

Asia Data Security Forum

Strategies to Prevent Data Loss and Information Theft

Parkroyal Kuala Lumpur • 3 & 4 May 2010

Our expert line-up of industry leaders:



Roderick MacKinnon
Associate Principle Consultant
Griffin Security Group, United Kingdom



Nigel Phair
Australian Graduate School of Policing
Charles Sturt University, Australia



Kanwal K Mookhey
Founder
Information Security Institute, India



Wong Onn Chee
Chief Technology Officer
Resolvo Systems, Singapore



Lt Col (Rtd) Sazali bin Sukardi
Head, Strategic Policy & Research
Cyber Security, Ministry of Science & Technology, Malaysia



Chan Kin Chong
Vice President – Information Risk Management
JP Morgan, Singapore



Vikram Asnani
Senior Consultant
Data Security Council of India, New Delhi



Antony Ma
Chairman
Professional Information Security Association, Hong Kong



Ramachandran Narayanan
Assistant Director – InfoComm Division
National Library Board, Singapore

The data of a company is increasingly becoming a major asset of the company. However, most are still unaware how vulnerable their customer data is and how much risk they are facing in the event of data loss or data theft. Safeguarding the data of the company is becoming a major concern for many organizations particularly those in government departments, banks, financial institutions, retail as well as data warehouses. With the rise of the internet today, your company data is increasingly at risk of theft or data loss. Data can be transferred or manipulated easily today and your business is at the highest risk of losing vital company data, theft of your customer information or worst, information of your customers fall into the hands of unauthorised person(s) or competitors with malicious intent. The guidelines and action plans provided during this forum by industry experts and information security guru's would give you the latest in data security vulnerability, trends and countering threats from inside and outside.

Key Highlights

In this conference, you would be able to learn about:

- **Latest** trends and developments in data security arena at an international level
- **Preventive** steps to assure security of data and protecting information of customers
- Planning and implementation of **best techniques** merging with available technologies
- **Shifting paradigms** of e-Security to management involving humanware from Security / Technology hardware
- **Latest techniques** to prevent loss and ways to investigate theft of information
- Enforcement and implementation of **IT policies** at organizational level to ensure its activation and functionality on day to day basis
- Novel ideas to **combat** security breaches and prevent identity thefts

Who Should Attend?

Vice Presidents, Directors and Heads of:

- IT / MIS / ICT
- Data Protection
- Legal (IT)
- Government
- IT Security / Internet Security
- Data Warehousing
- E-Business / E-Commerce
- Financial Institutions
- IT Vendors
- Any organization or company that has a large amount of customer data or information

FREE Publication

Register by 9th April 2010 for a FREE publication on Data Security

For sponsorship or registration, call
+603 4270 3331

Asia Data Security Forum

Strategies to prevent Data Loss and Information Theft

Monday, 3rd May 2010, Parkroyal Kuala Lumpur, Malaysia

+603 4270 3331

8:30 am Registration

9:00 am Welcome remarks from the chairman

Roderick MacKinnon
Principle Consultant
Griffin Security Group, United Kingdom

9:15 am **Laying The Foundation For Best Data Protection Strategy**

- Learning about industry's intention to bring a new policy initiative to ensure an adequate level of security and the resilience of critical data like Identity of customers
- Raising awareness about the risks and the need for preparedness and developing a sound IT governance system outlining e- security measures.
- Recommending key activities for improvement

Lt Col (Rtd) Sazali bin Sukardi
Head, *Strategic Policy & Research*
Cyber Security, Ministry of Science and Technology,
Malaysia

10:00 am **Assuring Data Leakage Detection and Prevention**

- Identifying points of leakage and preventive strategies for minimizing data loss
- Reviewing and Implementing new technologies to boost the preventive strategies
- Discussing the role of data breach notification laws and procedures

Wong Onn Chee
Chief Technology Officer
Resolvo Systems, Singapore

10:45 am Morning Refreshments / Network Break

11:15 am **Data Encryption: Enterprise Tool for Data Protection**

- The myths of encryption and adopting encryption to protect computer infrastructure
- Aligning encryption with communications and data storage
- Handling encryption and mobility
- Review of encryption market today: leaders and challengers

Kanwal K Mookhey
Founder
Information Security Institute, India

12:00 pm **Data Theft Investigation Processes**

- Understanding process of identification of theft
- Location of evidence and potential suspects
- Tracing the suspect through electronic medium
- Understanding format of reporting criminal activities to the authorities to improve data safety
- Liaison with law enforcement agencies

Nigel Phair
Australian Graduate School of Policing
Charles Sturt University, Australia

12:45 pm Networking Lunch

1:45 pm

Understanding and Implementing New Identification and Authentication System to Combat Identity Theft

