Featuring an Unprecedented Interactive Conference Format to Help You Unlock the Content That You Cannot Access Anywhere Else

3rd ANNUAL Cyber Security for Government Asia

LESS PowerPoint Presentations, MORE Speaker-Delegate Interaction!

Implementing Effective Cyber Security Programmes for the Public Sector, Combating and Stay Ahead of Increasing Threats

Main Conference: 29 & 30 January, 2013 ■ Post Conference Workshops: 31 January, 2013 ■ Venue: Prince Hotel and Residences, Kuala Lumpur, Malaysia

Hear Leading Insights from 16+ International and Regional Government Officials Including:

Dr. Du Yuejin
Deputy CTO National Computer Emergency Response Team and Coordination Centre (CNCERT/CC), **CHINESE GOVERNMENT**

Naeem Musa
Chief Information Security Officer
Federal Energy Regulatory Commission,
US GOVERNMENT

Kim Andreasson
Managing Director
DAKA advisory

Dr. Solahuddin bin Shamsuddin
Vice President
CYBER SECURITY MALAYSIA, MINISTRY OF SCIENCE, TECHNOLOGY AND INNOVATION

Alan Cabanlong
Head of Cyber Security
INFORMATION AND COMMUNICATIONS TECHNOLOGY OFFICE (ICTO), THE PHILIPPINES

Jim Zabala
Assistant Commissioner, IQPS
INFORMATION PLANNING AND QUALITY SERVICE, THE PHILIPPINES

Yudhistira Nugraha
Head of Information Management and Risk Directorate of Information Security
MINISTRY OF INFORMATION, TECHNOLOGY AND COMMUNICATION, INDONESIA

Dang Hai Son
Regional Director
VNCERT, VIETNAM MINISTRY OF INFORMATION AND COMMUNICATION

and many more!

120+ senior government IT officers have come together over the last two years to discuss the biggest challenges and strategies to enhance cyber security for the public sector in the Asia Pacific region. Join CIOs, CISOs and senior IT Security officers for the 3rd Annual meeting and receive:

An Unprecedented Interactive Format: G-5 Panel Discussions, One-on-One Live Keynote Speaker Interviews CIO Spotlights, Video Conferencing Session; **We aim to get rid of the 'death by PowerPoint' format** often seen in all conferences and instead provide truly innovative content

- **Brand New and Vastly Improved Speaker Line up:** Hear from **CIOs and CISOs** from leading international and regional governments such as **Australia, USA and China** to learn best practices and strategies.
- **Achieve and Unlock the Vital 10% of Content You Can't Access Anywhere Else to:** 90% of the content discussed in conferences can be accessed online. Get this inaccessible 10% now, through our interactive discussions as we ask our keynote speakers honest brutal questions regarding cyber security programmes.
- **Interact and network** with both **international and regional senior government IT officials** and key decision makers from over **10 countries** in a personal and business-conducive environment.

PLUS! Don't Miss out On Our Expert-Led, Post Conference Workshops:

WORKSHOP A:
Developing and Implementing an Effective and Robust Cyber Security Framework to Overcome Cyber Threats
Facilitator: Dr. Du Yuejin, Deputy CTO, National Computer Emergency Response Team and Coordination Centre of China (CNCERT/CC), **CHINESE GOVERNMENT**

WORKSHOP B:
Implementing Effective Staff Training and Awareness Strategies to Protect Data and Critical Infrastructure
Facilitator: Naeem Musa, Chief Information, Security Officer, Federal Energy Regulatory Commission, **US GOVERNMENT**

WORKSHOP C:
Enhancing Cyber Security through a Citizen-Centric Approach for Governments
Workshop Facilitator: Lyle Wray, Executive Director, **CAPITOL REGION COUNCIL OF GOVERNMENTS, US GOVERNMENT**

Researched and developed by:
Government iQ a division of IQPC
IQPC International Quality & Productivity Centre

"I look forward to meeting you at the 3rd Annual Cyber Security for Government Asia 2013 conference to have a fruitful discussion and equip yourself with the necessary skills to secure your organisation from increasing cyber threats."
Kim Andreasson
Managing Director, ***DAKA Advisory***

T: **+65 6722 9388** ■ F: **+65 6720 3804** ■ E: **enquiry@iqpc.com.sg** ■ W: **www.cybersecurityasia.com**

Dear Cyber Security Professional,

The rapid development of the ICT industry supported by various innovation-based approaches has also led to the increase in sophistication and range of cyber-attacks. As a result, Asian governments are playing an increasingly active role in developing a more comprehensive, holistic and sustainable form of defence to combat cyber-crime.

The **3rd Annual Cyber Security for Government Asia 2013** conference will, for the first time not only bring together regional CIOs, CISOs and IT Security Directors in the public sector, but go far beyond its shores to engage internationally recognised and leading best practice experiences from the USA and Europe. The conference will once again bring together the cyber security community and provide the perfect platform for CIOs, CISOs, Heads of IT Security, ICT Directors, senior government IT officers and industry stakeholders to share strategies and provide exclusive case studies on how to implement cyber security strategies for public organisations and enhance cyber security for the public sector.

With a brand new unprecedented format including a G5 Panel Discussion, Live One-on-One Speaker Interviews, C-Level and Government/Industry Debates, you will gain access to previously inaccessible content that you have always wanted.

Yours sincerely,

Kim Andreasson
Managing Director
DAKA Advisory

Who Will Be Attending Cyber Security for Government Asia 2013?

- CIO - Chief Information Officer
- CTO - Chief Technology Officer
- CISO - Chief Information Security Officer
- CSO - Chief Security Officer
- CRO - Chief Risk Officer
- Enterprise Security Director
- Executive Manager Security and Safety
- Director Enterprise Architect solutions
- ICT Strategies & Infrastructure Manager
- IT Security Manager
- ICT Centre Director/Manager
- Manager of Fraud & Intelligence
- Service Network Director Manager
- Data Centre Security Manager
- Disaster Recovery Manager
- Cyber Safety Manager
- Group Manager identity Solutions
- Executive Manager Information & Technology Services
- Director e-Security projects
- Director ICT Services
- Intrusion Manager/Director
- Head of Information Security Operations
- Enterprise Security Engineer
- Executive Manager Enterprise Infrastructure
- National Manager Data Services
- General Manager Security & Compliance Manager
- Infrastructure Support & IT Security Director/Manager

Media Partners:

How Will You Benefit From Attending Cyber Security for Government Asia 2013?

