



8th International Information Security Conference & Workshops

Information Security: The Cloud and Beyond

1-7 November 2011

@ UNIVERSITY OF NICOSIA, Nicosia



ORGANISED BY:



UNDER THE
AUSPICES OF:



SUPPORTED BY:

UNIVERSITY OF NICOSIA



SPONSORED BY:



2nd NOVEMBER CONFERENCE PROGRAM



CYPRUS
INFOSEC



8:00 - 8:45 Registration - Welcome Coffee
8:45 - 9:00 Conference Opening & Addresses

Session 1 *Coordinated by Mr. Yiannos Pitas*

9:00 - 9:40 **Dr. Mike Chung** - KPMG: **Identity & Access Management Challenges in the Cloud**
9:40 - 10:20 **Mr. Aldis Vilums** - MicroSoft: **Here comes the cloud... What does it bring?**
10:20 - 11:00 **Mr. Fotis Kosmatos** - IBM: **Cloud Computing: Rethink IT, Reinvent Business**
11:00 - 11:30 *Coffee Break*

Session 2 *Coordinated by Dr. Ioanna Dionysiou*

11:30 - 12:10 **Mr. Lars Jacobs** - KPMG Forensic: **CSI in a Digital World**
12:10 - 12:50 **Mr. Jorge Sebastiao** - Regional VP EMC:
Tracking and Implications of Stuxnet, modern weapons of Mass Destruction
12:50 - 14:00 *Lunch*

Session 3 *Coordinated by Mr. Dinos Konis*

14:00 - 14:40 **Mr. Vernon Poole** - Sapphire Technologies Ltd:
Governance of Information Security - emerging ISO27014 & other initiatives
14:40 - 15:20 **Dr. Andrew Jones** - Argus Systems Group: **Security 2.0**
15:20 - 16:00 **Mr. David Lacey** - ISSA-UK:
The Future of Information Security: New Priorities, New Skills and New Technologies
16:00 - 16:15 *Short break*
16:15 - 17:15 **Mr. Winn Schwartau** - Author, Futurist: **What Keeps Me Up At Night!** *via videoconference*

17:15 Conference Closure

WORKSHOPS 2011



CYPRUS
INFOSEC



WORKSHOP 1
Tuesday, 1 November
Mr. Vernon Poole ISACA's new Business Model on Information Security

Full Day - 9:00 - 17:00

BMIS: THEORY - morning session will outline why organisations need to adopt a Business Model for Information Security (BMIS) – and how to deploy the required 'cultural dynamic interconnection'.

Background

The present approach to information security within most organizations is piecemeal and with the growing number of information threats, we need a systemic Model. BMIS will allow organizations to both monitor and learn from information security events and set effective mechanisms in place to 'minimise the opportunity for such incidents to re-occur'. BMIS will be vital to protect critical IT activities and therefore to increase business value and reduce business risk.

Content

The training will outline how organizations are adopting BMIS to respond to a growing number of threats to meet regulatory and contractual requirements and demonstrate continuous improvement.

The main components of the Model will be explored:-

4 main elements:

1. Organisation (Strategy) – embraces risk/governance/IS at board level
2. People – addressing human behaviour & leveraging human intelligence
3. Process – need for an appropriate IS framework
4. Technology – embrace the most appropriate technical solutions available

6 dynamic interconnections:

1. Architecture – IS design in the overall infrastructure (h/w; s/w)
2. Culture – build an intentional culture (set of expectations & desires)
3. Emergence – be flexible to change (benchmarking; use of best practice)
4. Enabling & Support – aligned relationship between process & technology
5. Governing (Governance) – business alignment; trust & communication
6. Human Factors – usability factor (ease of use & understanding)

Benefits

1. Establish an effective Business Approach Businesses and organizations need to under the importance of the 'Organisation – Strategy/Direction' element to set up a comprehensive management & reporting. The approach calls for the concept of shared responsibility to be established supported by effective governance mechanisms.
2. Greater Emphasis on People element Most security incidents & breaches have a significant 'people' factor – but how well do we understand human behaviour & do we deploy human intelligence effectively? This training will provide practical examples on past cases & what can be learnt
3. Detailed coverage of Dynamic Interconnection - Culture The training will outline the

importance of the Cultural Dimension and the need to build an 'intentional culture' with appropriate interconnection values

BMIS: UK PRACTICE - afternoon session will outline why the UK Government adopted the concepts of BMIS – and how they translated its requirements into a new Security Policy Framework to create a new 'cultural approach to IS'.

Background

The training will outline how the UK are adopting BMIS to respond to a growing number of threats; to meet regulatory and contractual requirements; and demonstrate continuous improvement to UK citizens.

