*
- ⇨ *Could we reach agreement across security professionals on what a comprehensive information security competency framework should be?*
- ⇨ *Would it be possible to have an accreditation process dependent on interview, the same as professions like engineers or doctors?*
- ⇨ *Could public and private sector agree a common framework?*
- ⇨ *Could we reach break-even financial viability in three years?*

The past few months has seen a lot of activity, which has brought the last elements of our target list to fruition. Our financial review shows that (assuming you all continue to support the Institute!) we have achieved the financial break-even point.

"We must not lose sight of the fact that this is a marathon climb and not a sprint, and we are far from being able to declare the job as done."

High standards: We have never stepped back from the goal set by the membership that all members would have to be appropriately accredited to the same standard – with no special cases. This includes the professional standard of full membership now held by several hundred people and the ITPC and Associate grades of membership.

The competency framework for information security has now been fully endorsed and adopted by the UK government for its IA professionals and by a growing number of corporations who require a path to M.Inst.ISP to be part of professional accreditation for their security staff. It also looks, from take-up by the main consultancy firms, that we will see accredited membership status being the normal standard expected of an information security consultant. The operation of the ITPC accreditation scheme by the Institute for the UK government has further reinforced the need for accreditation.

Our corporate membership support process is now either in action or in planning for 10 different major companies and government departments. This allows companies to have their security teams assessed en masse in a way that integrates with their own staff evolution and development frameworks. Big employers are effectively now stating that an appropriate grade of membership is mandatory for information security roles. Others are expressing interest.

First base camp: This all has not been easy, and has required a remarkable level of personal support, time and patience across all of you as members. However, I would like to declare that we have reached our first base camp. This is something that all of you reading this journal can be justifiably and personally proud of.

TOWARDS THE NEXT SUMMIT

Full membership growth: We must not lose sight of the fact that this is a marathon climb and not a sprint, and we are far from being able to declare the job as done. We still have the challenge of driving the numbers of full members up from the lower hundreds to mid-thousands. We have made progress on speeding things up. The form is easier to complete than in the early days, and we continue to make the process quicker and simpler but the standard has NOT been reduced.

I am delighted as more and more people approach me to say they are signing-up. But we know there are quite a number of you who could also make the step. So I ask, is there a reason that you shouldn't apply now? Every new applicant shows their appreciation of the hard work put in by individual volunteers in the Institute who are your peers in the industry.

Graduates and professional development: As well as increasing numbers of full membership and assessed associates we need to continue to develop graduates and those in the development pipeline. Our graduate development programme is in action, and our links with universities continue to get stronger as we sign association agreements. Some international relationships are also developing.

In the next phase of our growth we can expect our own development work such as Top Gun and professional lectures

to expand much further into development programmes and continued professional development (CPD).

Companies and institutes will also continue to have their training courses accredited by the Institute so that we know that these courses will also contribute to our personal development. The published list of accredited courses is available to members.

Regional Branches and Special Interest Groups: The member-driven set-up of five regional branches in Scotland, the North West, London, the Midlands, and the North East shows that we have vibrant local communities. The demand for more UK and also international branches is growing, so that we can expect these to emerge. Special interest groups are also forming and will be used to increase our voice on policy, standards and key issues facing the profession.

SPECIAL THANKS

I close with special thanks to our office team and all of our volunteers from all of the classes of membership. I also want to close this article that has described the progress of the Institute with a special word of thanks to Gerry O'Neill who has been our part-time Chief Executive during the past two years. He has been the architect of many of the successes described above. His personal dedication caused him to volunteer far more time than his contracted duties and we are very grateful for his support and success.

INTRODUCING THE IISP ACCREDITED TRAINING SCHEME

In order to attain the highest level of membership with the IISP, that of full membership, it is necessary for applicants to demonstrate both knowledge and capability against topics on the Skills Framework. Claims of capability must be supported by appropriate evidence and are assessed, via interview, by other full members of the IISP.

Knowledge may be acquired in a number of different ways, such as attendance of formal information security courses, seminars and conferences, or on-the-job training. The Board of the IISP considered it prudent to establish a process that would provide members with training course content that could be validated against the various disciplines defined in the Skills Framework.

WORKING GROUP DEVELOPMENTS

At the beginning of 2008 a working group was established to deliver the following objective:

'To make validated training content available to professionals who aspire to full membership or those who wish to maintain and/or extend their knowledge and capability, in line with the IISP's Skills Framework.'

The working group has developed a scheme so that training providers can submit the content of their courses for accreditation. Its chair is Alan Lycett who has held many high profile positions as an IT auditor, information security professional and trainer. During his time at Zergo Consultants he managed the highly successful Zergo IT Security Training Club. He is the only person to have courses accredited by the British Computer Society's Information Systems Examination Board (ISEB) across three different disciplines (information security, data protection and software asset management).

Under the scheme, training providers must submit an application that includes details of how the content of their course satisfies the requirements of any relevant part of the Skills Framework. These claims are then assessed by a subject matter expert who is a full member of the IISP. The report that is sent back to the working group by the assessor contains a recommendation as to whether accreditation should be awarded or not. Once a course has been accredited, the training provider is duly notified and details of the course are posted on the IISP's website.

PILOT UNDERTAKEN

In order to validate the accreditation scheme a pilot test has been undertaken. We endeavoured to have a wide participation in the pilot, and involve as many training providers as possible. A number have already successfully completed applications, whilst others are being processed and were due to have completed their assessment by the close of the pilot at the end of June.

Courses can be accredited at two different levels:

⇨ *A score of 1 means that the course imparts just knowledge;*

⇨ *A score of 1+ means that it imparts and reinforces knowledge through practical content.*

An example of this scoring scheme is illustrated by a course successfully submitted by URM, 'A Practitioner Certificate in Business Continuity Management'. The syllabus of this course was developed by the ISEB. Its objective is to provide delegates not only with formal classroom training on this important subject but also the opportunity to complete a series of substantial mandatory practical exercises based on a case study. The course concludes with a challenging three hour written examination, independently set and marked by the ISEB, most of which is based around a case study. Upon review of the training materials, the assessor and the working group had no hesitation in awarding a score of 1+ to the content of this course.