- Identifying weak parts of your company and measure vulnerability of identified areas
- Developing a sound authentication system to prevent data being get stolen
- Formulating a policy framework for identification and authentication systems

Chan Kin Chong
Vice President – Information Risk Management
JP Morgan, Singapore

2:30 pm

Building and Enforcing Data Security and Identity Theft Policies

- Analyzing and understanding environment thoroughly of your company before formulating security policy
- Develop a change management mechanism to enforce security policies fitting with IT strategy
- Using technologies to enforce policies for data and Identity theft

Roderick MacKinnon
Principle Consultant
Griffin Security Group, United Kingdom

3:15 pm

Afternoon refreshments / Network Break

3:45 pm

Secured and Sustainable IT Environment for PoC projects:

- Importance of innovation in organizations, so as to be competitive and relevant in the era of rapid technological developments
- Problems of testing new hardware and software, without impacting security and performance of the existing IT infrastructure
- How IT is able to provide a secured and sustainable environment test the effectiveness and usefulness of a certain piece of new technology?
- Experience of National Library Board, in providing a Sandbox environment for PoC projects, with faster provisioning using Virtualisation techniques

Ramachandran Narayanan
Assistant Director – InfoComm Division
National Library Board, Singapore

4:15 pm

“Beyond the Firewall” – Strengthen Your Security System by Reviewing Data Security Essentials:

- Understanding and developing tools to assess threats and risks of environment your system is expose to.
- Building foolproof channel to facilitate secure data transfer and flow within and outside organization.
- Setting up standard security and communication processes among IT teams

Vikram Asnani
Senior Consultant
Data Security Council of India, New Delhi, India

5:00 pm

Conference Close

Speaker's Profile

Roderick J N MacKinnon

*Principle Consultant
Griffin Security Group, United Kingdom*

Roderick MacKinnon is the Principal Consultant with Griffin Security Group. His extensive specialist security profile spans some 30 years, encompassing all aspects of protective security and resilience within the modern business environment. His developed expertise is well-recognised and he has formerly held both senior executive 'in-house' appointments and as an independent consultant, within diverse and dynamic business environments in the UK and abroad, with high-profile UK Government bodies, international commercial organisations and 'big brand' global financial institutions; protecting knowledge and information in a way that enables smooth business has been a central and common theme. Roderick has developed an intimate understanding of the challenges facing organisations when determining their response to the many security-related and other disruptive risk natures that can threaten their business objectives. Consequently, Roderick focuses on demonstrating the 'added value' from effective risk management and building strategic risk-control solutions that match the operating environment and optimise business achievement. As part of an extensive range of specialist and professional development, Roderick served in the UK military and is a graduate of the UK Strategic Police Command Course for designated chief police officers from the UK and international policing arena.

Ramachandran Narayanan

*Assistant Director – InfoComm Division
National Library Board, Singapore*

Ramachandran Narayanan has more than sixteen years of experience in the development and management of Enterprise IT services. Rama graduated in *Electronics & Communications Engineering* from India in 1984, and obtained a postgraduate degree in *Communication & Network Systems* from NTU, Singapore in 2004. Rama also holds an MBA degree from Birmingham Business School (UK) that helped him to think beyond IT and to reinforce his experience in aligning IT services to the business. After starting his IT career as a Network Engineer, Rama has gained much expertise in Systems, Infrastructure, and ICT management. A strong believer in ITIL methodologies and processes, Rama has also attained certifications in ITIL, COBIT, and COMIT, the last one being awarded by Singapore Computer Society in the area of Outsourcing Management for IT. Since 2000, Rama has been with National Library Board (NLB), a statutory board under the Government of Singapore, with 37 million visitors and 28 million library loans per year across the 23 public libraries under the NLB. As Asst Director in the InfoComm Division of the NLB, Rama is responsible for the ICT infrastructure projects and operations. Through his leadership and technical strength, Rama has been able to deliver reliable and cost-effective IT services in supporting NLB's business operations.

Vikram Asnani

*Senior Consultant
Data Security Council of India, New Delhi, India*

Vikram is currently working as a Senior Consultant, Security Practices with Data Security Council of India (DSCI). He holds a foundation certificate in ITIL V3 and have been trained as ISO 27001 Lead Auditor. Data Security Council of India (DSCI) has been established as an independent self regulatory organization (SRO) by NASSCOM, as an industry initiative to focus on best practices and standards for data protection. Along with this program Vikram is also engaged in DSCI outreach program at national and international platforms for establishing collaboration with different legal and regulatory bodies, data protection authorities, global clients and outsource service providers of all categories including small and medium players. Vikram is also closely working with Department of Information Technology (DIT), Govt. of India, on cyber security initiatives, security and privacy surveys and making of rules for IT Act. Prior to joining DSCI, Vikram was attached to Protiviti India Pvt. Ltd, a Global Risk, Business Consulting and Audit firm as a Senior Consultant in Technology Risk Consulting Services, Tata Consultancy Services (TCS) as a Consultant, Information Risk Management. Under the consulting wing of TCS, he had executed different security consulting engagements for different clients across the globe and in different industry domains during his tenure at these organizations.

