Organisation de Coopération et de Développement Économiques
Organisation for Economic Co-operation and Development

18-Feb-2014

English - Or. English

DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY
COMMITTEE FOR INFORMATION, COMPUTER AND COMMUNICATIONS POLICY

DSTI/ICCP/REG(2014)1
Unclassified

Working Party on Information Security and Privacy

REPORT OF THE APEC-OECD SYMPOSIUM ON SECURITY RISK MANGEMENT IN THE INTERNET ECONOMY

18 September 2013

This report summarises the joint APEC-OECD Symposium on Security Risk Management in the Internet Economy, which took place in Hawaii, United States on 18 September 2013 as part of the 48th Meeting of the APEC Telecommunications and Information Working Group.

Contact: Aaron Martin: Tel: +33-1 45 24 9477; e-mail: aaron.martin@oecd.org

JT03352671

English - Or. English

REPORT OF THE APEC-OECD SYMPOSIUM ON SECURITY RISK MANAGEMENT IN THE INTERNET ECONOMY

18 September 2013, United States

Background

1. On 18 September 2013, APEC and the OECD held a joint workshop entitled *APEC-OECD Symposium on Security Risk Management in the Internet Economy* in Hawaii, United States, as part of the 48th Meeting of the APEC Telecommunications and Information Working Group (TEL). Through a series of panels and moderated discussions, the workshop considered policies and approaches for managing security risk, while taking into account accomplishments since the publication of APEC's *Strategy to Ensure a Trusted, Secure, and Sustainable Online Environment* (TSSOE) and the 2002 OECD *Guidelines for the Security of Information Systems and Networks* (Security Guidelines). The workshop sought to support the ongoing review of the Security Guidelines as well as a review of the TSSOE. By partnering to deliver this workshop, and by considering these important documents together, APEC and the OECD sought to ensure that both resonate beyond APEC's and OECD's respective member economies and are applicable to the broader global community.

2. The objectives of the workshop were to:

- Raise awareness and add value to the reviews of both the APEC TSSOE and the OECD Security Guidelines.
- Provide a platform for experts from government, industry, and the technical community to exchange views on policy issues and trends related to managing security risk for economic and social prosperity in the digital economy.
- Add a milestone to the longstanding relationship between APEC TEL and the OECD Working Party on Information Security and Privacy (WPISP), private sector and the technical community.

3. The workshop drew approximately 90 participants from APEC and OECD economies, including policymakers and representatives from the private sector and the technical community.

Opening Session

4. **Nur Sulyna Abdullah,** Chair of APEC TEL, welcomed participants to the symposium. She noted the timeliness of the symposium given our growing reliance on information systems and networks and provided a brief history of work items within APEC TEL, including a workshop held during TEL 43, that have informed a possible review of the APEC TSSOE. She reinforced the importance of continued collaboration between APEC and the OECD, to maximize resources and leverage joint efforts to achieve common goals.

5. **Laurent Bernat,** Cybersecurity Policy Analyst for the OECD, welcomed participants on behalf of the OECD. He provided an overview of the history of the Security Guidelines and their ongoing review. He underlined that the objective of the review is economic and social prosperity and that security is addressed as a means to foster it. He also reinforced the importance of the relationship between the OECD WPISP and APEC TEL.

SESSION I: STRATEGIES AND POLICIES TO MANAGE SECURITY RISK

Overview

6. This session aimed to take stock of developments since 2002 and 2005 when the Security Guidelines and TSSOE were adopted. It set out to explore recent policy developments in OECD, APEC and other economies. The session covered public policies as well as policies and approaches developed by non-governmental stakeholders. It aimed to address policy development at both the strategic and implementation levels, as well as future policy trends.

7. Key themes from this session include:

- Buy-in at all levels of government and among stakeholders, when developing national cybersecurity policy frameworks, is essential due to the way cybersecurity responsibility is distributed among them.
- Given our growing reliance on information systems and networks, improving all countries' capacity to address cyber threats is critical to security risk management in the Internet economy.
- Regional forums are important vehicles for addressing security issues and building cybersecurity capacity.
- There is an imperative to develop globally interoperable standards that benefit cybersecurity, reflect stakeholders' objectives regarding technology and policy innovation, and can be rapidly adopted.
- There is a need to bridge the gap between the policy and technical communities, at the national, regional, and global levels, both in the public and private sectors.
- There is a need to create and maintain mechanisms for stakeholders to engage in dialogue on security and security risk management.
- Security risk management is a never-ending task for government, private sector, and the technical community and requires dedicated budget and resources.

Summary of presentations

8. **Thongchai Sangsiri**, from the Electronic Transactions Development Agency (ETDA) in Thailand delivered a presentation on managing cybersecurity risk in the Thai public sector. He explained the importance of having legal infrastructure in place to support a policy framework to manage cybersecurity risk. Mr. Sangsiri described the experience of developing a National Cybersecurity Policy Framework, and underscored the importance of "top-level buy-in", international cooperation, and incentives for responsible parties, as key components of security risk management.