Less PowerPoint Presentations! Let's face it: everyone is tired of power point presentations. We learn less, and the same information can be found online. With our new interactive format at Cyber Security 2013, we will guarantee that you will:

- **Get your key questions answered:** With our brand new interactive polling system, we will help you **find the answers to key questions pertaining to cyber security and threats** that we will pose to our distinguished speakers
- Obtain leading industry insights from international and regional CIOs and IT Security Directors in our unprecedented **G5 Panel Discussion to empower and secure your organisation**
- Learn the best practices in **governing, managing and implementing effective strategies to enhance cyber security** through our 1-on-1 live speaker interviews with Dr. Du Yuejin, Deputy CTO, CNCERT, China and Naeem Musa, CISO, FERC
- **Obtain previously inaccessible information** from our CIO debates, country spotlights and interactive panel discussions from leading government officials in the USA, the Philippines, Indonesia, Vietnam, China and more
- Analyse the latest **National IT security strategies** and **how to successfully implement them** to mitigate cyber threats for government
- Overcome and combat the latest cyber threats through **effective CERT and integrated security programmes**
- **Utilise these excellent opportunities to penetrate** into the fast evolving Asia Pacific market

Cyber Security for Government Asia 2013 will feature senior government IT officials from all over the world, including

- Malaysia
- Singapore
- USA
- UK
- China
- Laos
- Indonesia
- Philippines
- Australia
- Thailand
- South Korea

"This is the premier conference in Asia that showcases ICT security and how to build a resilient cyber security strategy."

Shankar Aggarwal
Additional Secretary - Department of Information Security
Ministry of Communications & Information Technology, Government of India

3rd ANNUAL
Cyber Security for Government Asia

▸▸ LESS PowerPoint, MORE Interactive Discussions!

Workshop A: (0900 to 1100)

Developing and Implementing an Effective and Robust Cyber Security Framework to Overcome Cyber Threats

Rationale:
As cyber-attacks becoming increasingly prevalent and sophisticated, an effective and comprehensive framework must be developed and implemented to encompass and manage these threats and challenges. This workshop will cover various aspects of what should be included when developing such a framework, covering various criteria that must be considered, including: infrastructure, architecture, security technology and networks, protocol and management as well as personnel training.

Benefits of Attending:
- Learn how to effective develop and implement a comprehensive cyber security framework for your organisation to enhance security against cyber threats and attacks
- Analyse how an integrated approach to cyber security is crucial for preventing and responding to cyber attacks
- Overcome the challenges in implementing your security framework within your orgnaisation
- Learn from an unprecedented operational case study involving the CNCERT/CC and understand how the Chinese government is employing effective cyber security strategies to overcome internet and online threats

Workshop Facilitator:

Dr. Du Yuejin
Deputy CTO
National Computer Emergency Response Team and Coordination Centre of China (CNCERT/CC)

Dr. Du Yuejin is currently serving as deputy CTO of the national computer emergency response team and coordination center of China (CNCERT/CC), and director of NINIS, National Institute of Network and Information Security. He has more than 10 years of experience on Internet security, involved in the handling work of nearly all the large scale Internet incidents during 2001to 2008. Dr. Du has played a key role in setting up the Chinese National Incident Response Framework and is the leading figure in China to discuss effective policies to combat cyber attacks in the world's largest volume of targeted attacks.

Workshop B: (1300 to 1500)

Implementing Effective Staff Training and Awareness Strategies to Protect Data and Critical Infrastructure

Rationale:
In today's environment, there is only so much technology can do to combat against cyber attacks and threats. Ultimately, government officials and staff are the final and most valuable asset in protecting critical data and infrastructure within your organisation. Ensuring your staff is aware of all risks and threats is imperative to maximise the effectiveness of your cyber security framework against cyber threats. This workshop will equip you with the necessary skills and training strategies to ensure how to raise your staff's awareness of the most recent threats and how to implement these strategies into your organisation.

Benefits of Attending:
- Develop effective training programmes and ensuring the implementation and compliance within your organisation
- Analyse the best practices and training methods to empower your staff to deal with cyber threats
- Operational case studies of how to conduct effective training exercises to provide your staff with the relevant experience to handle real cyber attacks
- Finding the right equilibrium between technology and human expertise in enhancing cyber security

Workshop Facilitator:

Naeem Musa
Chief Information Security Officer
Federal Energy Regulatory Commission, **US Government**

Mr. Musa has over 20 years of experience in the Information Technology, Information Assurance and Systems Engineering fields. Mr. Musa currently serves as the Chief Information Security Officer (CISO) at the Federal Energy Regulatory Commission. Prior to that Mr. served as an independent consultant for the Department of Homeland Security in the area of Border Security. He previously served as the Head of IT for Organizational Strategies Inc. Mr. Musa supported various large scale programs with commercial and government clients.

Workshop C: (1530 to 1730)

Enhancing Cyber Security through a Citizen-Centric Approach for Governments

Rationale:
Cyber security policies are often driven by the top and left to filter down accordingly to the various government agencies and departments. Is there a more effective way of enhancing cyber security for the public sector? How do you motivate personnel and even your citizens at the ground level? This workshop will provide an alternative angle to cyber security, by adopting a citizen-centric, bottom-up approach. The workshop will equip with you the necessary skills and strategies to implement a citizen-centric approach to cyber security, while providing insightful case studies from the US government on how they have been effective.