Chan Kin Chong

*Vice President – Information Risk Management
JP Morgan Chase Bank, Singapore*

Mr Chan Kin Chong is the Information Risk Manager with JPMorgan Chase Bank for the Asia Pacific region, a regional risk management role. He has been actively involved in the related fields of technology and information security for more than ten years and has diverse experience in planning, designing, implementing and managing IT security initiatives. Kin Chong holds the position of Chairman of the Security and Privacy Standards Technical Committee under the Singapore IT Standards Committee (ITSC) and represents Singapore in ISO/IEC JTC 1 SC 27 and the RAISE Forum. He also sits on the Executive Committee of the Association of Information Security Professionals, looking after the interests of security professionals in Singapore. As recognition for his years of service and contribution to the Singapore standardisation programme, Kin Chong was awarded the 2009 Distinguished Award by SPRING Singapore. Kin Chong holds Double (Honors) Bachelor degrees in Mathematics and Computer Science from Carnegie Mellon University. He is also a Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA), and Member of the AISP.

Nigel Phair

*Australian Graduate School of Policing
Charles Sturt University*

Nigel Phair is a specialist in cyber crime and speak regularly both in Australia and internationally (most recently as an invited guest at Cambridge University). He is an executive advisor, internet analyst, media commentator, author and widely acknowledged as a authority in the intersection of society, technology and crime. Nigel has spent over four years at the Australian High Tech Crime Centre, where he led investigations and represented the Centre in numerous intergovernmental and external forums. He has extensive experience working with a variety of industry groups, including banking & finance and the telecommunications sector. Nigel is a Senior Fellow within the Centre for Transnational Crime Prevention, University of Wollongong and a Lecturer within the Australian Graduate School of Policing, Charles Sturt University. As well as an undergraduate degree, he holds a Master of Public Policy and a Master of Law. He is a Graduate of the Australian Institute of Company Directors and has published a critically acclaimed book detailing the international impact of cyber crime.

Kanwal K Mookhey

*Founder
Information Security Institute, India*

Kanwal K. Mookhey (CISA, CISSP, CISM) is the Principal Consultant and Founder at Network Intelligence as well as the Founder of The Institute of Information Security. He is an internationally well-regarded expert in the field of IT governance, information risk management, forensic fraud investigations, compliance, and business continuity. He has more than a decade of experience in this field, having worked with prestigious clients such as The Indian Navy, United Nations, Abu Dhabi & Dubai Stock Exchanges, State Bank of India, Atos Origin, Saudi Telecom, World Customs Organization, Capgemini, Royal & Sun Alliance, and many others. His skills and know-how encompass risk management, compliance, business continuity, application security, computer forensics, and penetration testing. He is well-versed with international standards such as COBIT, ISO 27001, PCI DSS, BS 25999, and ITIL / ISO 20000. He is the author of two books (Linux Security And Controls by ISACA, and Metasploit Framework, by Syngress Publishing), and of numerous articles on information security. He has also presented at conferences such as OWASP, Blackhat, Interop, IT Underground and others.

Wong Onn Chee

*Chief Technology Officer
Resolvo Systems, Singapore*

Onn Chee is currently working as the Chief Technology Officer in Resolvo Systems, a leading information leakage expert in Asia. He has led numerous large-scale projects, primarily in the government and defence sectors. His areas of expertise include information leakage protection, web security and security strategy. Onn Chee is a founding member and the first Vice-President of the Information Systems Security Association (ISSA), Singapore Chapter, the largest international, not-for-profit association for security professionals. He was also a former member of the Center of Internet Security (US) which provides well-recognised security benchmarks for various systems which are commonly used by US Federal Government and private organisations. Onn Chee is also the current Singapore chapter lead of Open Web Application Security Project (OWASP) which publishes the widely respected OWASP Top 10 web vulnerabilities. Other than being a information security professional, Onn Chee is also trained in BS 7799/ISO 17799, ISO 9000 and ITIL. He is also a certified Project Management Professional (PMP) and certified PRINCE2 Practitioner. In 2007, Onn Chee was appointed as the President of International Association of Software Architect (IASA), Singapore Chapter.

