Scottish Information Assurance Forum

in association with the

National Information Security Conference

SEMINAR: Preparing for tomorrow's world today.
The Westerwood Hotel, North Lanarkshire
Wednesday 13th June 2012

Agenda (Subject to Change)

11.30 Registration Desk (11.30 – 17.00)

12.00 Lunch, Networking & Exhibition Hall

14.00 Welcome & Opening Words

Alan Moffat, Chairman of SIAF

The Scottish Information Assurance Forum (SIAF) is leading the way in improving information sharing and security practices across the different industry sectors in Scotland, through knowledge awareness seminars, networking events, think tanks and best practice workgroups. SIAF is a membership based organisation and is very pleased to offer this seminar in conjunction with the National Information Security Conference and announce that the SIAF Seminar is **FREE** to all delegates.

14.15 Keynote Presentation: Cyber Security

Anne Courtney, Scottish Government

14.45 From Cloud Security to Cloud Stewardship

Simon Shiu, HP Labs

As part of the cloud stewardship economics project we have been exploring enterprise risks associated with using cloud computing. We have focused on the implications of relying on chains of services drawn from a growing ecosystem of cloud providers. Following a series of surveys and empirical studies (including those performed at NISC in 2010) we have built a series of economic and system models of the ecosystem which we have been using to illustrate and explore several potential scenarios for cloud stakeholders.

15:15 Keynote Presentation: Fortinet - 2012 Threat Landscape

Shane Grennan, Country Manager, Fortinet

Over the last few years the Internet Threat Landscape has changed dramatically.
The industry has coined a new term, Advanced Persistent Threats (APT's) to describe a new range of threats that has emerged in that time. APT's encompass new attach vectors and also new attack sources, from organized crime gangs, hactivism groups to state originated cyber warfare. In this session learn about the motivation, sophistication, personal risk, rewards and gapping holes associated with todays Advanced Persistent Threats.

15.45 Information Security Incidents – Are They Reported? If Not, Why Not?

Mike Humphrey, Head of Information Assurance and Accreditation, Serious Organised Crime Agency (SOCA)

- Why do people find reporting incidents a challenge?
- What are the barriers and what can be done to overcome them?

16.15 Get Wise, Get Prepared or Get Done

Tony Neate, Get Safe Online

Not a day goes by without a new piece of sophisticated technology being announced, and today's users are hungry for even more. From our children to silver surfers – most of us are embracing this new technology. But do we think about the security implications? In the press, next to the announcement of that new piece of hardware or new cloud-based service, is the horror story of doom and gloom, allegedly reflecting some people's experience of the internet. But do we care? Is complicacy taking the place of good old common sense? Do we all need to be a victim before we start taking security seriously? Yes, we all need to be aware of the potential threats and respond to the risks. We need to educate in a positive way and hand some control back to the computer user. The internet is a great productive, educational and fun place to be. Let's keep it that way for everyone.

16.45 Future Risks – Including The Rise of the Hacktivism

Bill Buchannan, Professor, School of Computing, Edinburgh Napier University

As organisations move towards infrastructures which are highly dependent on their Web infrastructure, they are now at great risk from external parties who can use a number of motivations, such as for a political agenda, to compromise their activities. This presentation will show a number of recent cases which have resulted in serious loss of business confidence, and outline methods that can be used to support the detection and mitigation of the risks.

17.15 Closing Words

19:00 to Late Welcome Dinner: Your Passport to the World of Security

The welcome dinner will set the theme for the rest of the conference; a relaxed and informal chance to catch up with some of the latest developments amongst security vendors. Dinner will be an informal buffet presented in the exhibition hall, the sponsors will be available on the exhibition stands to demonstrate their current and future products. It will be a chance to catch up with some old friends and maybe make some new ones.

Thursday 14th June, 2012

Morning Session

(Subject to Change)

08:00 Registration

09:00 Chairman's Welcome: Alan Moffat

Alan Moffat MBA is the Managing Director of RSC2 Solutions and Founder and Chair of the Scottish Information Assurance Forum. Alan's career spans 30 years in Information Security and 10 years in Management Profiling.

09:15 KEYNOTE: BYOD - Nicotine for Networks?

Roger Hockaday, Aruba Networks

BYOD is like nicotine; highly addictive and potentially dangerous. But unlike nicotine, BYOD has not been around 500 years and we still have time to get control of it. Is there a role for consumer and highly mobile technology in the workplace whether bought by the employee, guest or provided by the organisation?

09:45 Visionary Statement: Managing Bring Your Own Device

Sian John, UK Security Strategist, Symantec

The iPad was the most disruptive technology of the last 10 years. It appealed to executives leading to the introduction of a consumer device into organisations and leading to pressure to allow these access to services. During this session we will discuss some of the challenges and risks of BYOD and things to consider before allowing access to the network.

