

RAISS Forum Proceedings (Volume 3)

Meng-Chow Kang (Ed.)

12 November 2005



Editor

Meng-Chow Kang, CISSP, CISA

Co-Chair, RAISS Forum

Chair, Security & Privacy Standards Technical Committee
of the Information Technology Standards Committee, Singapore

Chief Security & Privacy Advisor, Asia Pacific Region, Microsoft

1 Marina Boulevard
#22-01 One Marina Boulevard
Singapore 018989

Contact

RAISS Forum Secretariat

c/o ITSC Secretariat
Infocomm Development Authority of Singapore (IDA)

8 Temasek Boulevard
#14-00 Suntec Tower Three
Singapore 038988

Email: nitsc@ida.gov.sg

ISBN 981-05-5252-1

Copyright © 2006
Printed in Singapore

Mr Meng-Chow Kang **Co-Chair, RAISS Forum**

What is information security? What is information security risk management? How do we achieve information security in organizations? What are the techniques and mechanisms for achieving information security objectives? How do we gain assurance of the design and implementation of a security feature, function, or system? How do we measure the effectiveness of information security system? These are but some of the common questions information security practitioners and business/IT managers have to deal with as part of their practices. The answers to these questions however often vary, from practitioner to practitioner, and organization to organization, depending on the knowledge and experiences of the individuals, as well as the policy and culture of the organization. To a newcomer in this field, as well as organizations wanting to step up their security practices, it becomes a challenge on whose answers they should base upon to develop and implement their plans and actions. These challenges are further heightened as we deal with the constantly changing and highly competitive business environment, fueled by technology innovation, convergence, and connectedness, which are constantly pushing for more information flow, more information exchange, and more information accessibility to provide more values and benefits to the businesses and users. While the objectives of information security and those of the technology innovations and changes converge to better serve the businesses and users, they also compete to gain control over the information involved, one for openness and the other for protection.

Security standards, while not the silver bullet, play a crucial role in helping practitioners and managers to work with the complexity of today's technology and business environment and manage the competing challenges involved in managing information and related risks. They form the baseline for managing known issues and risks, and provide a common language for people, organizations, and systems to communicate and interoperate, and come to a common understanding of the requirements and agreement for suitable solutions and actions.

However, not all questions relating to information security have an answer in the security standards today as well. This therefore presents many opportunities for new knowledge to be developed and contributed to the information security and related standards arena.

In a region like Asia, whereby a great diversity of culture prevails, we also see a great diversity in the area of standards development, adoption and practices. This presents many challenges as well as opportunities for us when we are addressing the issues and requirements and security standards development, adoption, and implementation relating to information security in Asia. At the same time, it also means that there are opportunities in which we could learn and leverage from each other and maximize the use of the limited resources within each economy.

The RAISS Forum is a regional gathering of information security standards experts, contributors, and organizations from around the Asia Pacific region aiming at these opportunities to deal with those challenges and potential leverages in the region. The Forum was conceptualized in late 2003, and officially inaugurated on 19 November 2004. The Forum aims to provide a platform for standard bodies in Asia to discuss and share knowledge and experiences on issues relating to information security standards adoptions, developments, and other related activities. The Forum also provides a platform for identifying and developing security standards and other supporting activities at a regional level to fulfill the needs of Asia.

Since the first meeting that was held in Tokyo in November 2004, members of the RAISS Forum have continued to meet informally and separately in different occasions, and discussed over emails and the online forum the issues that were shared at the meetings, and follow-up actions and projects that are meaningful to the Forum members and participants. These ongoing interactions have led to the successful completion of the second RAISS Forum meeting on 28 June 2005 in Singapore, and the execution of this third meeting in Kuala Lumpur, Malaysia, in conjunction with the ISO/IEC JTC 1/SC 27 working group meeting, and the Malaysia Information Security Standards Awareness Seminar.