The UK Government's position is that:

- 'Effective security is central to how we handle many of the challenges facing Government. It is vital for public confidence & the effective/safe conduct of public business'.
- The new Security Policy Framework replaces the Manual of Protective Security & the Counter-Terrorist Protective Security manual—sets out mandatory standards, with guidance on Risk Management & new compliance/assurance arrangements
- Focus – IS policies & processes in line with new & changing threats based on four levels:
 1. Security not only supports business goals but to be viewed as a business enabler
 2. 5 core security principles
 3. 7 key policy documents – 70 minimum

mandatory requirements (MR)

4. Detailed tools for practitioners (technical standards; policy/guidance; websites)

Content

This training will outline:

- A. The background to the new Security Policy Framework (SPF) & why the UK Government adopted the BMIS approach
- B. Explain in detail the seven IS policies outlined in the UK Government's SPF (and how they could be applied in other countries) namely:
 1. Governance, RM & Compliance
 2. Protective Marking & Asset Control
 3. Personnel Security
 4. IS & Assurance
 5. Physical Security
 6. Counter – Terrorism
 7. Business Continuity
- C. The SPF is currently on Version 5.0 (February 2011) – it is continually being improved and our speaker is instrumental to the changes and developments.

Benefits

1. What lessons can be learnt from the UK experience and how easy can they be deployed
2. Which aspects of Security Policy Framework can be implemented quickly
3. Can a similar framework be established in Cyprus using BMIS Model – an open discussion

WORKSHOPS 2011



CYPRUS
INFOSEC



WORKSHOP 2

Thursday, 3 November
Mr. David Lacey *Managing the Human Factor in Information Security*

Morning 9:00 - 13:00

Computers don't commit crimes, people do. It's also people that design and operate systems, manage access rights, cause incidents and help recover from them. This workshop will examine the increasing influence of people in a networked information society, and explore techniques for transforming their awareness, attitudes and behaviour.

The workshop is suitable for managers of all levels of experience and seniority who wish to improve the knowledge and skills in conducting security awareness programmes and influencing organisational behaviour.

Subjects covered will include:

- Why people are now the most important factor in information security
- Building a healthy security culture
- Managing the human factor in risk management
- Designing effective awareness programmes
- Shaping attitudes of managers
- Changing user behaviour

At the end of the workshop, attendees will have a good understanding of the principles and recommended techniques for designing an effective security awareness and behaviour change programme.

WORKSHOP 3

Thursday, 3 November
Mr. Lars Jacobs *Forensics Hands-on*
Co-organised with the ISACA Cyprus Chapter

Afternoon 14:00 - 18:00

In current lifetime it is more common that our daily activities are interacting with digital data than not. It has simply become almost impossible to live a normal life without leaving behind digital traces on computer systems, in communication systems or in the web. If it is not you who creates the trace it might be others who do so to record activities that relate to you.

With this growing amount of digital data the opportunity and possibilities for fraud or other forms of abuse are increasing as well.

Therefore the digital part in (forensic) investigations increases every day, in addition the continuous developments in IT introduce new challenges performing forensic investigations.

This workshop consists of an introduction into the world of digital forensics where the attendees will experience it themselves during an hands-on case study. This case study will revolve around the following question:

Confidential information has been leaked on the web, which traces does that leave behind and which information could we possible get out of it?

To answer these questions the workshop will look into: **Logging, Microsoft Windows systems and Networking.**

The workshop is suitable for:

Everyone with a basic knowledge of IT systems who like to be introduced into digital forensics.

WORKSHOPS 2011



CYPRUS
INFOSEC



WORKSHOP 4 Friday, 4 November Mr. Jorge Sebastiao Security Framework Formalization

Full Day - 9:00 - 17:00

Overview

The purpose of the security framework seminar/workshop is to define the overall set of methodologies, standards and tools which will be applied collectively to deliver a complete information security management strategy and associated practical implementation. The security framework provides the 'glue' to join these different disparate methodologies and approaches towards infosec, and it also defines any additional methods and security processes for those areas where there are shortcomings either due to maturity of used technologies.

Who Should Attend

This course is designed for Chief Security Officers (CSO), Senior Managers, IT Managers, Systems Managers, IT Security Officers, or ICT Auditors.

Pre-requisites

There is no formal technical pre-requisite for the course. Basics about ICT environment and applications. Basics about ICT processes and knowledge of ITIL is useful.