Benefits of Attending:
- Understand and learn new, alternate approaches to cyber security for the public sector by engaging your citizens more effectively
- Ensuring that a stronger foundation is put in place by a bottom-up approach, while at the same time integrating top-down policies to strengthen overall cyber security
- Operational case study of the US government to analyse the effectiveness and utility of a citizen-centric approach to cyber security
- Reviewing and achieving tangible action steps to move towards a citizen centric approach to enhance cyber security

Workshop Facilitator:

Lyle Wray
Executive Director
Capitol Region Council Of Governments, US Government

Since 2004 Dr. Wray has served as executive director of the Capitol Region Council of Governments. In this role, Dr. Wray serves as chief executive for this regional planning organization for Hartford, Connecticut and the 28 surrounding towns in transportation, community development, public safety and homeland security. Dr. Wray is also a subject on citizen-centric governance and information security and is the ideal candidate to approach this new and innovative approach to enhance cyber security for the public sector.

0830 **Registration & Welcome Coffee**

0900 **Welcome Address by Chairman**

Kim Andersson
Managing Director, **DAKA advisory**

0910 **Morning Keynote Presentations:**
Analysing Cyber Security in Malaysia: Integrating Inter Agency Efforts Effectively to Enhance Cyber Security

- Overview of Cyber Security Malaysia and its role for the Malaysian Government
- Case Study of integration efforts between government agencies in Malaysia: How does this promote cyber security?
- Highlighting the importance of public-private partnerships in enhancing cyber security efforts for government
- Reviewing the future of cyber security initiatives for the Malaysian government

Dr. Solahudin bin Shamsuddi
Vice President, Cyber Security Malaysia
Ministry Of Science, Technology And Innovation, Malaysia

0950 **CISO Perspective: Enhancing Cyber Security at the US Federal Energy Regulatory Commission: Effective Policy Planning, Implementation and Execution Strategies**

- Discussing the sophisticated nature of cyber attacks on the US Federal Regulatory Commission: Evolving Your Strategies to combat these threats
- Analysing the ongoing strategies and developments at the US FERC to overcome these threats
- Highlighting the importance of efficient implementation and execution processes to ensure maximum security

Naeem Musa
CISO, **Federal Energy Regulatory Commission, US Government**

1030 **Special Polling and Voting Session**
In preparation for our G5 panel, we invite our delegates to poll and vote on a series of trending topics and questions for our panel debate; in which we will answer the questions that YOU want answered from these leading government officials. Using special touch pads, vote for the questions that you want asked and our Chairman will collate the responses and direct these specially prepared questions to our G5 leaders in the panel after the tea break. Put your thinking cap on, because this is your moment to maximise your learning experience at our conference.

1050 **Morning Refreshments and Networking**

1110 **G5 Panel: Discussing Cyber Security for Government in Asia Pacific: The Hard Facts**
The G5 Panel comprises of 5 leading individuals from leading international and regional government agencies, who will be debating—live – the evolving trends and tools in cyber security that are shaping the public sector today. No stone will be left unturned, as we uncover some of the hard facts and harsh realities of cyber threats, and the innovative strategies used to combat these threats within these countries. Moderated by our Chairman, difficult questions will be posed, and truthful insights will be provided in this engaging debate. In addition, delegates will be able to poll their questions through our brand new polling system before the G5 debate begins and contribute to this debate.

G5 experts:
Naeem Musa
CISO, **Federal Energy Regulatory Commission, US Government**

Dr. Solahudin Shamsuddin
Vice President, Cyber Security Malaysia,
Ministry Of Science, Technology And Innovation, Malaysia

Dr. Du Yuejin
Deputy CTO, **CNCERT/CC, China**

Bambang Heru
Director General, Information Security,
Ministry of Communication and Information Technology, Indonesia

Alan Cabanlong
Head of Cyber Security, **Information and Communications Technology Office, Philippines**

1150 **Spotlight on C-Level Government Speaker Interviews:**
90% of the content found in conferences can be accessed online, here we bring you the 10% that cannot be found anywhere else. In these exclusive 1-on-1 live speaker interviews, we bring you the honest, insightful perspectives of two C-level government officers—the 10% of information that you CANNOT get anywhere else.

Keynote Interview with Naeem Musa
CISO, **Federal Energy Regulatory Commission, US Government**

1210 **Keynote Interview with Dr. Du Yuejin**
Deputy CTO, **National Computer Emergency Response Team and Coordination Centre of China (CNCERT/CC), Chinese Government**

1230 **Networking Lunch**

1330 **SOUTHEAST ASIA FOCUS SESSION**
Southeast Asian Perspectives on Cyber Security: Real Challenges and Practical Strategies:
You've heard from the International Keynotes, now hear the Southeast Asian perspective on cyber security and the measures that governments have been using to enhance protection. This session series is designed to give you the regional perspectives that are essential for you. After each session, there will be 5-10 timeframe for you to submit your questions and key comments to our Chairman, which he will bring them up during the SEA Focussed Discussion.

Analysing the Philippines' Government's Cyber Security Strategy: Improving Cyber Security Standards

- Analysing the ICTO's role in spearheading government efforts on cybercrime and cyber security
- Identifying the challenges and opportunities for a national cyber security framework development in the Philippines
- Analysing the latest cyber security attacks on government websites: Case study of recent hacktivist attacks
- Addressing and combating against cyber security threats: Evaluating the measures that have been taken to overcome these threats

Alan Cabanlong
Head of Cyber Security, **Information And Communications Technology Office, Philippines**

1400 Case Study:
Managing High-Volume Cyber Attacks Through Effective Strategies in Indonesia

- Providing an overview of the high number of cyber attacks on the Indonesian government
- Outlining the main challenges in dealing with cyber attacks: Lack of a coherent national guideline and cyber security programme
- Analysing the strategies employed to manage and overcome these cyber threats
- Highlighting the importance of international collaboration in mitigating cyber attacks in Indonesia

Yudhistira Nugraha
Head of Risk Management Section, Directorate of Information Security, **Ministry Of Communication And Information Technology, Indonesia**

Conference Day One
Tuesday, 29 January 2013

3rd ANNUAL Cyber Security for Government Asia

1430 **Case Study:**

Combatting Internet Attacks in Laos: Imperatives of the Laos National Internet Centre

This session focuses on the challenges that Laotian government; with a rapidly developing ICT industry and implementation, how does the recently established Laos National Internet Centre deal with increasing cyber attacks on government websites and intellectual property? This session is essential in providing cost-effective and applicable strategies to overcome internet attacks and to secure government websites from hacktivists.