10:00 Vulnerabilities of Communications Devices

John Bayliss, Communications Risk Management

It is generally agreed that education is the most important aspect of protecting your information. Some attacks are almost impossible to mitigate against, so knowing what form an attack might take is critical. With ever-increasing vulnerabilities around communication (Blackberries, mobiles, laptops, Bluetooth, WiFi), keeping your company data secure is critical to your business' survival. How can you ensure that your private commercial information stays just that - Private?

10:35 Visionary Statement: Advanced Evasion Techniques – How Scared Should You Be?

Bill Wood, Solution Architect, Stonesoft

Over the last year the cyber security landscape has changed - there are new risks, more complex threats and the innovation of hackers has accelerated at an astounding pace. We have also seen major security breaches against some of the largest global organisations: RSA, BAe Systems, Lockheed Martin and Nortel. Since their discovery a year ago, it's clear that Advanced Evasion Techniques are being used in anger and are a key player on the threat landscape. Many of the world's leading IT security professionals have been researching the threat in order to establish where AETs are being used and the extent of the risk they pose to organisations worldwide. See AETs in action bypassing Gartner quadrant IPS solutions.

10:50 Break, Exhibition and Networking

11:25 The Legal Aspects of Cloud Computing

Dai Davis, Technology Lawyer and Chartered Engineer

Is cloud computing for everyone? What are the contractual and legal risks of cloud computing? What are the legal-security implications? How should they be addressed? How can they be minimised and avoided? This workshop examines how cloud computing can be adopted and the dangers avoided on a practical level.

11:55 Visionary Statement: The 3 C's

Adam Perks, Barracuda

Today's IT department needs more technologies than ever before to protect effectively against attacks - both internal and external. As the internet continues to gain momentum, it's also essential to safeguard IT processes and corporate communications on a 24/7 basis. But with so many potential threats, it's easy to lose focus on where to begin. Barracuda Networks see the three "C"s; Cybercrime, Consolidation and Cloud, that are the main factors concerning all those responsible for IT security across the globe.

12:10 Physical Protection of Vulnerable Buildings

Government Security Adviser, CPNI

The session will cover the effects of blast and the various countermeasures than can provide stand-off distance from vehicle borne threats and mitigate damage to the fabric of the building and its contents and occupants.

12:50 How to survive in these Dangerous Times

Michael Oldham, CEO, Portsys

Security has always had its challenges. But today with the explosion of mobile devices, "bring your own device" and the cloud, organisations are losing control over their critical business information. The level of risk has gone up tremendously and shows no signs of abating. In days past, the IT Security department was the house of "NO". It was easier to control who could get access and who could not. Those days are largely gone in most organizations. Business needs almost ubiquitous access to information wherever it resides. And, if you impact the end-users and make it harder for them to do their day to day activities, they will sabotage any attempts at providing higher levels of security. So, how can you manage to regain control and make it easier for end-users so everyone wins?

13.05 Lunch, Exhibition and Networking

Thursday 14th June, 2012

Afternoon Session

(Subject to Change)

14:10 Securing the Mobile Enterprise

Adrian Price, CIO, Ministry of Defence

Trying to meet the user expectation to embrace new technologies, at the same time trying to preserve National Security, is a challenge at the best of times. When the mobile workforce is spread across the globe, often in inhospitable environments, the challenge is greater. This session explores some of the thought processes and development work the MoD has undertaken to solve this problem.

14:40 The Deadly Sins of Cloud Computing (and how to avoid them)

Mike Small, KuppingerCole

The Cloud provides an increasingly popular way of procuring IT services that offers many benefits including increased flexibility as well as reduced cost. It extends the spectrum of IT service delivery models beyond managed and hosted services to a form that is packaged and commoditized. However - many organizations are sleepwalking into the Cloud. Moving to the Cloud may outsource the provision of the IT service, but it does not outsource the customer's responsibilities. There are issues that may be forgotten or ignored when adopting the cloud computing. This presentation sets out the deadly sins of Cloud computing and then commandments to avoid them.

15:10 Visionary Statement: Discover how to share IL2 & IL3 data with external 3rd parties without the need to install or manage complex infrastructure.

Tony Pepper, Egress Software

Up until now, sharing confidential information across and outside Government typically presents organisations on both sides with various challenges to overcome. These include:

1. How can I access the data quickly and easily, without the need to install software or pre-establish trust relationships?
2. How can I guarantee that my recipient(s) will not lose or mishandle the data, placing my organisations reputation in danger and risking costly fines by the ICO?

Learn how Egress Software Technologies and their industry partners can offer a unique combination of on-premise and hosted accredited infrastructure, enabling individuals and business to deliver 'follow the data' control and auditing when sharing sensitive or personal information electronically.