Contents and detailed agenda

Part 1: Service Description

This general description will cover the following points:
Nature of the business, general purpose of the service being provided;

- Your business, its Customers, other parties involved;
- General security objectives and outline security policy of the business;
- General security features required;

- Obligations of the user of the IT services;
- General conditions for use, limitations of use of the IT services;
- Compliance with standards, laws and regulations, achieved certificates, licenses or accreditations;
- Overview of the security measures and trust assessment methods used (i. e. a summary of the other parts of the Trust Assessment Specification) and a high-level view of their relationships.

Part 2: Technical Security Aspects

This part addresses all technical security features used in the provision of the service. It is structured into those technical features that are part of products developed independently by a third party. It also addresses technical security features implemented in hardware or software developed by the company or by a third party under a contract by the company. The following information will be covered in this part:

For products/Services:

- Description of IT-products/Services used and the security features of these products;
- Description of the way the IT-products are used to provide the service;
- Description which risks are addressed by the security feature;
- Description of the relevance of the product within the life cycle phases;
- Description of dependencies on other security features;
- Description of the assurance given by the product

manufacturer as well as additional own or third party assessments performed.

For own developments:

- Description of the hardware and software developed by the company or on its behalf;
- Description of the security features of this hardware and software;
- Description of the way this own developments are used to provide the service;
- Description which risks are addressed by the security feature;
- Description of the relevance of the developed hardware or software within the life cycle phases;
- Description of dependencies on other security features;
- Description of the assurance methods applied within the development as well as during operation and maintenance.

Part 3: Physical Security Aspects

This part addresses all physical security measures. It will contain:

- Description of the physical protection features used for the protection of service critical assets;
- Description of the risks reduced by those security features;
- Description of the relevance within the life cycle phases;
- Description of the dependencies on other security measures;
- Description of assurance methods used to assess the effectiveness of the physical security measures.

The security framework presents just an overview of

the aspects mentioned, referencing further documents that contain additional details on the physical protection features or the methods used to assess their effectiveness.

Part 4: Operational Aspects

This part addresses the Operational Procedures defined by the company to counter risks identified in the risk assessment. It covers the following components:

- The security critical operational procedures implemented;
- The risks addressed by the procedure;
- The life cycle phases addressed by the procedures;
- The dependencies on other security measures;
- Change and Configuration Management
- Patch Management;
- The assurance methods used to assess the effectiveness of the operational measures.

Part 5: Personnel Aspects

This part addresses the Procedures and Conditions imposed upon Personnel by the company to counter risks identified in the risk assessment. It must provide descriptions of:

- The personnel measures implemented to protect the service;
- The risks addressed by the measure;
- The dependencies on other security measures;
- The assurance methods used to assess the effectiveness of the measures.

WORKSHOPS 2011



CYPRUS
INFOSEC



WORKSHOP 5
Monday, 7 November
Mr. Demetris Kachulis Applications Security and Auditing Essentials

Morning 9:00 - 13:00

All companies today depend on software applications for important aspects of their operations. An erroneous piece of code can have disastrous implications for a company, such as losing huge amount of money or even threatening their very existence. In today's world, where we have off-shore development, third-party software, wireless devices and so many other factors, the risk exposure increases substantially. This makes the need of application security crucial within every organization. When we say "Securing an application" we mean trying to avoid security compromises, reduce vulnerabilities and prevent data corruption.

IT Auditors and Security Experts should be involved in every phase of the development process. After the application goes live, application reviews and audits should be conducted on a yearly basis, or after product enhancements. This workshop will cover the functions of both the Security Experts and the IT Auditors as both roles aim at ensuring error free software.

Subjects covered will include:

- What is Application Security?
- Software Development Life Cycle and Security.
- Best practices for developing secure applications.
- Security maturity models.
- Application Systems Reviews requirements.
- Application Auditing Planning Considerations.
- Documenting transaction flow and testing system controls.

This workshop is suitable for everyone with a basic knowledge of IT systems, interested in application security and auditing.

SPEAKERS 2011



CYPRUS
INFOSEC



Dr. Mike Chung

Dr. Mike Chung is currently manager at KPMG in the Netherlands, and is responsible for IT- and business architecture advisory services with emphasis on information security. He also leads Identity Management and performance audits. He is the foremost specialist within KPMG NL on cloud computing and online sourcing. Dr. Chung has been active in the IT sector for over 12 years ranging from system design to programme management. KPMG's clients describe Dr. Chung as being "exceptionally disciplined, focused on results and a real team player with a great sense of humour."

He has previously worked for T-Mobile and the Deutsche Telekom AG before joining KPMG.

Mike publishes frequently on various IT topics, and teaches IT architecture at several universities.