PARTICIPATING

Members wishing to attend an accredited training course must reserve their place through the appropriate training provider. Details can be found on the IISP website together with those topics in the Skills Framework that the content of the course satisfies. It is worth emphasising at this stage that it is the content of course that has been accredited and, whilst the working group has obtained some further information about the courses, other aspects (such as the quality of trainers and venues) have not been assessed.

At the time of publication of this edition of Pulse, three courses have successfully achieved accreditation and a further two are being assessed. Up to five further courses are expected to be submitted in the immediate future.

On completion of the pilot a report will be sent to the Board which will contain a full assessment of the strengths and weaknesses of the scheme. The report will also highlight how other approaches might be adopted to satisfy the need for validated training to be made available to members. One of the main challenges in the future will be how to make validated training courses available which cover the entire Skills Framework.

In addition to Alan Lycett, present active members of the working group include recent IISP CEO Gerry O'Neill, Chief Operations Officer Triona Tierney, and board members Amanda Finch, Sharon Wiltshire and Professor Fred Piper. Matthew Martindale from KPMG has also recently joined, replacing the earlier contributions made by Martin Tyley. Our thanks to all for their help in progressing the pilot scheme in preparation for the full service to launch this autumn.

UPDATE ON ASSOCIATE (ITPC) MEMBER APPLICATIONS

We are happy to report that we are currently up-to-date with Associate ITPC applications and that the application processes are now embedded within the Institute.

It is a little over a year ago that the management of the ITPC accreditation scheme passed to the IISP. It has been quite a challenging year for all concerned; for the secretariat – absorbing this scheme with no additional resource; for the assessors – becoming familiar and confident with the new application format; for the applicants – as we embedded processes and improved guidance.

We are lucky to have the majority of the original ITPC assessors still marking applications, thereby ensuring consistency of the standard. We have also recruited extra assessors, and have plans in place to recruit and train more, in anticipation of further increased demand.

There are a number of parties with an interest in the ITPC; this is still 'owned' by HMG and run by a steering committee, made up of a wide representation of government departments and interested academics. The second meeting of this committee is taking place in July this year.

To improve the process we recently ran our first teleconference workshop, which gave advice on how to approach the application form, the level of detail required and what constitutes good evidence. This was oversubscribed, and a second workshop is being held in early July. These will be a regular feature if there is demand.

The purpose of these workshops is to help both the candidates and the assessors; the candidates in focusing their effort, which in turn helps the assessors as it is much easier to mark a good application, and applications passing first time free up the assessors' time.

We will continue to fine tune and enhance this process and would like to thank all those involved in making this scheme a success.

Triona Tierney
Chief Operations Officer

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

We would like to congratulate the following IISP members who have, since publication of our last Pulse magazine, achieved the Institute's professional accreditation, M.Inst.ISP. Well done to all of you.

In addition to now having full voting rights, and the ability to nominate directors to the Board of the IISP, we look forward to your further support in helping to develop the Institute, or contribute to its initiatives and working groups. Congratulations once again!

Paul Akass
Max Allen
Thomas J. Armstrong
Chikara Atulomah
Alex Baruttis
Martin Betts
Stewart Blackman
Mark S Blagg
Kevin Brewer
Gary Evans
Chris Few
Steve Forrester
Vince Freeman
Prof. Steven Furnell
Julian C Glendinning
Tracy Goodison
Mark Grover
Martin Henry
Chris Hill
Simon Jarnell
Matt Johnson
Richard Jones
John Laskey
Chris Mayers
Davy McGerrity
Michael McKinnell
Roger Millar
Mark Overend
Vijay R Patel
Matthew W A Pemble
Jonathon Powell
Lee Rawcliffe
Debbie Richards
Glyn Richards
Denis Stewart
James Todd
Ian L Williams
Keith Williams
Piers Wilson

CORPORATE MEMBER PROFILE – SPOTLIGHT ON SAPPHIRE

This is the first in a new series of articles where we take a closer look at some of the leading IISP corporate members and their views on the Institute.

Sapphire has been involved in Information Assurance consultancy services for a number of years and we have seen a lot of changes in that time. We were involved in Information Assurance even before the industry knew what IA was. In that time stock markets have boomed and bust, Big Brother has come and gone and yet Moore's Law continues to drive us at a relentless pace in terms of size, speed and storage.

When Sapphire started you didn't see much more than servers, PCs and some backup storage facilities. Now, with an explosion in the number and range of hardware devices, the amount of 'stuff' out there and the possibilities for connecting all this together is driving the pace of change.

Our industry moves fast, first Tuesday software patching, another lost laptop and subject access request are issues that are probably sat in your inbox right now. Having the capability to deal with all this and still do your day job can be daunting.

And this is where the IISP can help. Yes there are other trade and industry bodies out there, and they encompass a broad church, but they lack the depth and detail that the IISP can bring to your role, your career and your company. Security and Information Assurance is just too important to your organisation not to treat as a profession in its own right.

Before the inception of the IISP, there was a gap in our security industry for a credible badge that IA/IS professionals could wear – a form of 'chartered' status. It was difficult for industry professionals to prove their competence, value and worth to clients or peers. Creation of the IISP reduced the opportunity for 'cowboys' and provided security professionals with the opportunity to gain industry-recognised certification in their chosen field with a much more defined career/training path. To help get the IISP off the ground and to support such an admirable idea, Sapphire joined the IISP as a corporate member in May 2006.

"As the Managing Director of a leading IA/IS consultancy, I find the IISP extremely valuable at a number of levels – the ability to access a focused network of leading professionals from other organisations, the involvement in innovative research and thought-leadership and, most importantly, a structured programme which helps me to develop and accredit the skills of my entire consultancy team. These are extremely valuable services and are benefits which are not available elsewhere."

Corporate membership is not just another badge to put on your website. There are tangible benefits such as the Jobs Board and I feel that this is a unique service offered by the IISP to its corporate members. By securing just one placement on the job board, organisations can save recruitment fees and recoup the IISP corporate membership fee in a single shot.