The third meeting brought together the original members of the RAISS Forum, except for Chinese Taipei, which could not send a representative this time, and with the addition of New Zealand, as an observer, represented by Mr Andrew Mason, Director of BSA International. We were also honored by the presence and presentation of His Excellency Lar Narath, Secretary of State for the Ministry of Post and Telecommunications, Cambodia, on the state of information security development in Cambodia.

The meeting opened with a keynote by Mrs Fadillah Baharin, on behalf of Mrs Mariani Mohammad, Director General of the Department of Standards, Malaysia, which provided an update on the security standards activities and development in Malaysia and reaffirmation of the Malaysian government and industry's supports of security standards in the economy.

In addition to the economy updates on the respective security standards related strategies, activities, progresses, and challenges, which are reported in this proceedings, the meeting also discussed several project proposals that were originally raised by Singapore and Thailand at the second meeting. These proposals were discussed in two parallel breakout sessions, chaired by Mr Philip Sy and Mr Kin-Chong Chan, of the Security and Privacy Standards Technical Committee (SPSTC), IT Standards Committee (ITSC), Singapore. This includes a proposal to adapt the BS 7799 Lead Auditors training program for Network and Systems Security Administrators, a security standards toolkit to share best practices in security standards related organizations and activities, and an application security assurance framework. The Singapore security standards on business continuity and disaster recovery for service providers (SS 507) was also presented and discussed.

As in the previous proceedings, all the papers that were presented in the meeting have been included in this publication in order to document the knowledge and information shared and extending them to other economies that could not be present at the meeting. A summary of the consensus reached and key action items identified in the two breakout sessions and panel discussion are also included to capture the main outcome of the meeting, and serves as a basis for follow-up in subsequent meetings.

The third meeting in November 2005 has achieved another important milestone in the objectives that we have set forward in the inauguration of the RAISS Forum and re-endorsed in the second meeting. To realize and reap the benefits of security standards, continued supports, participations, and contributions from regional economies in Asia Pacific are critical. This includes the continuous supports from the respective national bodies and government agencies, and the industry, that provided much of the expertise and sponsorship needed to make ongoing progress possible.

While this proceedings is being published, the fourth meeting is also being planned, which is scheduled to be held on 22 April 2006, in Jeju, Korea, in conjunction with the ITU-T SG17 meeting. Regional security standards bodies or groups interested in joining the meeting should contact the Secretariat of the RAISS Forum via email at nistc@ida.gov.sg.

Acknowledgement

As in any forums and knowledge sharing events and meetings, the desired outcome would not be achieved if not for the generous contribution and active participation of the members, speakers, and participants involved. I am grateful to have the continuous supports of all the members, speakers, and participants who have in one way or another contributed to the success of the third meeting, as well as the speakers' follow-on work to have their presentations written for this Proceedings, which would not otherwise materialize. I would also like to thank Microsoft (Asia Pacific), ITSC Singapore, Standards, Productivity & Standards Board (SPRING Singapore), Infocomm Development Authority of Singapore (IDA Singapore), Department of Standards Malaysia, and National ICT Security and Emergency Response Centre (NISER), Malaysia for the management and financial supports rendered for organizing the Forum meeting and publishing this proceedings. In particular, Mr Ariffuddin Aizuddin, Mr Mohammad Zahari Zakaria, and Ms Rafidah Abdul Hamid for assisting in organizing the third meeting, and Phillip Sy and Kin-Chong Chan for their facilitation and follow-up actions for the two breakout sessions. And finally, special thanks to Mr Koji Nakao (Co-Chair of RAISS Forum), and Ms Yean-Lan Thay (Secretariat of RAISS Forum), for all the efforts and hard work put into the realization of the Forum and this meeting.

Mr Meng-Chow Kang

*CISSP, CISA
Co-Chair, RAISS Forum, Singapore*

*Chair, Security & Privacy Standards Technical Committee
ITSC, Singapore*

Chief Security & Privacy Advisor, Asia Pacific Region, Microsoft



Based in Singapore, Meng-Chow is the regional Chief Security & Privacy Advisor for Microsoft Asia Pacific region. His current responsibilities include developing and implementing Microsoft's trustworthy computing strategy in the region, and providing advice and guidance to customers and IT professionals on security best practices and solutions for implementing and managing information security in their organizations.