Phavanhna Douamaboupha
Director, **Laos National Internet Centre**

1500 **Afternoon Tea and Networking Session**

1530 **Enhancing Cyber Security for Southeast Asia: Developments and Future Roadmaps for The Philippines, Indonesia and Laos**

Join in the debate as questions and comparisons will be made based on the 3 earlier presentations. What are some of the security challenges that these 3 rapidly developing countries are facing? What best practices and strategies can be utilised? How can countries in Southeast Asia learn from each other? Moreover, you've heard their presentations and submitted your questions, now hear from our SEA discussion leaders themselves.

SEA Discussion Leaders:
Alan Cabanlong
Head of Cyber Security, **Information And Communications Technology Office, Philippines**

Yudhistira Nugraha
Head of Information Management and Risk, **Ministry Of Communication And Information Technology, Indonesia**

Phavanhna Douamaboupha
Director, **Laos National Internet Centre**

1550 **Panel Discussion:**

Hear from Our Hosts: Spotlight on Malaysia

The Malaysian Government has recently been stepping up its efforts in promoting and enhancing cyber security for its government agencies and ministries. Understand what these policies actually entail from various ministries in Malaysia how they have been faring thus far

- Analysing cyber-attacks at various government agencies and departments: What are the current and latest threats and what are some of the solutions to overcome them?
- Human Expertise vs Technology: Is there a right blend? How do you achieve the right blend?
- Analysing the ISMS guidelines for the Malaysian government: How effective has it been so far?
- Highlighting the importance of interagency collaboration between various ministries and agencies in Malaysia

Malaysian Experts:
Dr. Mingu Jumaan
Director, State Computer Services, **Sabah State Government**

Yazid Ahmad
Senior IT Officer, **Inland Revenue Board Of Malaysia**

Dato Husin Jazri
Former CEO, **Cyber Security Malaysia**

1630 **Closing Address by Chairman**

1640 **End of Conference Day One**

Conference Day Two
Wednesday, 30 January 2013

3rd ANNUAL Cyber Security for Government Asia

0830 **Registration & Welcome Coffee**

0900 **Welcome Address by Chairman**
Kim Andersson
Managing Director, **DAKA advisory**

0910 **Morning Keynote Presentations:**
Analysing the United Nations Approach to Cyber Security: Benefits of Collaborative Inter-Agency Efforts to Enhance Cyber Security

- Highlighting the current cyber security efforts by the United Nations
- Analysing the ongoing strategies and developments at the United Nations: Challenges involved and how they can be overcome
- Providing practical case studies on collaborative inter-agency efforts to enhance cyber security
- Reviewing current projects and future trends in cyber security for the public sector

Kim Andersson
Managing Director, **DAKA advisory**

0950 **Technology Debate: Minimal Solutions vs. Comprehensive Packages**

This debate focuses on the biggest challenge to adopting and implementing the latest security solutions in Asian governments: Cost-effectiveness and the justification of its return of investment. Budgets will always be a constraining factor when it comes to choosing and selecting the best security solution for government; However, is a minimalist solution always the right answer? What are the justifications for investing in a comprehensive security package? This debate will bring together leading Asian government officials and pit them against IT security solution providers as they engage in an honest and insightful debate on security solutions and cost implications on procurement processes.

Dr. Du Yuejin
Deputy CTO
National Computer Emergency Response Team and Coordination Centre of China (CNCERT/CC)
People's Republic of China Dang Hai Son,
Regional Director, Vietnam Computer Emergency Response Team
Ministry of Information and Communications, Vietnam

Spot Reserved for Industry

Spot Reserved for Industry

Spot Reserved for Industry

1030 **Exclusive Video Conference: Mitigating Cyber Threats at the Department of Transport: A CIO's Perspective**

As the former CIO of the US Department of Transport, Nitin will share his perspectives on managing and mitigating cyber threats in the US government; and the strategies that he implemented to ensure that the organisation's services and policies ran smoothly. Nitin will also share the tips and tricks on leading a federal organisation, ensuring that the information technology vision, strategy, planning and policies were implemented securely and smoothly.

Nitin Pradhan
Former CIO, **US Department Of Transport**

1100 **Morning Refreshments and Networking**

1130

China and Vietnam Spotlights:
China and Vietnam are two countries that have recently come under the highest number of cyber-attacks. Yet not much is known about these governments' efforts to combat and manage these threats. In this exclusive country spotlights, hear from leading Directors on how they have implemented strategies to manage high volume and sophisticated cyber attacks

Overcoming Cyber Threats in China: Trojans, Botnets, Viruses, Web Defacement and Phising

- Providing an update on security statistics in China: How significant are cyber threats to the Chinese government?
- Highlighting the increasing quantity and sophistication of cyber attacks in China: Does the government have the available tools to combat these threats?
- Analysing the ongoing strategies and developments used to overcome these threats
- Emphasising the need for international collaboration and cooperation to enhance cyber security

Dr. Du Yuejin
Deputy CTO, National Computer Emergency Response Team and Coordination Centre of China (CNCERT/CC), **Chinese Government**

1200

Vietnam's CERT Strategy to Mitigate Cyber-Intrusion

- Defining the technical, socio-cultural, legal and institutional criteria for a cyber-identity management system
- Addressing the challenges of identification, authentication and access
- Managing and responding effectively to cyber attacks in Vietnam
- Highlighting an operational case study of the VNCERT in mitigating cyber-attacks

Dang Hai Son
Regional Director, Vietnam Computer Emergency Response Team, **Ministry Of Information and Communications, Vietnam**

1220

China and Vietnam Spotlight Roundtable Discussions
We invite Dr. Du and Mr. Dang back for roundtable discussions, where our delegates can ask them questions regarding their presentations and find out more how China and Vietnam have coped with cyber attacks and cyber threats. Do not miss this exclusive opportunity to have an informal but open discussion.

