Symposium on Security Risk, Cybercrime and Critical Infrastructure

Context and Aim

The main focus for the Symposium is to engage a wide range of domains to collaborate effectively, and to understand current and future threats to our citizens and society. The event is free, and is intended to increase the collaboration of organizations around Scotland. The Symposium is organised and delivered with the support of Scottish Enterprise, Finmeccanica Cyber Solutions, and Edinburgh Napier University.

This symposium aims to bring together knowledge from many different domains in order to create knowledge exchange and collaborative infrastructures, which address the key risks that Scotland faces. The focus on this symposium is security risk, cybercrime and the protection of critical infrastructure, with a key focus on:

- Collaborative networks within Scotland and links to the EU and the UK.
- Knowledge networks related to computer security, cybercrime and in risk analysis.
- Security and Cybercrime risks of the Cloud.
- Training requirements for Scotland related to Computer Security and Cybercrime.
- Emergency response infrastructures, and risk within critical infrastructure.
- Criminal risks and new attack vectors.
- Risks to privacy and identity theft.
- Intelligence-led activities.

The main Web site for the Symposium is at: http://scotlandcyber.com

Timetable

9-9:30am	Registration and coffee/tea (provided)
9:30-10am	**Introduction (Prof Bill Buchanan/Scottish Enterprise/Scottish Police)**
10-10:30am	**Sir Kevin Tebbit (Chairman of Finmeccanica UK)**
10:30-11am	**David Livingstone (Associate Fellow of Chatham House) Cyber Security -Time to Move Forward** A précis on the state and maturity of policy development when compared against the emerging cyber threat. The role of Government and an assessment of the level of regulation required to incentivise, or otherwise, the development of countermeasures in the commercial and public domains. What appears to be working, and what is not. The Virtual Task Force concept and its wider applicability. Collaboration within stakeholders and the importance of Trust in an integrated response. I will include some salient findings from the recent Chatham House study on Cyber Security and the Critical National Infrastructure.
11:05-11:30am **Parallel Session**	**Martin Borrett (IBM), The Cyber Security Landscape** Views and approaches to Cyber Security continue to evolve and mature. We will discuss current thinking on what cyber security actually is and the importance of public/private partnerships and information sharing in tackling this global threat. **Tony Povoas, Mobile technology and consumerisation: challenges for security models and practices. [Riady Lecture Theatre]** The talk addresses how consumerisation undermines traditional security models and control environments. It considers the complex trust relationships between the personal, mobile, corporate and data entities that make obsolete the traditional models and practices. It concludes by considering what the appropriate response is in order to address security and control in this context.

11:30-12:00pm **Parallel Session**	 **Ian Whittaker/Neil Logan (Amor Group), Basil Philipsz (DMS), Next Generation Identity Assurance** As the world continues its progression towards a cloudy future, public and private sector organisations are embracing the digital by default agenda. As citizens and customers the services we consume will be increasingly delivered electronically. Identity Assurance, the ability to reliably determine the identity of citizens and consumers, is a key enabler to facilitating this shift. Single-factor and two-factor authentication services work well in many cases but as recent high-profile news events have shown for our most sensitive services we need something better. The next generation of identity assurance offers mutual multi-factor authentication services. This talk looks at the topic Identity Assurance, explaining why it's become so important and describes a solution to providing the next generation of identity assurance. **Nathan Dornbrook (Vacta), Advanced Persistent Threats Detecting Insider Threat [Riady Lecture Theatre]** More attacks come from inside the enterprise than outside it. How can enterprises, most of which already have robust policies, ensure that they are detecting the internal threat? In this talk, Nathan Dornbrook will describe the tools that organisations have at their disposal to ensure that the internal threat is mitigated, and ways of measuring the success of these tools.
12:00-12:30pm **Parallel Session**	**Tabassum Sharif (Flexiant)/ Jamie Graves (Inquisitive Systems)** **David Stubley (7elements), APT in a Nutshell [Riady Lecture Theatre]** APT is used to describe a variety of attacks but has its origins in what would be categorised as state sponsored cyber espionage. This traditional cyber espionage was concentrated on government agencies and supporting defence contractors. This has been extended to encompass a wider focus, resulting in what is known today as APT. This talk will take a critical look at how APT is presented and the reality behind the hype.
12:30-1pm **Parallel Session**	 **Richard Nethercott (Logica), Monitoring Cyber Space: Considerations for international organisations.** Regardless of the size of our organisations, we are all moving towards operating on a global scale, given the nature of the web, how our partners and service providers operate, and the rise in cloud computing. However, these new international networks also bring greater exposure to Cyber Risks. How can we balance the need to embrace new technologies and ways of working while taking into account the increasing complexity of Cyber Threats as well as the ever-present legal requirements? **Nigel Jones/Cormac Callanan 2CENTRE – Cybercrime Centres of Excellence for Training, Research and Education – supporting a culture of international cooperation. [Riady Lecture Theatre]** 2CENTRE is an embryonic network of national centres of excellence that will provide a platform for future collaboration. A European Commission funding programme application has provided funding to begin the network. (**www.2centre.eu**) A Centre of Excellence is a cooperative effort of law enforcement, industry and academia to improve the knowledge and skills of those responsible for investigating cybercrime. For many years, Law enforcement Agencies have insufficient training options in IT forensics and cybercrime investigations, and, in Europe, generally depend on courses provided by Europol and/or Interpol. In addition, a number of countries have developed their own law enforcement cybercrime training programmes either alone or in conjunction with academic institutes.