Meng-Chow has been a practicing information security professional for more than 18 years, with experiences spanning from technical to management in the various security and risk management roles that he has held in the Singapore government, major financial institutions, and security technology provider. His last position prior to Microsoft was Vice President and Regional Information Risk Officer of JPMorganChase.

Since 1998, Meng-Chow has also been concurrently chairing the Singapore's IT Security and Privacy Standards Technical Committee (SPSTC), representing Singapore in the ISO/IEC JTC 1/SC 27 Security Techniques committee. In 2004, Meng-Chow initiated and begun co-chairing the Regional Asia Information Security Standards (RAISS) Forum. In November 2004, Meng-Chow was also appointed Associate Rapporteur of Study Group 17 (Security and Language), ITU-T focusing on addressing the Study Question relating to Cybersecurity. Meng-Chow is also a Board Member of the Asia Advisory Board for the International Information Systems Security Certification Consortium (ISC²).

In August 2005, Meng-Chow was presented with the accolade "IT Evangelist of the Year 2005" by the Singapore National Infocomm Competency Centre (NICC) in recognition of his work and contribution to the IT security community and standards arena. Meng-Chow was also presented the "Distinguish Award" from the Standards, Productivity and Innovation Board (SPRING Singapore) in September 2005 for his effort and leadership in shaping the IT security standardization landscape in Singapore.

Meng-Chow received his MSc degree in Information Security from the Royal Holloway and Bedford New College, University of London. He has been a Certified Information Systems Auditor (CISA) since 1997, and a Certified Information Systems Security Professional (CISSP) since 1998.

Contents

01	Agenda Of The 3rd RAISS Forum Meeting	07
02	Opening Speech Y. Bhg. Puan Mariani Mohammad Director General, Department of Standards Malaysia (DSM)	08
	Status Update From Each Economy	
03	Australia Australian Standardization Priorities In 2005 John Snare	10
04	Japan Information Security Activities In Japan - Progress And Updates Koji Nakao	18
05	Malaysia Updates On Information Security Standards Activities In Malaysia Rafidah Abdul Hamid	30
06	Singapore Guidelines For Information And Communications Technology Disaster Recovery Services Standard Kin-Chong Chan	36
07	South Korea New National Identification Infrastructure On The Internet In South Korea Prof Heung-Youl Youm	44
08	Thailand Information Risk Management Course For Technical Personnel, Based On BS 7799 / ISO/IEC 17799 Standard Komain Pibulyarajana, Banchong Harangsi, Siriwan Apisiridej, Doungkamol Suppitayakorn, Puth Nateesuwana	54
09	SC 27 Report An International Common Language For Information Security - An Update On ISO ISMS Standards Ted Humphreys	64
	Contribution	
10	RAISS Forum Projects Discussion Kin-Chong Chan, Philip Sy	72
	Appendix	
11	Appendix A Questionnaires To Gather Information For Security Standards Toolkit And Mutual Recognition Of Security Certification Projects	86
12	Appendix B Regional Asia Information Security Standards (RAISS) Forum - Terms Of Reference	89