The softer benefits of being a corporate member of the IISP are there as well, they are just a little more difficult to put down on the profit and loss statement. For instance the networking opportunities are plentiful and varied; from the quarterly corporate member meetings to the various events, work groups and seminars provided by the IISP. I have met many great fellow members and learnt a great deal from their experiences; and hopefully they have picked up one or two useful pieces of advice from me.

Recently, we saw the launch of the IISP Graduate Development Programme; we have taken advantage of this and three junior members of my security consultancy team have joined. Specifically, one of the younger members of my team is self-taught and although he is extremely competent as a consultant, he has no formal qualifications. By progressing through the IISP Graduate Development Programme, he has been able to use the framework to track his progression, qualifications and experience which, in turn, enables us to provide customers with a level of assurance in the quality and professionalism of his work. It has also given us a good formal point to start from and track his development/growth plans over the coming years.

Sapphire's corporate membership with the IISP has also enabled us to become involved with some new and exciting projects. One of these is a research project into the economics of cloud computing.

Through its relationship with the IISP, Sapphire was invited to work with HP Labs, the University of Aberdeen, the University of Bath and Validsoft on a three year collaborative research project entitled 'Cloud Stewardship Economics: securing the new business infrastructure'. The work is partially funded by the UK Technology Strategy Board.

In a nutshell the research project aims to establish new approaches for how to assess and manage risk for all the cloud eco-system participants, regulators and policy makers and, in particular, to understand how information about perceived attacks can be shared, interpreted and acted on in real time by other parties in the ecosystem. Cloud computing eco-systems of service providers and consumers, including individuals, charitable and public bodies, SMEs, large enterprises and governments will become a significant part of the way these services are provided, allowing more agile coalitions, cost savings and improved service delivery. Our critical national infrastructure is increasingly dependent on information systems and the services they support.

Sapphire's annual conference, National Information Security Conference (www.nisc.org.uk), provided an excellent platform to launch this joint research project. NISC is one of the UK's largest, annual, delegate-focused security events. Our event gives our clients and potential clients the opportunity to increase both their practical and theoretical knowledge. We encourage a great deal of networking, not unlike the IISP, and although fully funded by sponsorship, delegates often comment on the relaxed, no-pressure environment. When asked to comment about the event, John Finch, Information Security Manager at Plymouth City Council said "The calibre of the speakers is hard to match and there is not the constant sales pitch found at other conferences."

NISC attracts a range of professionals from within the industry, from both the private and the public sectors. So, Sapphire worked with HP Labs and the University of Aberdeen, and held a number of elicitation and knowledge-sharing workshops. Delegates were invited to participate in one-to-one sessions with members of the cloud research team and share their views, thoughts and comments. The feedback was used to gather inputs from security professionals and stakeholders, and to help the team to shape their research over the coming years.

Sapphire invited the IISP to exhibit at the NISC conference, to generate interest in its work within the industry. During the conference, we held an abridged version of the IISP Top Gun workshop, aptly entitled Top Slice as we were in the home of golf, St. Andrews.

NISC delegates had previously asked for more hands-on workshops demonstrating a practical approach to risk management. The IISP Top Gun provided a great opportunity to do this.

The IISP agreed to provide the Top Gun workshop, which is normally held over the course of a day to NISC delegates in only two and a half hours. At first, several of us were very sceptical and not convinced that a workshop with 162 people would succeed. However, thanks to the hard work of several members of the IISP, the workshop proved to be a huge success. The feedback from our delegates rated the workshop as a 4.3 out of a maximum of 5.0 and proved to be one of the more successful presentations of the conference.

I would like to thank all members of the IISP for their contribution to the workshop including: Andre Campbell, Gerry O'Neill, Mark Brett, Paul Dorey, Nick Prescott, John Amer and Jonathan Bedford.

I would entirely recommend the IISP's Corporate Membership programme as I find it extremely valuable at a number of levels – the ability to access a focused network of leading professionals from other organisations, the involvement in innovative research and thought-leadership and, most importantly, a structured programme which helps me to develop and accredit the skills of my entire consultancy team.

THE AUTHOR
John Morrison is Managing Director of Sapphire

REGIONAL BRANCH UPDATE

There's been lots happening on the regional branch front with the recent addition of two new branches and a range of activities taking place up and down the country. Here's a quick update together with news of forthcoming meetings…

LONDON BRANCH

This month brings news on the crackdown of criminals responsible for running cyber crime forums and launching credit card frauds on petrol station customers. Despite this coup, further widespread Internet vulnerabilities have been disclosed, this time targeting users reading PDF files. The global online media coverage of this year's World Cup has tested us on the agility of our corporate security policies and practices from a security, productivity and availability perspective. The threat of malicious media content riding off the back of the euphoria of the World Cup has yet to fully materialise although samples of malware have been identified in the wild.

The introduction of iPads and new version of the iPhone also provide us with some new challenges in the months ahead as their adoption rates rapidly increase and information security policies and controls aim to catch up. Budget cuts have been announced which may stifle the growth of information assurance activities in the UK government sector. Cloud computing continues to show great promise for Infrastructure and Software as a Service, offering compelling solutions in cost constrained environments. Our profession continues to play a role in shaping how we will provide innovative ways of adopting and managing these changes into our society.

Join us for our next London Chapter meeting which will be held in Central London on the 29th July 2010. We have an exciting agenda planned which will include an exercise in speed dating, infosec style, giving members the opportunity to meet and greet fellow London Chapter members. Topics on the agenda for forthcoming meetings include:

- ⇨ *Security in the cloud – protecting the silver lining?*
- ⇨ *Understanding the dangers online – discussing the latest online threats and defence strategies;*
- ⇨ *Identity and access management – are we ready for wider adoption and what are the implications?*
- ⇨ *Social engineering – changing behaviour to protect from the enemy within;*
- ⇨ *Data privacy – are we doing enough to satisfy the regulator?*
- ⇨ *Government security – is information assurance investment on the way out with the new government?*
- ⇨ *Establishing your own business continuity plan;*
- ⇨ *Addressing the board without getting them bored.*

If you would like to actively participate in any of the future chapter meetings as a speaker or host, please contact me at **ryan.rubin@protiviti.co.uk.**
Ryan Rubin, Protiviti – *Chairperson*

NORTH EAST ENGLAND BRANCH LAUNCHED

July 2010 will see the establishment of a new North East England branch of the IISP. This will be chaired by Mark Grover and assisted by Chris Bell and Graeme Parker. The branch aims to support IISP members who live and work in the North East area, and who would like to meet up with like-minded security professionals and participate in topical debate, presentations, networking or knowledge sharing.