15:25 Break, Exhibition and Networking

16:00 Visionary Statement: Business Continuity & Remote Access in 1 Simple Solution

Alwyn Nash, DataSecurity Manager, Checkpoint

16:15 To 17:30 Panel Session: The Diminishing Network Perimeter

Chair – Gerry O'Neill
Mark Brett, PSN Cyber Defence Team, **Cabinet Office**
John Strange, Deputy Director, **Serious Organised Crime Agency (SOCA)**
Mike Small, Fellow Analyst, **Kuppinger Cole**
Roger Hockaday, **Aruba Networks**
Shane Grennan, Fortinet

19:30 Drinks Reception

20:00 Gala Dinner: Ballroom

Join us in celebrating the 13th annual NISC Conference at the Gala Dinner.

Friday 15th June, 2012

(Subject to Change)

08:00 Delegate Networking Breakfast

Breakfast on the last day will be served in the exhibition hall. It will also be your last chance to get your passport stamped and submitted for the grand prize draw.

09:10 Chairman's Opening: Alan Moffat

Alan Moffat MBA is the Managing Director of RSC2 Solutions and Founder and Chair of the Scottish Information Assurance Forum. Alan's career spans 30 years in Information Security and 10 years in Management Profiling.

09:20 Keyonote: 12 Steps to Mitigating the Risk of Mobile Data Loss

Alistair Mutch, MobileIron

Corporate data has moved to the mobile device. IT professionals need to have strategies to reduce the risks from data loss, device loss, and employee misuse whether the device is corporate-owned or employee owned. This talk discusses 12 steps to achieve this.

09:50 Should we still worry about terrorist attacks in the UK, and if so, what form will they take?

Andrew Erving, former Head of Counter-Terrorism Intelligence, GCHQ

Now that Usama bin Ladin and co have been pretty well put out of action what is the present terrorist threat in the UK and elsewhere? What should we be concerned about now, especially in the run–up to London 2012? What can the government and the agencies do both to prevent attacks and, heaven forbid, to deal with the consequences? This session contains the personal impressions of a former practitioner, with experience in the London CT community and central government's COBR.

10:20 The Policing Response to Cyber Crime

Paul Hoare, Met Police

The remit of the PCeU is to reduce the harm caused to the UK and its citizens through serious cyber-crime. The main programmes of work are to improve mainstream law enforcement capability through training, improved process and tools, establishing regional PCeU's and building the central PCeU operational capability.The PCeU investigates the activities of criminals actively committing offences within in its remit, taking a dynamic team approach, combining the technical expertise and experience of its technical team, with the experience of detectives attached to the enforcement team, backed-up by a specialist intelligence development team, working up cases with urgency, and, where appropriate, drawing on the wider resources of the Metropolitan Police and other ACPO forces. Latterly the unit has also been combating the activities of loosely affiliated groups of individuals responsible for intrusions or denial of service attacks (DDoS) against the computer servers of large UK and US corporations and public and government bodies, in order to steal sensitive data, or to deny such bodies Internet access. These groups are motivated by a desire to disrupt, inconvenience or embarrass their victims in the furtherance of particular causes and have named themselves 'Hacktivists'.

10:50 Break, Exhibition and Networking

11:20 Social Media – Information Security Friend or Foe?

Graham McKay, Chief Information Security Officer, DC Thomson & Co Ltd

Graham takes you on a social media journey including the good, bad and ugly of social media from his companies perspective. Tips and tricks a plenty as well as advice on policy and strategy.

11:50 Common Sense is not that Common – Seizing the Initiative

Gerry O'Neill / Des Ward

The challenge of meeting multiple compliance and certification demands is overburdening already stretched businesses. Add to that, the move into the uncharted waters of mobile devices, supply chain and cloud assurance, ever increasing services and application available to both citizens and businesses, as well as the increasing criminal or activist risk, and you have a very challenging environment in which to operate. This update session will announce an exciting new development, The Common Initiative, which will aim to join up many of the perspectives and players who can steer a path of simplicity and visibility to the above environment, and bring back some common sense to how we are responding to these challenges. The session will also give an update on the repurposed forward direction of the CAMM initiative (the Common Assurance Maturity Model), a related project, which will bring transparency and measurability to the task of demonstrating assurance in the supply chain.

12:20 The Human Factor

Brian Hunter, Information Assurance Manager, Baillie Gifford

You may spend thousands on ensuring that you have the best technical defences against today's cyber attacks, but a good social engineer could breach your security with the unwitting and obliging assistance of your trusted staff members. Using phishing, deception, trickery, scams and maybe even some charm, coupled with a little technical wizardry, you could find the security of your environment compromised. This is a real-life example of what's possible. Artificial intelligence is no match for natural stupidity.

12:50 Chairman's Closing Words

13:00 Close and Lunch