Mr. Lars Jacobs

Mr. Lars Jacobs works within the Forensic Technology unit of KPMG in the Netherlands. This unit supports forensic investigations (such as fraud, AML, compliance, tax irregularities) as well as performing Data Analytics and Electronic Discovery projects. Within the larger domain of

fraud and misconduct Lars specializes in Computer and Network Forensics. Prior to joining KPMG, Lars studied towards his degree in network forensic research at Zuyd University of Applied Sciences(the Netherlands).



Dr. Andrew Jones

Dr. Jones is the recent Chief Executive Officer and President of Argus Systems Group.

Argus Systems Group is the developer of PitBull trusted operating systems that are based on various commercial operating systems. Argus developed an alternative to Trusted Solaris based on Solaris 8 over twenty years ago. Later Argus offered a similar product for Solaris 10 that provided the same architecture and features of PitBull for Solaris 8.

Argus developed PitBull for IBM's AIX operating systems and now that product is sold by IBM as Trusted AIX. Most recently, Argus developed PitBull for Red Hat Enterprise Linux. General Dynamics C4Systems bought Argus and continues to develop the PitBull product line.

Dr. Jones was a founding member of Open Prairie Ventures where he evaluated business plans and potential investments. He was also the lead investor when Open Prairie acquired the assets of Argus.

Dr. Jones has been the founder and operator of several new technology business and taught technology commercialization and other subjects at the University of Illinois.

Dr. Jones received his PhD from the University of Alabama in Physics (1975), an MBA from the University of Illinois (1978), and a BS and MS in Physics and Math from the University of Alabama (1965, 1972).

SPEAKERS 2011



CYPRUS
INFOSEC



Mr. Demetris Kachulis

Mr. Kachulis is currently the managing director of Eldion Consulting and an Associate of the Consultancy Unit of the University of Nicosia. He is a Collaborative Technical Management and IT Security professional with more than 20 years of Wall Street experience; strong technical base developed and extensive “hand-on” IS experience in the development; maintenance and operations of various financial systems.

With over 20 years experience in the IT consulting industry, he has provided technical and management consulting to a number of clients. He has created new IT organizations; managed multiple complex projects; created IT strategies; procedures and policies. He has provided expert analysis and

reviews in critical projects; IT security system implementations; auditing procedures helping clients deliver outstanding solutions.

He has worked with Goldman Sachs, Citibank, Morgan Stanley, Bankers Trust, Deutsche Bank, New York Life, Consolidated Edison of New York and The Depository Trust Company

He holds an M.S. in Computer Science from Polytechnic University, an MBA from Adelphi University, and he is a Certified Information Technology Auditor (CISA), Certified Information Technology Security Professional (CISSP) and Master Project Management(MPM).



Mr. Fotis Kosmatos

Mr. Fotis Kosmatos is the Cloud Services Leader of IBM Greece and Cyprus.

Within his role, he is helping enterprises of all sizes in Greece and Cyprus to assess cloud readiness, develop adoption

strategies and identify business entry points in order to accelerate the adoption of a Cloud Computing strategy within their companies.



Mr. David Lacey

Mr. David Lacey, Director of Research, ISSA-UK

Mr. David Lacey is a leading expert on information security and risk with more than 25 years experience of directing corporate policy and programmes for the UK Foreign & Commonwealth Office, Royal Dutch/Shell and the Royal Mail. David is a keen innovator and is responsible for developing many contemporary ideas and techniques. He was the creator of the body of text that is now ISO 27002, and the

founder of the Jericho Forum. David is now an independent researcher, writer and consultant, and the author of the books “Managing the Human Factor for Information Security” and “Managing Security in Outsourced and Offshored Environments”. He is a member of the Infosecurity Europe “Hall of Fame”.

SPEAKERS 2011



CYPRUS
INFOSEC



Mr. Vernon Poole

Mr. Vernon is Head of Business Consultancy, responsible for Sapphire's team of consultants who deal with Information Assurance/Governance and all best practice standards on Information Security Management and associated areas (ISO27000 series; ITIL; COBIT5; RiskIT).

Vernon began his career in consultancy with CAPITA and has over 20 years experience in information security management consultancy & training. He has also worked in the public sector (local & central government) and with Aid to Industry (audit & security training group) – the latter being acquired by Deloitte which resulted in Vernon becoming a European leader performing a number of Information Security and Control related assessments on behalf of a number of major clients.

Vernon is a CIPFA qualified accountant and a qualified Information Security Manager (CISM). He is currently one of the most respected CISM trainers for ISACA. Vernon is also a founder member of the UK & International 27001 User Groups and a recognised adviser to senior management on the importance of 'Information Assurance'.