The NE branch will meet on a quarterly basis with expected venues in Rotherham, Newcastle and York during the year. A joint NE and NW (aka North of England Branch) meeting will also be arranged annually as we move forward.

NEW BRANCH MEETS IN THE MIDLANDS

The latest IISP regional branch formed with an inaugural meeting (over lunch break) on 27th May, hosted by HMRC at their offices in Telford, Shropshire, thanks to the drive of local enthusiasts.

A total of 15 members heard Martin Taylor outline how 'A picture paints a thousand words', as he went on to discuss the part played by system diagrams and flowcharts in communicating the security and control features of business systems and technical architectures.

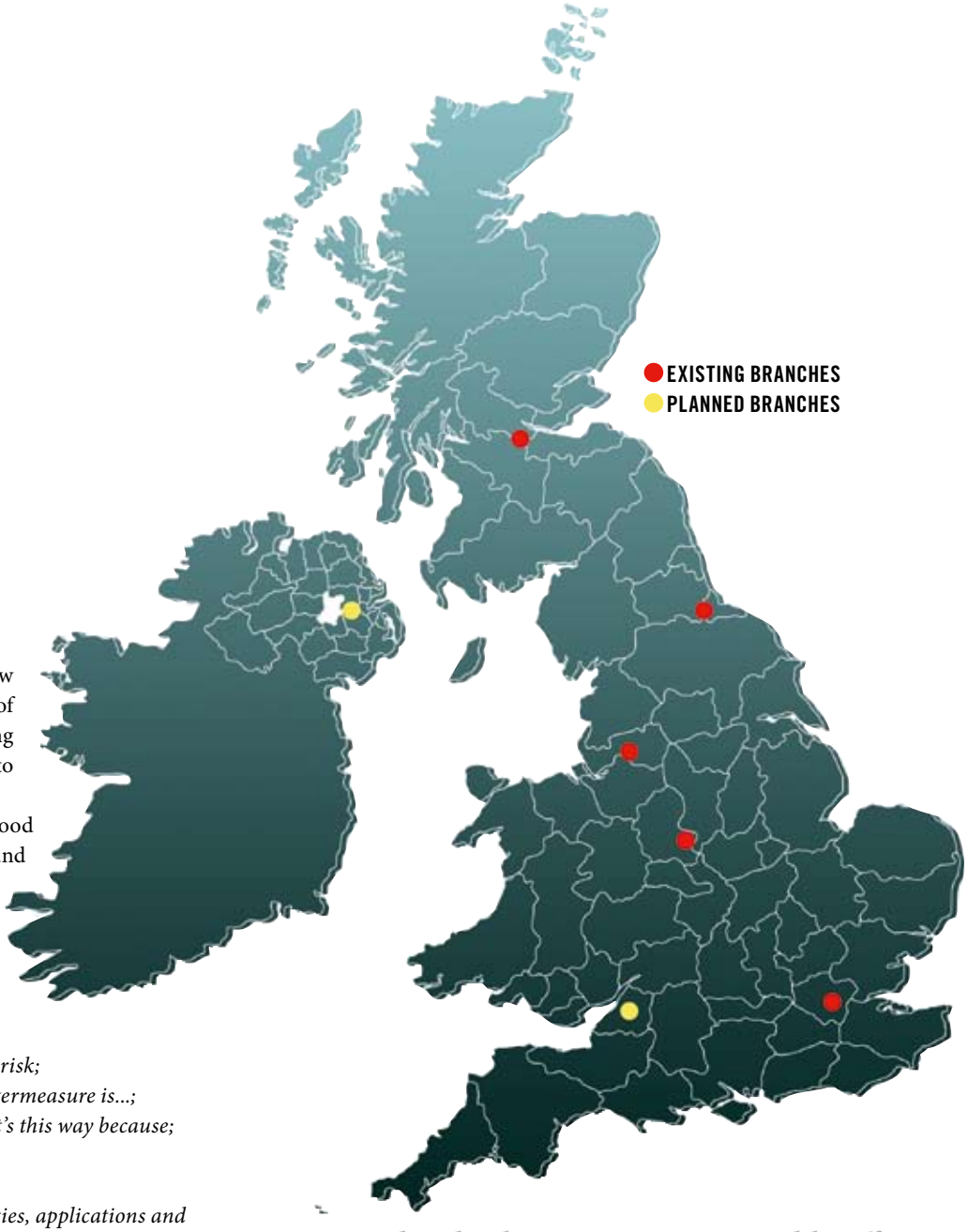
The attendees, many of whom have experience in preparing security and systems documentation, including the diagrammatic elements, engaged with Martin in the discussion which followed and outlined those approaches that had succeeded for them.

The Telford/Midlands Branch plans to meet again in September, once again hosted by our HMRC sponsor, Chris Mortlock. Topics for the meeting, volunteer speakers, and a candidate to act as Chair for the Branch would be most welcome.

NORTH WEST BRANCH

Now this may seem all the same to readers south of Watford Gap, but the North of England branch of IISP is splitting up in the best possible way. In the North East, Mark Grover is championing a new group that will have a bit o' cracky (the chairman is a Geordie...sorry!) on information security matters.

Meanwhile, the new North West branch, re-formed with a Churchillian stroke of a



pen will seek to share experience and know-how in group therapy sessions on the Irish side of the Pennines – although our autumn meeting is planning to make the foray across the M62 to Leeds with thanks to Ben Jefferson.