1320

Lunch and Networking Break

1400

Case Study:

Enhancing HMI Security at MINDEF Malaysia

- Highlighting the importance of cyber security for the Ministry of Defence
- Examining the main source of security lapses: Human Machine Interface
- Analysing the strategies used to enhance the HMI process: Training, building awareness and conducting regular checks
- Analysing the latest technologies at MINDEF to enhance cyber security for defence organisations

First Admiral Mohd. Haji Maidin Saha
Director of Cyber Defence, **MALAYSIA MINDEF**

C-Level Debate:

The Role of the C-level Executive in Enhancing Security for the Public Sector
This session will be dedicated to our C-level officers from Malaysia, China and USA in which they talk shop regarding the changing role of the C-level executive in driving and enhancing cyber security for the public sector. Requirements, technology, setting strategy, policies, effective implementation, cost-savings; these are the issues that our C-level experts will address in this session. Other discussion topics will include:

- How important is cyber security for the CIO?
- Challenges in implementing security programmes and procedures in the government
- Examining the strategies and best practices in leading change and implementing guidelines to enhance cyber security

C-Level Debate Experts:
First Admiral Mohd. Haji Maidin Saha
Director of Cyber Defence, **Ministry of Defence, Malaysia**

Naeem Musa
CISO, Federal Energy Regulatory Commission, **US Government**

Dr. Du Yuejin
Deputy CTO, National Computer Emergency Response Team and Coordination Centre of China (CNCERT/CC), **People's Republic of China**

1500

Afternoon Tea Break and Networking Session

1540

Case Study:

Managing the Increased Security Threats of Web 2.0 in the Philippines

- Addressing new challenges faced by policy makers and cyber security organisations to guard against malicious threats from Web 2.0
- Outlining the real cyber threats from Web 2.0: How have they impacted the Philippine government?
- Analysing the strategies for using and assessing Web 2.0 sites: Developing safety protocols and effective emergency response teams
- Reviewing the current state of cyber security in the Philippines: What can be improved?

Jaime Zabala
Assistant Commissioner, Information Planning and Quality Service, **Bureau Of Internal Revenue, Philippines**

1620

Bottom-Up Approach of Cyber Security for Government: Enhancing Cyber Security from a Citizen-Centric Approach
Most government cyber security programmes are driven by the top, and slowly filtered down all the way to various departments, agencies and then to its citizens. Taking it from an alternate angle, Lyle will revisit this model, and share his experiences from the bottom up: Cyber security can be most effective when a citizen-centric approach. Lyle will discuss his experience with citizen-centric cyber security initiatives as the Executive Director of the Capitol Region Council of Governments for the US government, and how if cultivated, can enhance overall security from increasing threats.

Lyle Wray
Executive Director, **Capitol Region Council Of Governments, US Government**

1630

Closing Remarks by Chairman

1640

End of Conference

Praise for our Cyber Security Asia Series

"I benefitted from the experiences and expertise of speakers on technology trends and the role of a government sector preparing in a cyber security area. I built a great connected network between the government sector and private sector."

Lt Col Apichart Aphichanont
Deputy Superintendent
Technology Crime Suppression Division, Thailand

Dr. Du Yuejin
Deputy CTO, National Computer Emergency Response Team and Coordination Centre of China (CNCERT/CC), **CHINESE GOVERNMENT**

Dr. Du Yuejin is currently serving as deputy CTO of the National Computer Emergency Response team and Coordination Center of China (CNCERT/CC), and director of NINIS, National Institute of Network and Information Security. Dr. Du has more than 10 years of experience on Internet security, involved in the handling work of nearly all the large scale Internet incidents during 2001to 2008. Dr. Du contributed a lot on national Internet security capacity building, leaded the project of national Internet intrusion monitoring and warning platform, played key role on setting up national incident response cooperation framework, did a lot of work on public-awareness-raising, etc. Dr. Du was one of the several top level network security experts during many important event, include the Olympic Games in 2008, the World Expo and the Asian Games in 2010, and the Summer Universiade in 2011. Dr. Du earned many very high level awards because of his contributions. Dr. Du also played an active role on international cooperation. He proposed the China-ASEAN cooperation framework on network security, leaded an APEC-TEL project on botnet countermeasure, made many presentations on various international conferences. Dr. Du worked as deputy chair of APCERT.

Dr. Solahudin bin Shamsuddin
Vice President, Cyber Security Malaysia, **MINISTRY OF SCIENCE, TECHNOLOGY AND INNOVATION, MALAYSIA**

Dr. Solahuddin is the current VP of Research at Cyber Security Malaysia. He received his PhD from University of Bradford, United Kingdom in Network Security. He received a post-graduate Diploma in Systems Analysis from UiTM, Malaysia in 1991. He started his career with the Malaysian Armed Forces after completing his first degree in Electrical Engineering from Wichita State University, USA in 1986. He served in the Royal Signal Regiment of the Malaysian Army for 10 years holding various posts such as communications engineer and IT manager before joining the industry after the completion of his stint with the Malaysian Armed Forces.

In 1997 he joined Softlabs Technologies Sdn Bhd as the General Manager. He was entrusted to manage and lead system development projects with various industries such as oil and gas, defence, telecommunications and local governments.

In 2002 he joined National ICT Security & Emergency Response Centre (NISER) now known as CyberSecurity Malaysia as the Expert Service Manager. Later on, he was entrusted to be the manager for Malaysia Emergency Response Team (MyCERT). He has earned 4 professional certifications namely CWNA, CISSP, CEH and ISMS Lead Auditor.

Jaime Zabala
Assistant Commissioner, Information Planning and Quality Service, **BUREAU OF INTERNAL REVENUE, PHILIPPINES**

Jaime is an IT and telecom industry veteran with more than 20 years of experience, a Professional Electronics and Communications Engineer (PECE) from the University of the City of Manila with a post graduate degree in management. He is currently the Assistant Commissioner and Head Revenue Executive Assistant of Information Planning and Quality Service, responsible for the ICT planning, standards development, security management, technology management and quality assurance. Jaime is currently managing major outsourcing off- premise core ICT systems operations and sustainability project as well as being the Head of the BIR Information Security Technical Working Group.