9. **Dmitri Kostrov**, from the Russian Ministry of Communications and Mass Media presented on the Russian Federation's approach to ensure information security, a concept that is broader than cybersecurity. He explained the key responsibilities of the Ministry of Communications and Mass Media, with include, among others, developing State policy on security and privacy for the Russian Federation.

He also discussed the Ministry's involvement in technical standards processes underway in the International Telecommunications Union Standardization sector (ITU-T).

10. **Peter Lord**, from Oracle, underscored the importance of developing globally relevant standards, both to increase interoperability and to accomplish our collective goal for economic and social prosperity. He explained that technology that reflects local preferences without taking the global Internet economy into account will likely limit choice, reduce security, and increase cost. He offered four recommendations for public policies: *i*) make choices that lower barriers to adoption of the technology; *ii*) promote harmonization and interoperability; *iii*) continue to participate in global policy and standards activities; *iv*) build capacity through regional forums.

11. **Jürgen Treib**, from the German Federal Ministry of the Interior (BMI) provided an overview of the current threat environment and a history of BMI's approach to cybersecurity issues over the past three years. He described the elements of the 2011 German Cybersecurity Strategy, including the establishment of a National Cyber Response Centre, which serves as a platform for operational collaboration, and the National Cyber Security Council, which serves as a mechanism for policy coordination.

12. **Matthew Healy**, from Macquarie Telecom, discussed the private sector's role in supporting national cybersecurity policy in Australia. He described Australia's *Protective Security Policy Framework*, which provides a consistent and structured approach to risk assessment for private sector management of public sector data. It was noted that where data is located is an important aspect of risk assessment.

SESSION II: FOSTERING CO-OPERATION AMONG STAKEHOLDERS

Overview

13. Co-operation among stakeholders is a key theme of both the Security Guidelines and the TSSOE. This session focused on how public and private stakeholders' cooperation to develop and implement policies to manage risk in the Internet economy has evolved since 2002, current best practices, and the direction such co-operation could take in the future. The session addressed government co-operation with other stakeholders including the private sector, civil society, academia, and the technical community. There was also discussion of voluntary initiatives among these non-governmental stakeholders.

14. Key themes from this session include:

- There is an imperative for collaboration, given the increasingly interconnected global environment as well as the rising cost of cybercrime.
- Stakeholder buy-in is critical to successful cooperation.
- Public-private partnership frameworks can enable innovative solutions to complex challenges, as each stakeholder brings different expertise and resources.
- Collaboration can be fostered by undertaking joint work on specific, non-controversial items.
- Technical solutions alone cannot address all security issues.
- The development of security risk management policy frameworks should be undertaken through a process that enables inputs from all stakeholders.

Summary of presentations

15. **Chris Drew** from the Australian Department of Communications, formerly the Department of Broadband, Communications, and the Digital Economy, discussed the role of the Computer Emergency Response Team, CERT Australia, in partnering with businesses to address cyber threats. He also provided an overview of the "iCode", a voluntary code of practice developed by the private sector and government to promote a better cybersecurity culture within ISPs and provide a consistent approach to help ISPs educate their customers on cybersecurity issues.

16. **Kai Koon Ng**, from Symantec, underscored the imperative for collaboration between government and the private sector to address cyber threats. He offered examples of successful public-private partnership (PPP)frameworks including cyber exercises conducted by the US' Critical Infrastructure Partnership Advisory Council (CIPAC), information sharing through Australia's Trusted Information Sharing Network (TISN), child online safety under the UK Council for Child Internet Safety, botnet remediation under Germany's Botfrei.de initiative, awareness raising by the Cybersecurity Awareness Alliance, and best practices developed by the European Public Private Partnership for Resilience (EP3R). Mr. Ng posed three questions for participants to consider: *i*) are these initiatives relevant to the threat landscape in your economies? *ii*) how can national public private partnerships (PPP) be expanded to be globally collaborative? *iii*) how can PPPs be leveraged for lessons learned to incorporate into globally accepted best practices and standards?

17. **Duangthip Chomprang** from the Internet Society (ISOC) described the importance of multistakeholder cooperation in addressing issues related to both security and privacy. She highlighted that technical solutions alone will not address all issues and must be complemented by education and awareness raising as well as norms.

18. **John Weigelt**, from Microsoft Canada, illustrated the importance of collaboration with respect to cybersecurity as well as critical infrastructure protection through the example of Canada's approach to public-private partnership. He also highlighted ongoing partnerships for cybersecurity education and awareness in Canada, including the awareness campaign "GetCyberSafe" and academic partnerships. Mr. Weigelt offered three main lessons from Canada's experience in developing strong public-private partnerships: *i*) engage early,; *ii*) put work items in front of the community; *iii*) collaborate with local and international partners.