Our last meeting left us with a particularly good insight into the security opportunity of free and open source software (thanks Gurbir Singh) and the professionalism of the Institute (hats off to Gerry O'Neill). Still on the agenda for the coming semesters are:

- ⇨ *Confessions of an infosec professional;*
- ⇨ *Information security challenges in emerging risk;*
- ⇨ *The greatest security threat is... and its countermeasure is...;*
- ⇨ *The most overrated security threat is... and it's this way because;*
- ⇨ *Blending defences against blended attacks;*
- ⇨ *Cloud computing for aspiring dummies;*
- ⇨ *Hardware, firmware, operating system, utilities, applications and data: how to draw up a white list of what you want;*
- ⇨ *What happens when data enters an unintentional information system?*
- ⇨ *Convincing granny and the board without scary breach stories – the 'elevator pitch' for information security;*
- ⇨ *What I did at Infosec? or What has Infosec done for us?*

And contrary to Kipling, the twain shall meet annually at a location between the two branches. The Institute is a grand gesture but information security is achieved through small, frequent, actions – the branches are realising these actions and making membership a badge worn with pride.
Danny Dresner, National Computing Centre – *Chairperson*

SCOTTISH BRANCH

Activity in IISP Scotland has been increasing, with members taking advantage of events to network and communicate with peers. With the launch of the Scotland and Northern Ireland Centre of Excellence in Security and Cybercrime (http://www.coe-security-and-cybercrime.net/) we have an opportunity to help steer not only the academic side of information security in Scotland, but also to be a key part of the industry as a whole.

Individuals are putting in visible effort to mentor and guide potential new members, and to spread the word

In addition, we are forging strong ties with ISACA Scotland and OWASP – with many IISP members belonging to other organisations we are using this to build appropriate presentation schedules and are looking at the possibility of a joint one day workshop with technical and management threads. More on this later…

Individuals are putting in visible effort to mentor and guide potential new members, and to spread the word. This is helping the profile of the IISP immensely. If you need any materials or support please get in touch with Rory Alsop, the Scottish branch chairman.

Our last branch meeting at the end of April was well attended, with numerous discussion topics sparking off ongoing interest, and feeding in to plans for further meetings this year. From feedback it looks like July is not going to be the best time for our next meeting so we are now planning for mid-August.

In saying that, we would still welcome volunteers to present or host branch meetings – especially in the west. It has been easiest to host in Edinburgh, but in the interests of fairness we would like to present in Glasgow as well.

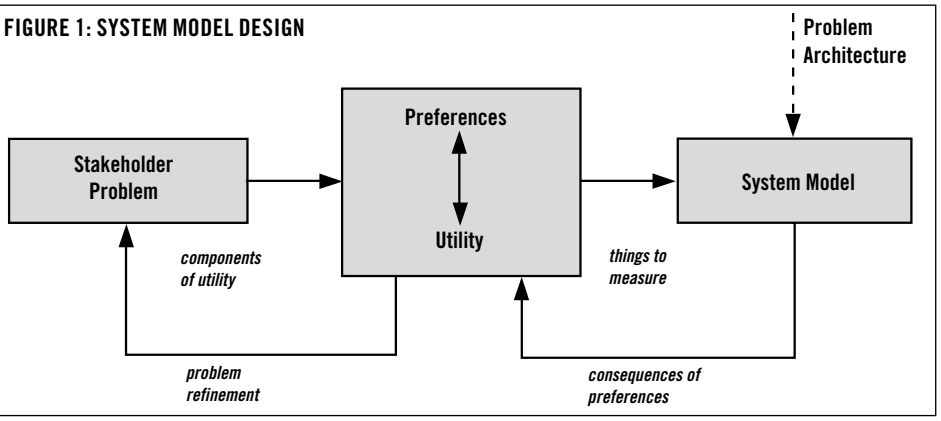
Cheers,

Rory Alsop, Ernst & Young –*Chairperson*

SECURITY ANALYTICS: BRINGING SCIENCE TO SECURITY MANAGEMENT

Most security professionals recognise the difficulty of justifying security investments. How much should be spent, what should be prioritised, how to choose between lowering perceived risks and disrupting business? Security Analytics is about creating tools and a methodology to rigorously address these types of challenges. Our conceptual approach is to use mathematical systems models and economic models to analyse not only the technological aspects of the infrastructure, but also social, economic, behavioural, and policy aspects crucial to the deployment of a computing service. As such it involves the integration of a wide range of sciences including computer science, mathematics, economics, and cognitive science.

FIGURE 1: SYSTEM MODEL DESIGN



Security Analytics is primarily a project within HP Labs Bristol, although such a broad programme clearly requires broad input and expertise. For this we rely on collaborative partnerships with customers, partners, and academia, with the support of the UK Technology Strategy Board — through its partial funding the 'Trust Economics' project (see box below) and the 'Cloud Stewardship Economics' project, which involves the IISP (see box over page) — being pivotal.

In contrast to a typical return on investment or cost benefit analysis, our starting point is economics. The point is that security investments inevitably affect multiple outcomes — such as confidentiality, availability, integrity, and cost — and different stakeholders will have different priorities relating to these outcomes. Economics can provide a framework where stakeholders can properly explore and discuss their preferences for how these should trade off. In this way, economics provides tools to help the CISO align stakeholders and align security with business priorities.

Because information systems are so complex, it is very difficult to predict the effect of security policies and investments, even when the intent is clear. To address this, we construct mathematical models — semantically justified; based on process theory and logic — of the underlying system, allowing predictive simulation of the space of controls and outcomes. Tying back to the economics, we design the system model to predict the magnitudes identified by the economic models (see Figure 1).

For example, in one particular case study performed on software vulnerability and patch management, the problem was to decide whether and how to improve on an enterprise's threat-management process. Intuitively, doing more patching costs money and causes more business disruption; in contrast, not patching increases exposure to malware. That is, there is a trade-off between cost, business disruption, and exposure to risk: how do the IT operations staff feel about more patching, and how much planned disruption would they prefer, as opposed to emergency (unplanned) disruption? Different stakeholders will have different priorities for how these aspects should trade off, and our methods help to explore the choices and their consequences.