1-2pm	**Lunch and coffee/tea (provided)**
2-2:30pm	**Prof Merabti Madjid (Liverpool John Moores University), Critical Infrastructure Cyber Security: The Global Challenge** This talk addresses the research and technical challenges of developing secure systems that encompass both existing legacy SCADA systems and new cyber communications systems and provide the fundamental foundation of technical security required to ensure critical infrastructure chains.
2:30-3pm	**Don Smith (Dell SecureWorks), Failure Forever? How to break the cycle of failure in IT Security** Had Wanamaker been referring to information security instead of advertising he would have said, "Half the money I spend on information security is wasted; the trouble is I don't know which half." Despite significant spend from organisations on security technology, security breaches are still a daily occurrence and all too often the result of a known threat and vulnerability that should have been fixed. Considering the risk landscape - Don will describe why new threat actors have changed this landscape adding significant complexity and entropy to the life of the security professional. In this session Don will present a bold view of the current state of information security and propose a refreshing, pragmatic approach for improving the security stance of any organisation.
3-3:30pm	**Coffee and tea (Provided)**
3:30-4pm	**Scott Chase (Raytheon Cyber) Five Things Hackers Do (And You Should Know About)** A look at some of the more unconventional techniques emerging in the hacker community including social network exploitation, physical attacks, psychological attacks and supply chain vulnerabilities. Scott will present a number of techniques that don't fit well into the broad categories of vulnerabilities we're all familiar with, and discuss how your organization can deal with them.
4-4:30pm	**Prof John Howie (Microsoft plc), Analysis of current cyberthreat trends, industry response, and defending the ecosystem.** Threats against computing continue to evolve, with potential impact to consumer, industry and society. In order to defend against cybercriminals, cyber terrorists and nation states engaging in cyber warfare, a broad coalition comprised of academia, industry law enforcement and government must come together to develop new tools, strategies and technologies. In his presentation, Microsoft Senior Director John Howie will provide a synopsis from Microsoft's most recent Security Intelligence Report, examine worrying trends, and discuss industry initiatives such as CloudSIRT.
4:30-4:45pm	**Scottish Cipher Challenge Award/Global Security Challenge**
4:45-5:15pm	**Oscar O'Connor, Services Director, Finmeccanica Cyber Solutions, Securing information and services in an environment without boundaries** In the early days of international networking, concepts like the *air gap* had not only resonance but real validity as it was easy to identify the one or two external access points and to erect reasonable defences on them. But things have changed and new ways of thinking about the security of information and services are required. The proliferation of the internet and networked services combined with the advent of the smartphone, 3G, WiFi and so on mean that every laptop and phone in an organisation represents an external access point to the

	network in one way or another.
5:15-5:30pm	**Refreshments**
5:30-6pm	**Roundup**

Organisers

- **Bill Buchanan** is a Professor in the School of Computing at Edinburgh Napier University and a Fellow of the IET and also a Fellow of the BCS.
- **James Cameron** (Scottish Enterprise).
- **Ross White** (Scottish Enterprise).
- **Sharon McGettrick** (Edinburgh Napier University). After graduating, Sharon began her career as a research scientist for an Oxford University spin out company
- **Aileen Wood** (Edinburgh Napier University). Aileen has more than 30 years' experience working with businesses in the private, public and third sector including chemical sciences, IT and agriculture.
- **Wendy Stewart** (Edinburgh Napier University).

Speakers

The speakers include:

- **Sir Kevin Tebbit**, Chairman of Finmeccanica UK.
- **Professor Merabti Madjid** is Professor of Networked Systems and Director of the School of Computing and Mathematical Sciences, Liverpool John Moores University, UK.
- **John Howie**, CIPP/IT, CIPP, CISA, CISM, CISSP is the Senior Director of Technical Security Services for the Online Services Security and Compliance (OSSC) team within Global Foundation Services at Microsoft Corporation.
- **Don Smith** is VP Engineering and Technology at Securework. He has worked in the IT industry for 18 years, starting his IT career with the groundbreaking Edinburgh University spin-off, Vision Group.
- **Scott Chase** is a technical director for Raytheon SI Government Solutions, and actively promotes information operations and information assurance.
- **Tabassum Sharif** is Director of Operations at Flexiant, a leading independent cloud platform provider and software and services company.
- **Nigel Jones MBE FBCS** is currently the law enforcement coordinator of the Cybercrime Centres of Excellence Network for Training, Research and Education (2CENTRE) and a director of Technology Risk Limited, a company specialising in technology risk solutions.
- **Martin Borrett** is the Director of the IBM Institute of Advanced Security in Europe. He leads the Institute and advises at the most senior level in clients on policy, business, technical and architectural issues associated with security.
- **Ian Whittaker** BSc FCA FIIA. Ian is a Senior Consultant with Amor Group, www.amorgroup.com, Scotland's largest independent IT Company having, inter alia, previously been an eBusiness Advisor to Scottish Enterprise, Group IT Director for one of Scotland's fastest growing Energy Service Groups and Head of Computer Auditing in Scotland and Northern England for an international accountancy firm.
- **Dr Basil Philipsz**, MIISP is the Managing Director of Distributed Management Systems, www.dms-soft.com, which has developed CASQUE, a multi factor authentication, key distribution and key management system.
- **Cormac Callanan** BA, MSc, MICS operates an independent consultancy company from Dublin, Ireland named Aconite Internet Solutions which provides expertise in policy development in the speciality area of international cybercrime and Internet security & safety.
- **Oscar O'Connor BSc CEng CITP FRSA MBCS MBCI**, is the Services Director, Finmeccanica Cyber Solutions at Selex Elsag and Committee Member BS25777:2008 (Pro Bono) at British Standards Institution. In the past he was a Programme Director at Adam Continuity and the Head of Professional Services at Dell Corporation, along with being the Programme Manager at Computacenter.
- **For others see http://scotlandcyber.com**