Kim Andreasson
Managing Director
DAKA advisory

Mr. Kim Andreasson has advised the United Nations since 2003, most recently in preparation for a cyber security policy framework, and is a Managing Director of DAKA advisory AB, a consultancy. He is regularly giving presentations around the world on cyber issues. Previously, Kim was an interim Associate Director and a Senior Editor at The Economist Group's Business Research division where he co-edited the annual report on the Digital Economy Rankings. He serves on the editorial board of the Journal of Information Technology and Politics and is an elected member of the International Institute of Strategic Studies and the Pacific Council of International Policy and is a John C. Whitehead Fellow at the Foreign Policy Association. His book, Cybersecurity: Public Sector Threats and Responses, was published in December 2011.

Yudhistira Nugraha
Head of Risk Management Section, Directorate of Information Security, **MINISTRY OF COMMUNICATION AND INFORMATION TECHNOLOGY, INDONESIA**

Yudhistira Nugraha is a Head of Risk Management Section, Directorate of Information Security, the Ministry of Communications and Information Technology of Republic of Indonesia since March 2011. He graduated from Telecommunication Engineering of Telkom Institute of Technology (IT Telkom) in 2003. After completing his undergraduate education, he worked as a Radio Access Network Engineer at many Telecommunication vendor and operator in Indonesia before joining the Ministry of Communication and Information Technology (MCIT) in 2006. His Master of Information and Communication Technology Advanced, in the field of Information Technology Strategic Planning, was awarded with Distinction by University of Wollongong in July 2009. His expertise includes 3 years as policy and regulatory research staff at the Post and Telecommunication Research and Development Center as well as an assessor for Implementation of Information Security Governance regarding ISO 27001.

Phavanhna Douamaboupha
Director, **LAOS NATIONAL INTERNET CENTRE**

Phavanhna is currently the Head of the Laos National Internet Centre. Previously she was working as the Acting Director of Database and Information division, E-Government Center, Ministry of Posts and Telecommunications, Laos. She was also recently assigned to be responsible to coordinate with companies and organization concerned to include the Lao Language into existing and emerging products for Lao people in Laos and overseas. Phavanhna joined E-Government team since 2010 and before this she was working at Management and Promotion Division, the Department of Informatics of the National Authority of Science and Technology (and now it is known as Ministry of Science and Technology).

Lyle Wray
Executive Director, **CAPITOL REGION COUNCIL OF GOVERNMENTS, US GOVERNMENT**

Since 2004 Dr. Wray has served as executive director of the Capitol Region Council of Governments. In this role, Dr. Wray serves as chief executive for this regional planning organization for Hartford, Connecticut and the 28 surrounding towns in transportation, community development, public safety and homeland security. The metropolitan regional population is approximately one million. Initiatives include: region wide municipal service sharing projects, regional geographic information system, cooperative purchasing online system, and contributions to state and regional outcomes measurement systems in workforce development, education and training, transportation systems and economic development.

Dang Hai Son
Regional Director, Vietnam Computer Emergency Response Team, **MINISTRY OF INFORMATION AND COMMUNICATIONS, VIETNAM**

Dang Hai Son is currently in charge of VNCERT branch in central Vietnam. Assisting Vietnam organizations and Internet users in implementing proactive measures to reduce the risks of computer security incidents and to assist them in responding to such incidents when they occur. Regular coordination with the emergency response headquarters VNCERT handles incidents that originate in Vietnam networks and are reported by any Vietnam or foreign persons or institutions.

Naeem Musa
Chief Information Security Officer
Federal Energy Regulatory Commission,
US GOVERNMENT

Mr. Musa has over 20 years of experience in the Information Technology, Information Assurance and Systems Engineering fields. Mr. Musa currently serves as the Chief Information Security Officer (CISO) at the Federal Energy Regulatory Commission. Prior to that Mr. served as an independent consultant for the Department of Homeland Security in the area of Border Security. He previously served as the Head of IT for Organizational Strategies Inc. Mr. Musa supported various large scale programs with commercial and government clients.

Lt. Col. Dato' Husin Jazri (Retired)
Former CEO
CyberSecurity Malaysia

Lt. Col. Dato' Husin Jazri (Retired) is the Chief Executive Officer of CyberSecurity Malaysia, the Malaysian cyber security specialist centre under the purview of the Ministry of Science, Technology and Innovation Malaysia (MOSTI). Husin has been at the helm of CyberSecurity Malaysia since its inception, leading the organization's efforts to secure the nation's cyber space for the government, business, industry and society.

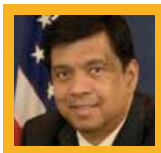
Husin has also stamped his mark at the overseas arena by leading the way in collaborative efforts and consultancy for cyber security initiatives abroad. Currently, he is the Chairperson of the Organisation of Islamic Conference Computer Emergency Response Team (OIC-CERT), the Chairman of the Malaysian Vocational Advisory Committee on ICT to the Ministry of Human Resources, and the Interim Chairman for both the Business Continuity Society Malaysia and Information Security Professional Society Malaysia. Husin is a retired serviceman from the Malaysian Armed Forces.

Throughout his career in the cyber security industry, Husin has received both domestic and international awards on numerous occasions for his exemplary leadership, innumerable contributions and outstanding achievements such as PIKOM ICT Personality of the Year 2010 from the National ICT Association of Malaysia, (ISC)2 Information Security Leadership Achievements (ISLA) Award 2009 for Exemplary Leadership and Dedication in Enhancing the IT Security Workforce as well as the Harold F. Tipton Lifetime Achievement Award 2010 and CSO ASEAN Award 2010.

Dr. Mingu Jumaan
Director, State Computer Services Department,
SABAH STATE GOVERNMENT

Dr. Mingu Jumaan is the Director of the Sabah State Computer Services Department. A member of the Malaysian National Computer Confederation. He also acts as State ICT Chief Security Officer, the Secretariat for the State Chief Information (CIO) and State Public Service ICT Security Working Committee. He is a member in a number of IT technical committees, such as a member of the State Inter-Agencies Planning Group for IT sector, Chairman of State Public Sector ICT Technical Committee and also Chairman of the Sabah State Government Computer Emergency Response Team (sgCERT). He has 30 years working experience in Information Technology.