This work lead Vernon to becoming a respected representative on the IT Governance Institute – where Vernon is recognised as one of the thought leaders on Information Governance. He now sits on ISACA's new COBIT5 Taskforce developing ISACA's new in depth approach to Information Governance. In January 2008, he gained the ISACA certification – CGEIT (Certified in the Governance of Enterprise IT) which has led Vernon to being involved in many Information Governance assignments in UK. In August 2011, he gained the latest ISACA certification – CRISC (Certified in Risk & Information Systems Control).

At Sapphire, Vernon has worked with many organisations in developing tailored Information Security Governance models to enable clients to benchmark their Information Security Improvements. Vernon covers a wide range of topics, from Corporate Governance; ISO27002; Government's Security Policy Framework; & Board Level Assurance.



Mr. Winn Schwartau

Mr. Winn Schwartau is one of the world's top experts on security, privacy, infowar, cyber-terrorism and related topics. Provocative, informed, challenging, he's on the leading edge of thinking, writing and speaking. Highly technical security subjects are made understandable, entertaining, engaging and thought-provoking. Audiences find themselves challenged with original ideas which are related through historical analogy and metaphor and made relevant to the present and future world.

Among his numerous awards, he was named one of the Top 20 Security Industry Pioneers in November 2009, one of the Top 25 Most Influential People for 2008 by Security Magazine, and voted one of the Top 5 Security Thinkers for 2007 by SC magazine.

In 2002, he was honored as a Power Thinker and one of the 50 most powerful people by Network World.



Mr. Jorge Sebastiao

Mr. Jorge Sebastiao
Regional Vice-President
EMERGING MARKETS COMMUNICATIONS, CYPRUS

With over 26 years of experience Jorge helps organizations and individuals understand and get the best out of latest in Telecom, Satellite, Cloud Services, Managed Services, IT Outsourcing, Business Continuity and Disaster Recovery Planning. Jorge focus on: ITO , SAAS , BCB , DRP , Risk Management, security , telecommunications , wireless , satellite, wimax, voip , training , Education and International Professional Speaking. Jorge as done outsourcing

transformations in diverse geographies Canada, Europe, Middle East and Africa, with a career spanning Consulting, Government, Business, Integrator, Vendor and High tech startup. I lead a very busy schedule helping people and organizations with the management of risk, security, wireless, education, mobility, so that leaves very little time for family and relaxing. So the little personal free time we have with family and friends is very valuable. Languages: English, French, Portuguese, Spanish More details on Jorge are available at: <http://www.linkedin.com/in/sebastiao>

INFOSEC 2011



CYPRUS INFOSEC



DATE	TIME	EVENT	MEMBER PRICE *	NON MEMBER PRICE
1 Nov	Full Day 9:00 - 17:00	Workshop 1: Mr. Vernon Poole - ISACA's new Business Model on Information Security	€125	€150
2 Nov	Full Day 8:30 - 17:30	Conference	€100**	€125**
3 Nov	9:00 - 13:00	Workshop 2: Mr. David Lacey - Managing the Human Factor in Information Security	€75	€100
3 Nov	14:00 - 18:00	Workshop 3: Mr. Lars Jacobs - Forensics Hands-on	€75	€100
4 Nov	Full Day 9:00 - 17:00	Workshop 4: Mr. Jorge Sebastiao - Security Framework Formalization	€125	€150
7 Nov	9:00 - 13:00	Workshop 5: Mr. Demetris Kachulis - Applications Security and Auditing Essentials	€75	€100

All prices include 15% VAT.

* For CCS members, CEPIS members and members of the ISACA Cyprus Charter.

** 25% disc to be granted on conference price for delegates attending any workshop.

ROOMS:

Conference: UNIVERSITY OF NICOSIA: UNESCO Amphitheater, Europa Building

Workshops: UNIVERSITY OF NICOSIA: M106 Conference Room, Millenium Building, 1st Floor

Lunch (Conference and full day Workshops): UNIVERSITY OF NICOSIA: Gallery Restaurant, Main Building, Level -1

REGISTRATION AND PAYMENT THROUGH www.ccs.org.cy

FOR ANY INFORMATION OR ENQUIRIES: info@ccs.org.cy

CLICK
HERE TO
REGISTER



CYPRUS
COMPUTER
SOCIETY

Cyprus Computer Society

11 Florinis Str, City Forum, 3rd Floor, Office 303, 1065 Nicosia, Cyprus

P.O.Box 27038, 1641 Nicosia, Cyprus

Tel: +357 22460680 Fax: +357 22767349

www.ccs.or.cy info@ccs.org.cy