The next step in our methodology is to construct a system model that captures how the processes and technology affect planned and unplanned downtime (our proxy for business disruption) and expected time to mitigate a vulnerability (our proxy for risk exposure). Figure 2 shows a picture of the system model, and Figure 3 shows how, by varying the parameters in the model, we can see the following: predicted risk-exposure performance with no investments; the effect of investing in HIPS technology; and the effect of deploying more resources to improve patching. In the Trust Economics project, we have explored with our partners similar examples incorporating empirical work on human factors.

In the new **Cloud Stewardship Economics** project, we are expanding the scope of our research to study information stewardship issues in cloud computing. The operations of cloud computing will consist in an ecosystem of service-providers and consumers, with reliance on complex networks of people, processes, and technologies.

To-date, most research in cloud computing security has been limited to making the technology infrastructure 'safe'. We would emphasise that the people, process, and policy implications of cloud computing must also be understood and managed. It is difficult for stakeholders to establish when they are taking risks, what those risks are, when they (as stakeholders) are (or should be) accountable for certain standards of diligence or control, and how to achieve them. It is, therefore, vital to understand how to structure and regulate such an ecosystem in order to align incentives and create sufficient trust or 'social capital', and thereby make it easy for new entrants to comply with cloud stewardship requirements, and so 'plug and play' in the ecosystem. In summary, it is essential to achieve effective and resilient standards of information stewardship.

In the context of the cloud ecosystem, many of the stakeholders will have misaligned incentives, there will be information asymmetries

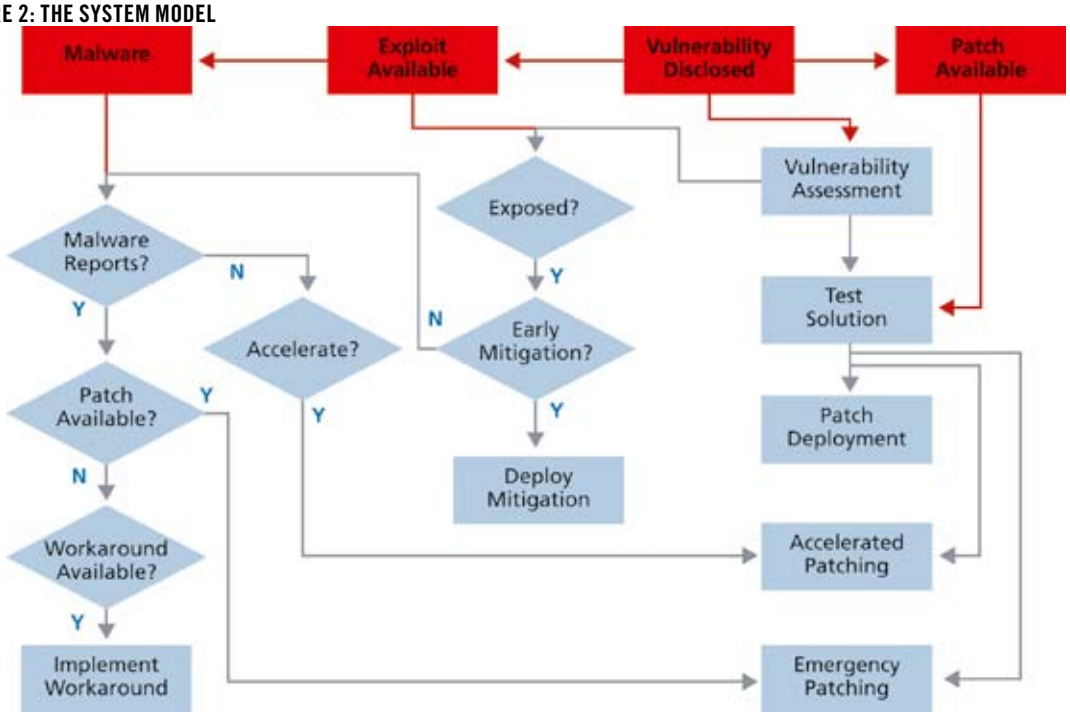
TRUST ECONOMICS: A UK COLLABORATIVE RESEARCH PROJECT

HP Labs, the University of Bath, the University of Newcastle, University College London, Merrill Lynch, and the National Grid are two years into a three year collaborative research project. The work is partially funded by the UK Technology Strategy Board.

This project is about integrating techniques from economics, cognitive science, human factors, and mathematical modeling to reason about security decision-making.

The Technology Strategy Board is a national body that promotes and supports innovation for the benefit of UK business, to increase economic growth and improve the quality of life.

FIGURE 2: THE SYSTEM MODEL



between the stakeholders, and associated moral hazards. Policy makers must ensure that appropriate standards of information stewardship — aspects of which may be seen as public goods or club goods — are maintained. It follows that so far we have primarily relied on ideas and methods from macro- and financial economics to explore the dynamics of utility functions that express security and investment preferences, and thereby facilitate quantified illustrations of the consequences of different policy and investment choices. However, in the new project, we expect to exploit more micro-economics to explore the perspectives of different factors in the ecosystem.