Alan Cabanlong
Head of Cyber Security
Information and Communications Technology Office (Icto), The Philippines



Nitin Pradhan
Former CIO, **US Department of Transport**

Nitin Pradhan is the head of Public Private Innovations (PPI), the nation's first federal technology accelerator program and partner consortium focused on growing highly competitive federal contractors and technology suppliers that maximize public value from federal systems through private growth.

Prior to launching PPI, Nitin was an award winning, nationally recognized federal CIO for the US DOT where he provided information technology vision, strategy, planning, policy and oversight for DOT's more than $3.0 billion IT portfolio, the 6th largest in the federal government.

The CIO magazine honored Nitin and US DOT with CIO 100 award for the innovative approaches to use IT to reduce costs and increase efficiency and public value. Computer World Magazine also recently named Nitin to its Premier 100 life time recognition award where he joins an elite group of top US IT executives. Nitin has been on Information Week's "Government CIO 50: Driving Change in the Public Sector" for bringing a business person's point of view to management of the federal IT strategy, policy and implementation. Under his leadership, the DOT Office of CIO has also won awards from the White House, Information Week, AFFIRM, and the U.S. General Services Administration for leadership, innovation, open government, governance, service and culture.

Bambang Heru Tjahyono
Director General, Information Security,
Ministry of Communication and Information Technology, Indonesia

Bambang Heru Tjahjono is a Director of Information Security, Directorate General of Informatics Application, the Ministry of Communications and Information Technology of Republic of Indonesia. Before joining the Ministry of Communication and Information Technology (MCIT) on February 2011, He was a leading expert in digital broadcasting and digital electronic media policy with extensive experience in the evaluation of related technical standards and regulatory practices at Assessment and Application of Technology Agency.

First Admiral Mohd. Haji Maidin Saha
Director of Cyber Defence
Malaysia Mindef

Yazid Ahmad
Senior IT Security Officer
Inland Revenue Board of Malaysia

Interested in Sponsorship and Exhibition Opportunities?

Build and Develop Key Relationships with Senior Government Officials

Why Cyber Security for Government Asia 2013 gives YOU the best value for your marketing spend:

- **A complete exposure to key decision-makers** who are responsible for the procurement and operations of IT projects around the world: Meet these decision makers now at a time where contracts and tenders are going out for existing and new government IT projects across the Asia Pacific region
- **An intimate environment** for networking and knowledge sharing with **senior IT government officers** where you can discuss the potential of acquiring further business
- The perfect opportunity to **showcase your products or services**, forge strategic relationships with your potential clients and establish your brand in the industry: **Why go through your individual agents in various countries?** Attend Cyber Security for Government and pitch your product to an eager and personable audience

Cyber Security for Government Asia 2013 will gather CIOs, CISOs, Heads of IT Security, Heads of IT, Heads of Procurement, and Heads of Procurement Committees from various Ministries and Government Agencies, providing with you accessibility levels you cannot get anywhere else.

You'll have direct access to the in-depth profiles of leading senior IT officers and receive information on their budgets, operational objectives and purchasing and investment strategies. This is your opportunity to offer strategic guidance and help them and build a world-class cyber security strategy.

Take advantage of this opportunity to enjoy sponsor benefits:

- **Achieve thought leadership** by exhibiting in this event: showcase your expertise, superior products and services, and **impress your prospects**
- **Maximise your exposure** by leveraging on our marketing resources, including print advertisements, online advertisements, website, email campaigns to various legal personnel in Asia.
- **Optimise your influence:** chair the event– it is your opportunity to **influence the audience and position your organisation** as industry leader
- **Position yourself** a step forward from other vendors by hosting a networking lunch or drinks reception and discuss **business in an informal way**
- Tailored business development arrangements: target prospect invitation and pre-arranged meetings to **ensure you are meeting the right people** and developing the business **relationship you desire**
- **Enhance your credibility** through free live product demonstrations.

Sponsorship opportunities are deliberately limited. Call us today to explore how we can best leverage this platform to customise a package that achieves your business objectives. Get in touch at **+65 6722 9388** or email **sponsorship@iqpc.com.sg**

3rd ANNUAL Cyber Security for Government Asia

29 & 30 January 2013
Prince Hotel & Residence
Kuala Lumpur

Please complete in BLOCK CAPITALS as information is used to produce delegate badges.
Please photocopy for multiple bookings. Your priority registration code is printed below. Please quote it when registering.

EVENT CODE: 19564.003

BOOK AND PAY BEFORE 24 NOVEMBER 2012 AND SAVE $1350 ON THE CONFERENCE PACKAGE!

CONFERENCE PACKAGES

ALL PRICES SHOWN ARE IN US DOLLARS

	EARLY BIRD PRICE Payment BEFORE 24 November 2012	STANDARD PRICE Payment AFTER 24 November 2012
VENDOR PACKAGE		
☐ Conference + 3 workshops	**5,746** (SAVE 1350)	**6,046** (SAVE 1050)
☐ Conference + 2 workshops ☐ A ☐ B ☐ C	**4,597** (SAVE 1000)	**4,897** (SAVE 700)
☐ Conference + 1 workshop ☐ A ☐ B ☐ C	**3,448** (SAVE 650)	**3,748** (SAVE 350)
☐ Conference only	**2,299** (SAVE 300)	**2,599**
☐ Workshop only ☐ A ☐ B ☐ C	**1,499** (each workshop)	
PRIMARY PACKAGE		
☐ Conference + 3 workshops	**2,446** (SAVE 1350)	**2,746** (SAVE 1050)
☐ Conference + 2 workshops ☐ A ☐ B ☐ C	**2,197** (SAVE 1000)	**2,497** (SAVE 700)
☐ Conference + 1 workshop ☐ A ☐ B ☐ C	**1,948** (SAVE 650)	**2,248** (SAVE 350)
☐ Conference only	**1,699** (SAVE 300)	**1,999**
☐ Workshop only ☐ A ☐ B ☐ C	**599** (each workshop)	

- Discounts DO NOT apply to workshop(s)-only bookings
- Registrations without immediate payment or credit card details will incur a processing fee of USD99 per registration

DELEGATES REGISTRATION DETAILS

Title: Mr. ☐ Mrs. ☐ Ms. ☐ Dr. ☐ Other

First name: Surname:

Job Title: Department:

Email Address: Company:

Address:

Country: Postcode:

Telephone: OFFICE MOBILE Fax:

Approving Managers Name:

Email Address:

Delegates Signature: Approving Managers Signature: Date: DD / MM / YYYY

☐ I agree to IQPC's payment terms.