01 Agenda Of The 3rd RAISS Forum Meeting

12 November 2005

The Regent Hotel, Level 3, Regent VIII

Kuala Lumpur, Malaysia

Agenda

Time	Topic
1415hrs to 1430hrs	Registration
1430hrs to 1445hrs	Introduction by Host and Co-Chairs' Opening Address <ul style="list-style-type: none">■ Opening Speech by Mrs Fadilah Baharin on behalf of Mrs Mariani Mohammad, Director-General, Department of Standards Malaysia■ Koji Nakao, Co-Chair, RAISS Forum■ Meng-Chow Kang, Co-Chair, RAISS Forum
1445hrs to 1530hrs	Recent Regional Developments and Updates on Information Security and Related Standards <ul style="list-style-type: none">■ Australia: John Snare■ Cambodia: H.E Lar Narath■ Japan: Koji Nakao■ Malaysia: Mohd Zahari Zakaria■ Singapore: Kin-Chong Chan■ South Korea: Prof Heung-Youl Youm■ Thailand: Dr Komain Pibulyarajana
1530hrs to 1545hrs	Coffee Break
1545hrs to 1730hrs	Project Discussion <ul style="list-style-type: none">- Two parallel tracks focusing on selected projects■ Track 1 - Facilitated by Philip Sy, Singapore<ul style="list-style-type: none">• Security Standards Toolkit• Mutual Recognition of Security Certifications• Business Continuity and Disaster Recovery■ Track 2 - Facilitated by Kin-Chong Chan, Singapore<ul style="list-style-type: none">• Guidelines for Risk Assessment for Network and Systems Security Administrators• Application Security Standards
1730hrs to 1815hrs	Panel discussion and action plan
1815hrs to 1830hrs	Closing remarks and plan for next meeting
1830hrs to 2000hrs	Evening reception

Y. Bhg. Puan Mariani Mohammad

Director General, Department of Standards Malaysia (DSM)

At the

Regional Asia Information Security Standards (RAISS) Forum

(read by Pn Fadilah Baharin, Director of Standards DSM)

12 November 2005, The Regent Hotel, Kuala Lumpur, Malaysia

Distinguished Guests, Speakers, Ladies and Gentlemen,

Assalamualaikum warahmatullahi wabarakatuh and Good Afternoon,

First of all, I would like to extend a warm welcome to you in attending this Regional Asia Information Security Standards (RAISS) Forum.

I would like to take this opportunity to convey my appreciation and gratitude to the RAISS Forum committee members for organizing this event and giving me the honor to say a few words. I would also like to congratulate the RAISS Forum members for their efforts to gather in Kuala Lumpur.

Ladies and gentlemen,

It is encouraging to note that this RAISS Forum was formed to reap the potential benefits and values through regional security standards bodies' participation and collaborations with the objectives of providing a platform for:

1. sharing of knowledge and learning experiences in regional economies on information security standards development, adoption, and deployment;
2. regional bodies to identify opportunities for future collaborations to further the course of developing international security standards and its more effective promulgation in the Asia regions.

This initiative may include, but not limited to establishing regional security standards requirements and directions and establishing regional agreements or understandings to promote interoperability and consistency in standards implementation and use.

I am pleased to inform you that the Malaysian Government recognizes the importance of standards as one of the tools for the country to compete globally. Hence, to promote standards development and its related activities, DSM has obtained such recognition from the Cabinet on 24 July 2002.

As for Malaysia's involvement in the RAISS Forum, the country will be able to ensure that it remains at the forefront of the latest ICT security standards development, especially those that impact the nation and the Asian region as a whole. Various issues with regard to the international ICT security standards development will be discussed first-hand at the RAISS Forum and then later will be presented as a jointly recommended improvement plans from the RAISS Forum members at the ISO meetings. These activities will increase Malaysia's visibility as being a driving force in standards development at both regional and world platforms. Malaysia will also have the opportunity to learn and review the developments being made in the field from other Asian countries and adapt/adopt some of the relevant developments if it is feasible to be implemented in the country.

As for the participating economies in the RAISS Forum, increasing participation from more economies in the Asian region will be crucial towards the overall progress and development of the RAISS Forum. By having more economies participation, more initiatives can be taken that could possibly bring more benefits including economic and social ones. Also, it would be good if more technical experts can be brought in to discuss the various technical ICT standards available. It is recommended that many other Asian countries to be involved in the Forum more actively as they will benefit tremendously by the sharing of ideas & expertise between the economies represented in the Forum.

Ladies and gentlemen,

It is our hope that that this Forum will continue in years to come and be able to foster a good understanding between the RAISS Forum members.

Finally, I hope that all of you will have an enjoyable time learning and sharing experiences during this meeting and please do take some time to visit many interesting places around Malaysia.

On that note, I hereby declare this meeting open.

Thank you.