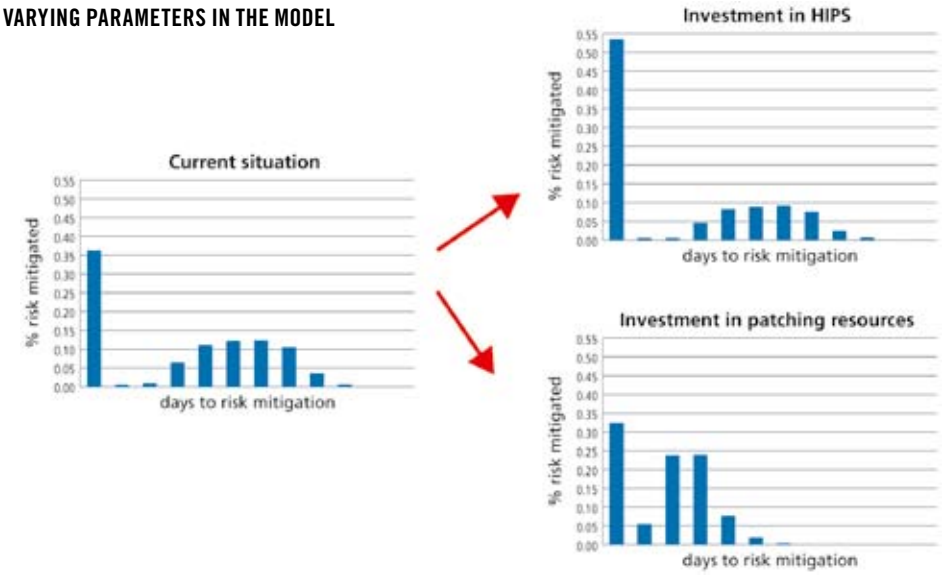
Alongside the economic theory, this project will conduct a series of empirical studies. The IISP has been instrumental in bringing appropriate SMEs into the project. Looking to the future development of these ideas and methods, as well as in the shaping of the ongoing empirical studies, the intent is for the IISP to act as a bridge between Security Analytics and the security profession, disseminating and exploiting the outputs.

CLOUD STEWARDSHIP ECONOMICS: A FUNDED COLLABORATIVE RESEARCH PROJECT INVOLVING THE IISP

HP Labs, the University of Aberdeen, the University of Bath, Sapphire Technologies Ltd, Validsoft, Marmalade Box and the IISP have just started a three year collaborative research project titled 'Cloud Stewardship Economics: securing the new business infrastructure'. We are also engaging with Lloyd's of London as a case study in cloud stewardship. The work is being partially funded by the UK Technology Strategy Board.

As part of this project we will be gathering inputs from security professionals and stakeholders on the way in which information stewardship issues are, and will continue to affect cloud computing. Our aim is to begin to build a community of stakeholders to shape and benefit from this work. The IISP will be instrumental in bringing the profession's view to this community.

FIGURE 3: VARYING PARAMETERS IN THE MODEL



THE AUTHORS

Professor David J. Pym is 6th Century Chair in Logic, School of Natural and Computing Sciences, University of Aberdeen

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

ASSURING THE WEAKEST LINK – INTRODUCING THE COMMON ASSURANCE MATURITY MODEL (CAMM)

Raj Samani and Gerry O'Neill report on the development of a new framework, intended to help in establishing the security maturity of business partners and third-party providers.

Popular sayings are popular because they are often ring true. Within the information security industry the old adage that 'Security is only as strong as the weakest link' is ringing true for organisations dealing with third parties.

Concern over third parties is largely focused on two areas: a) connectivity to the corporate network by business partners, and b) third party service provisioning organisations.

"In an environment that is increasingly driven by regulatory and cost issues, confidence that your information is secure is a key factor to business success. But knowing who to trust your information to is an issue many businesses struggle to deal with effectively. The Common Assurance Maturity Model will provide businesses with that confidence to choose the most appropriate partner to whom they can entrust their sensitive information." - **Brian Honan, Principal Consultant with BH Consulting.**

'TRUSTED' BUSINESS PARTNERS

The proliferation of third party access connections to corporate networks is rising exponentially, with the number of partners requiring access often running into the thousands for many large organisations. Information security departments are being overstretched with the responsibility of ensuring business partners do not represent an unacceptable risk to the business. Sadly, this is due to the unavailability of scalable measurement tools that can quickly assess the security maturity of an organisation; resulting in each new business partner requiring significant time and investment from internal resources to assess the level of risk they represent.

SERVICE PROVISIONING

A similar issue is being heard by those tasked with performing due diligence against third party service providers. Current frameworks are either far too heavy to be seriously considered for use, or they provide the respondent with the opportunity to bury bad practices 'out of scope'. What's worse is that even providers that have mature risk management practices are unable to translate investment into turnover. With so many choices facing organisations about where to send their data, the only quantifiable and objective assessment criterion is cost. Sadly, those organisations investing in security are often overlooked in favour of those with strong marketing departments and the ability to work with lower margins.

A NEW APPROACH

The two examples above clearly demonstrate a need for a framework that can satisfy the following objectives:

- ***Transparency:*** *a framework capable of providing the necessary transparency in attesting to the maturity of a third party;*
- ***Scalable:*** *a repeatable approach, that can be done without considerable burden on the internal resources performing the necessary due diligence;*
- ***Rewarding:*** *an approach that allows those organisations who do invest in security to reflect this in an open and trustworthy manner to potential customers.*

Clearly the above requirements are only a part of the total number of wishes that a security professional, CIO, cloud provider, and supplier would potentially demand. Additional requirements would include being able to leverage existing investment, and to be an efficient process to apply. Oh, and of course, to be cost-effective.

WHITE KNIGHT

A new framework to address these issues is now in development. Known as the Common Assurance Maturity Model (CAMM), its purpose is to create a model that simply requires the organisation to set the level of maturity it requires from its third parties. For example, it may set a quantifiable metric for all third parties to attain before being allowed access to the corporate network. Setting the metric will, of course, depend on the level/type of access, and the risk appetite. The risk appetite may, for example, demand that the security maturity of a third party is independently verified, or alternatively, self assessment may be suitable. However, the fundamental difference is that the response provided by the third party is objective, quantifiable and, most importantly, does not require the organisation to use resources to provide the assurance, because the trust rests with the framework (and the verification via audit – if required).