Lt. Col. (Rtd) Sazali bin Sukardi

*Head, Strategic Policy & Research
Cyber Security, Malaysia*

Lt Col Sazali bin Sukardi is the Head of Strategic Policy & Research Department, CyberSecurity Malaysia, an agency under the Ministry of Science, Technology and Innovation, Malaysia (MOSTI). He holds Master of Science in Information Security from Royal Holloway, University of London, Master of Arts in Defence Studies from King's College, University of London, Post Graduate Diploma in System Analysis from Universiti Teknologi MARA (UiTM), and Bachelor of Science in Civil Engineering from University of Hartford, Connecticut, USA. He has more than 20 years experiences in the Malaysian Armed Forces mainly in the research and evaluation works involving military technologies. He joined CyberSecurity Malaysia in April 2009, and his current post deals with strategic policy research. He is the committee member of Strategic Planning Committee of the London Action Plan – European Union Contact Network for Spam Authorities, an official network under the European Commission. He was also a visiting lecturer in information security at the Universiti Teknologi Malaysia in 2009.

Antony Ma

*Chairman
Professional Information Security Association, Hong Kong*

Antony Ma is currently the CTO in a financial information provider. He has over 9 years experience in the banking industry and taking the roles in different areas including software development, IT auditing and IT security. Antony has the qualifications of CISSP, CISA, Oracle DBA and BS7799 assessor and also completed Master of Law in Technology and Intellectual Property Law. Antony was the Vice-Chairperson (External Affairs) in the term 2006-2007, Program Director in the term 2008-2009 and he is now serving as the Chairperson of Professional Information Security Association. He is a keen writer focusing his interest in IT related risk and Security.

Asia Data Security Forum

Strategies to prevent Data Loss and Information Theft
Tuesday, 4th May 2010, Parkroyal Kuala Lumpur, Malaysia

+603 4270 3331

8:30 am Registration

9:00 am Welcome remarks from the chairman

Nigel Phair
Australian Graduate School of Policing
Charles Sturt University, Australia

9:15 am

Measuring Overall Effectiveness of Data Security System Convincing Management of ROI

- Developing metrics to measure effectiveness of security program
- Implementing metrics that reflects process and policy effectiveness
- Developing event logs to extract information

Antony Ma
Chairman
Professional Information Security Association,
Hong Kong

Workshop

Developing an effective and efficient plan to address the risk of data loss with focus on countering identity theft.

Many Governments are placing an increasing onus of responsibility on corporations to protect their customers from becoming victims of fraud and other crime. Consumers are overwhelmingly concerned about fraud and demand assurance that their personal information is protected to a high standard, Corporations must take significant action to protect their enterprise – and consequently their brand. This issue has become a business winner – or loser!

This workshop session will be interactive with delegate participation. This program is presented in non technical terms in an easy to understand format. Frontline employees, managers and supervisors will all benefit. Key areas of focus in this program will include:

10:00 am

Identity Theft Security

Understand the extent of the problem, its impact on employees, customers and business partners - and how to protect them

Identity theft facilitates crime – and identity fraud has become the primary concern for corporations who rely on e-transactions with their customer base.

- Find out what makes your business at risk
- Understand the data assets that are at particular risk and the ways in which your business and customer base may be attacked
- Learn how to protect your business from being victimized

10.45 am Morning refreshments / Network Break

11.00 am

Building an Appropriate Risk-Control Regime

Understand the features of an effective protective system

Whilst all businesses must deal with information and privacy protection, excessive and unwarranted defensive measures can also inhibit business achievement.

- There are a number of business drivers to be considered, including legal and regulatory influences
- Risks from internal sources are a key consideration
- Consequently, businesses should take an informed 'risk-based' approach and apply a formal and disciplined system of protective controls that enable the business objectives to be achieved
- The risk profile will change over time and so the control regime must be agile to maintain effectiveness
- Understand the approach to building an appropriate protective regime for your business environment

1.00 pm

Lunch Break

2.00 pm

Enabling your 'Guardians'

Building competency in your people

Companies are increasingly accountable for the actions and failures of individual employees. Whilst enterprise technical controls are an essential part of your defensive armoury, your people are the principal 'guardians' of your business.

- Skills and competencies that you should develop in your employees, at various seniority levels and roles, across your enterprise

3.40 pm

Afternoon refreshments / Network Break

3.55 pm

Countering Threats

- Methodologies to reduce the likelihood of an attack succeeding or a vulnerability being exploited



Workshop Leader

Roderick MacKinnon
Principle Consultant
Griffin Security Group, United Kingdom

Q & A Session

5.00 pm

End of Conference

After the conference, you would be able to:

- **Know** and develop new ideas to implement at work place for data security related issues
- **Develop** a security program in order to protect customer data and prevent loss of reputation arising from information theft
- **Use** technology more smartly and creatively than merely just implementing as current practice of security solution
- **Implement** new security management principles for data privacy and business continuity
- **Solve** mysteries in thefts while identifying and detecting stolen data with efficiency in the system
- **Enforce** security policies effectively in given time frame
- **Formulate** strategies and develop a sound fool proof data security governance system