If the invoice is to be addressed for the attention of a different person than the delegate, please complete the details below:

First name: Surname:

Email Address: Telephone: OFFICE

If you have not received an acknowledgement before the conference please call us on **+65 6722 9388** to confirm your booking.

PAYMENT METHOD

☐ **I WISH TO PAY BY CHECK / BANK DRAFT:** MADE PAYABLE TO IQPC WORLDWIDE PTE LTD

☐ **I WISH TO PAY BY CREDIT CARD:** PLEASE DEBIT MY CREDIT CARD

Card Type: Visa ☐ MasterCard ☐ American Express ☐ Expiry Date: M M / Y Y Y Y

Card Number: / / /

Name Printed on the Card: DD / MM / YYYY

Signature: Date:

☐ **BY DIRECT TRANSFER** Please quote **19564.003** with remittance advice

IQPC Bank Details:
Account Name: IQPC Worldwide Pte Ltd **Bank Number:** 7232
Account Number: 260-085824-690 **Swift Code:** HSBCSGSG
Bank Address: The Hong Kong and Shanghai Banking Coporation, 21 Collyer Quay, #08-01 HSBC Building, Singapore 049320
Correspondent Bank: HSBC Bank USA, New York
Swift Code for Correspondent Bank: MRMDUS33

All bank charges to be borne by the payer. Please ensure that IQPC receives the full invoiced amount.

5 WAYS TO REGISTER

+65 6722 9388 +65 6720 3804
enquiry@iqpc.com.sg www.cybersecurityasia.com
IQPC Worldwide Pte Ltd, 61 Robinson Road, #14-01 Robinson Centre, Singapore 068893

TEAM DISCOUNTS

IQPC recognises the value of learning in teams. Group bookings at the same time from the same company receive these discounts:

◆ 3 or more 7% ◆ 5 or more 10% ◆ 8 or more 15%

This offer is exclusive of the early bird discount. Call us for a special discount rate for teams of 10 and above.

Not applicable to workshop(s) only bookings.

VENUE & ACCOMODATION

Prince Hotel & Residence Kuala Lumpur
Opposite Pavilion Kuala Lumpur
No.4 Jalan Conlay, 50450 Kuala Lumpur, Malaysia
Tel: +603-2170 8888
Fax: +603-2170 8999
Web: http://www.princehotelkl.com

Hotel accommodation and travel costs are not included in the registration fee. A reduced corporate room rate has been arranged at **Prince Hotel & Residence Kuala Lumpur** for attendees at this conference. To take advantage of this special rate, please process the hotel room reservation form provided upon confirmation of your attendance.

CONFERENCE DOCUMENTATION

☐ I am registering as a delegate, please send me an extra set of Conference Documentation with Audio CD with a USD100 discount: USD699.

☐ I cannot attend the event, please send me the Conference Documentation and Audio CD at USD799.

☐ I cannot attend the event, please send me the Conference Documentation only at USD549.

Orders without immediate payment or credit card details will incur a processing fee of USD99 per order.

(N.B. Advance orders will determine whether or not this conference will be recorded - Please enclose payment with your order.)

Any custom duties & taxes imposed on the shipment of order/s shall be borne by the recipient.

IQPC CANCELLATION, POSTPONEMENT AND SUBSTITUTION POLICY

• You may substitute delegates at any time by providing reasonable advance notice to IQPC. • **For any cancellations received in writing not less than eight (8) days prior to the conference, you will receive a 90% credit to be used at another IQPC conference which must occur within one year from the date of issuance of such credit. An administration fee of 10% of the contract fee will be retained by IQPC for all permitted cancellations. No credit will be issued for any cancellations occurring within seven (7) days (inclusive) of the conference.** • In the event that IQPC postpones an event for any reason and the delegate is unable or unwilling to attend in on the rescheduled date, you will receive a credit for 100% of the contract fee paid. You may use this credit for another IQPC event to be mutually agreed with IQPC, which must occur within one year from the date of postponement. • Except as specified above, no credits will be issued for cancellations. There are no refunds given under any circumstances. • IQPC is not responsible for any loss or damage as a result of a substitution, alteration or cancellation/postponement of an event. IQPC shall assume no liability whatsoever in the event this conference is cancelled, rescheduled or postponed due to a fortuitous event, Act of God, unforeseen occurrence or any other event that renders performance of this conference impracticable, illegal or impossible. For purposes of this clause, a fortuitous event shall include, but not be limited to: war, fire, labor strike, extreme weather or other emergency. • Please note that while speakers and topics were confirmed at the time of publishing, circumstances beyond the control of the organizers may necessitate substitutions, alterations or cancellations of the speakers and/or topics. As such, IQPC reserves the right to alter or modify the advertised speakers and/or topics if necessary without any liability to you whatsoever. Any substitutions or alterations will be updated on our web page as soon as possible.

DISCOUNTS:
All 'Early Bird' Discounts require payment at time of registration and before the cut-off date in order to receive any discount. Any discounts offered whether by IQPC (including team discounts) must also require payment at the time of registration. All discount offers cannot be combined with any other offer.

YOUR DETAILS:
Please email our Database Manager at enquiry@iqpc.com.sg and inform them of any incorrect details which will be amended accordingly.

DATA PROTECTION:
Personal data is gathered in accordance with the Data Protection Act 1984. Your data may be passed to other companies who wish to communicate with you offers related to your business activities. If you do not wish to receive these offers, please tick the box below.

☐ Please do not pass my information to any third party.

PAYMENT TERMS

Registrations/orders received without immediate payment or credit card details will incur a processing fee of USD99 per registration/order. Payment is due in full upon receipt of invoice. Full payment prior to the event is mandatory for attendance.

IQPC WORLDWIDE PTE. LTD.
Company Registration No: 199702288Z

IQPC International Quality & Productivity Centre