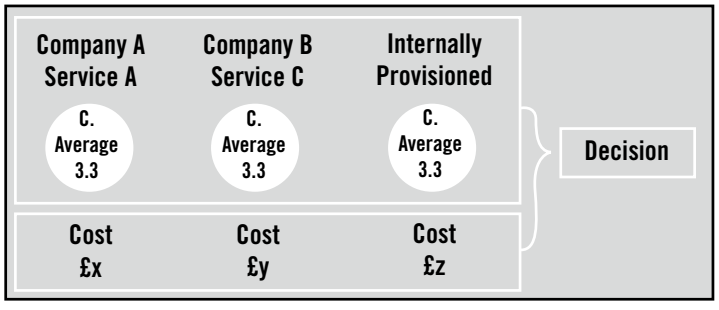
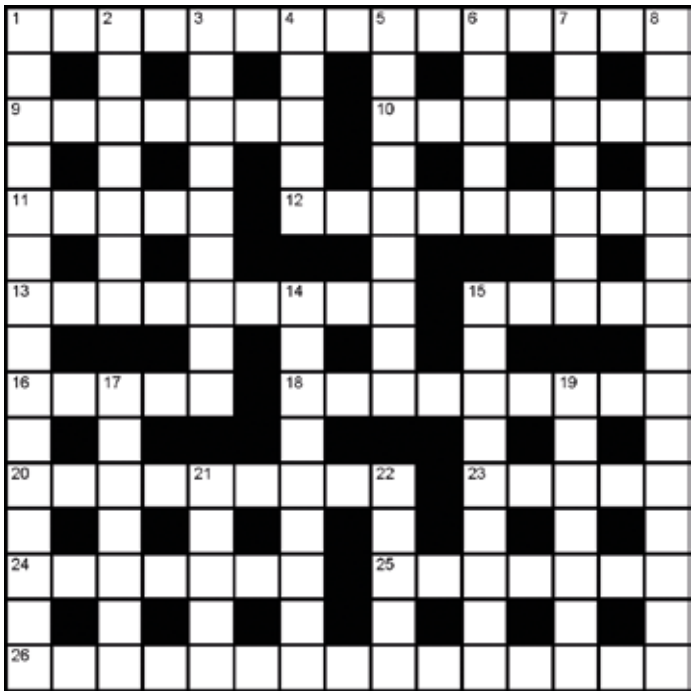


FIGURE 1: COMPARING MATURITY OF PROVIDERS

Having a trustworthy score that outlines the security maturity of an organisation is equally beneficial for third party provisioning. In the first instance it will allow organisations to compare the security maturity of providers, both internal and external (see Figure 1). In addition, organisations will be able to quantify residual risk, but also pay for the level of service they actually need. This will allow providers who invest in security to demonstrate their maturity in an objective and easily understood manner. So how does it work?

CRYPTIC CROSSWORD by DREX



Across

1 Meddlers without wheels? (8,7)
9 Constant pain reported after drink for toasting, with butter perhaps (7)
10 Parcel I opened up is copy (7)
11 Rush endless discipline (5)
12 Ford blabbed and communicated online in no more than 140 characters (9)
13 Rank about three quarters, moving from the balcony to the circle possibly (9)
15 Large-eyed animal is odd going west after the French (5)
16 Some Incas tell those separated from others by distinctions of hereditary rank (5)
18 A defence port backed up by one with greater reason (1,8)
20 Soya gunge pulped for place of worship (9)
23 I'm in two articles showing the inner self (5)
24 To the extent that Afro's in confusion... (7)
25 ... if Ghana's in revolution, thus appears native of another country (7)
26 Nondescript consequence of Viagra usage with a small change (right to left), and its time for the swingometer again! (7,8)

Down

1 Mode of running programme arising from Operations Committee overwhelmed by pile of ironing (5,10)
2 150 idiots found in object-oriented development environment (7)
3 A free package and not enough clothes to go around, reportedly? (9)
4 Get an uncontrolled background process (5)
5 Heroic feats from wandering party following head of department (7-2)
6 Data entry I head without power (5)
7 Martial's crack for example – drug with good weight (7)
8 Result of imposing ISO 27002, 03 or 04 – a dissonant triad of sorts (15)
14 Maiden a LAN guru harrassed under okapi's tail (9)
15 Pulverise the garlic without energy (9)
17 Becomes clear that bathroom's finally finished! (5,2)
19 Japanese art circle gets fix on a motorway (7)
21 Respond favourably to game pro (2,3)
22 Oedema illness obfuscates communication (5)

HOW TO WIN THE PRIZE!

This issue's codeword is concealed about this crossword, and can be solved by completing the numbered boxes below as you solve the fiendish cryptic clues – courtesy of DREX.

16	11	25	10	9	7	13	22	5

If you discover the codeword, then email your entry to **info@instisp.com**
Closing date is 12.00 on Friday 27th August 2010, and the winner will be drawn at random from correct entries at that time. A prize of £40 in Amazon vouchers is on offer to the winner. Good luck with the challenge!

Last issue's Codewords were Browser and Chrome. The winning entry was submitted by Anne Heinrichsons, who won the prize of £40 of Amazon vouchers. Congratulations, Anne.

LAST ISSUE'S SOLUTION

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

HOW CAMM WORKS

By focusing on the core controls, an organisation can quantify their maturity in a comparable manner. The method also utilises existing standards, allowing organisations to leverage existing investment. Of course one key issue with such a simplistic approach is that it provides absolutely no flexibility to cater for individual organisational needs. For example, having controls to adhere with PCI requirements would only be beneficial to those that process credit cards. Therefore, the CAMM model will produce one common set of controls, and then allow the flexibility of additional modules to be added. What this means is that an organisation can demand a level of maturity of 'x' for the common controls, but also demand compliance against any number of pre-provided modules, or even a set of bespoke modules.

The net result is transparency. Not just for the customer considering outsourcing, but also for the provider who knows with absolute certainty exactly what controls are sought by their customer(s). Equally the third party knows exactly what is needed in order to connect to their business partners.

WHEN WILL IT BE READY?

The initial set of reviews have now begun, with pilot studies scheduled for later this summer. It is anticipated that the common control set will be ready by Q4 2010. Although scepticism about its likely success will be rife, one fundamental difference about this project is the support it has already received. Participants of the project are from around the world, with strong support from public and private sectors, industry associations, and global key industry stakeholders.

"With today's complex IT architectures and heavy reliance upon third party providers, there has never been a greater demand for transparency and objective metrics for attestation", **said Jim Reavis, Executive Director of the Cloud Security Alliance.** "The Common Assurance Maturity Model framework has great promise to address this demand and the Cloud Security Alliance is proud to support this initiative and align our own cloud security metrics research with it."

83 VICTORIA STREET
LONDON SW1H 0HW

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