SESSION III: PRACTICAL APPROACHES TO INTERNATIONAL CO-OPERATION

Overview

19. This session focused on practical means of fostering and improving international co-operation for security risk management in the Internet economy, including a discussion on capacity building at policy and operational levels. The session also aimed to better understand the role played by regional and international organisations in this area.

20. Key themes from this session include:

- There is a need for country comparable statistics to enable a comparison of the environment within and between nations.
- There is a need for greater linkages between policymakers and operators, at the national, regional, and global levels, to better assess the effectiveness of policies and to improve crisis response readiness.
- Cybersecurity capacity building is needed to raise the bar globally and regional and international organisations can contribute.
- Cohesive approaches are being applied more broadly than in the past, both with respect to technical and policy innovation. International cooperation is increasingly considered a key part of the development process rather than as a next step.
- The value of international cooperation at multiple levels, including the regional and local levels, cannot be underestimated

Summary of presentations

21. **Yurie Ito**, from *Asia Pacific Computer Emergency Response Team (AP-CERT)* explained the history of collaboration among Computer Emergency Response Teams (CERTs) and how the changing nature of threats caused them to evolve from academic entities to government entities. She highlighted the importance of regional cooperation and described some of AP-CERT's ongoing activities, including information sharing, incident response support, cyber exercises, and mutual participation in ICT forums and meetings, which both improve mutual security and build trust. Ms. Ito offered a future vision for how to foster successful cooperation between CERTs: *i*) change the conversation from "security" to "risk reduction"; *ii*) keep discussions of cyber warfare or national security separate from CERT cooperation; and, *iii*) focus on global and regional cyber risk reduction and management.

22. **Audrey Plonk**, from Intel, discussed how international cooperation permeates all aspects of the Internet economy, including how technology is built. She emphasised the need to build partnerships, establish flexible and technology neutral laws, develop accountability systems, and foster policy innovation in addition to technical innovation. Ms. Plonk also explained that international cooperation does not always need to occur at the global level, highlighting the importance of working at multiple levels, including the regional and local levels.

23. **Jaesuk Yun**, from the Korea Internet and Security Agency (KISA) delivered a presentation on the importance of cybersecurity capacity building. He highlighted several key initiatives that support developing countries in improving cybersecurity capabilities including "K-Link", an ICT training course, and its Knowledge Sharing Program, through which Korea shares its development experience. Mr. Yun also discussed the Korean national strategy for Information Security Capacity Building, which trains individuals for careers in digital security and assists them with career transition through high-level workforce development programs designed and offered through public-private partnerships.

SESSION IV: AWARENESS, EDUCATION AND SKILLS

Overview

24. In this session, participants discussed various approaches and best practices to raise awareness, improve education and develop skills for managing security risks in the Internet economy. The session addressed cybersecurity awareness raising initiatives underway by both the public and private sectors for a range of target audiences, from policymakers to the general public. It also covered skills training to build technical capacity within the national workforce as well as in developing countries.

25. Some key themes that emerged from this session include:

- Public-private partnerships play a key role in raising cybersecurity awareness and improving technical skills.
- An understanding of the target audience is needed to effectively develop and adapt awareness raising materials and approaches.
- There is value in having a harmonised and clear message that can be delivered through multiple channels to raise cybersecurity awareness.
- Measuring how effective or successful programs are at changing or influencing behavior is difficult, and there is a need to develop metrics.

Summary of presentations

26. **Chris Boyer**, discussed AT&T's US and global efforts to disseminate best practices and raise cybersecurity awareness. He explained efforts by the Messaging, Malware, and Mobile Anti-Abuse Working Group (M3AAWG), an organization with global private sector membership that issues best practices, papers, and position statements targeting messaging abuse. Mr. Boyer also described ongoing global online cybersecurity initiatives, including the National Cyber Security Alliance and the "Stop.Think.Connect" campaign, which delivers a single harmonised message around online safety and security, during the National Cyber Security Awareness Month, held annually in October, and the Data Privacy Day, held annually on January 28th.

27. **Estelle Moungseob Shim**, from the Center for Asia-Pacific ICT Development delivered a presentation on ongoing efforts to raise awareness on ICT misuse through skills education. She explained the methodology for developing educational materials and "train-the-trainer" modules and how successful training programs in the Asia-Pacific region were implemented. Ms. Shim noted three key factors behind successful training programs: *i*) Listen to and accept local expert advice, *ii*) Ensure that content is tailored for the local context, *iii*) Use visual content in diverse activities.

28. **Kiyomi Sakamoto**, from the Japanese Ministry of Economy, Trade, and Industry provided an overview of Japan's approach to cybersecurity, including its cybersecurity strategy, information sharing framework, and Security for Industrial Control Systems (ICS). She discussed ongoing awareness raising initiatives, including a portal called "Kokokara Security!" which aggregates ongoing awareness raising efforts being implemented by private sector partners. Ms. Sakamoto also discussed workforce development activities, including a public-private effort to organise seminars for security leaders of small businesses.

She finally described recent cybersecurity capacity building activities to support CSIRT development in the APEC region.

29. **Saravanan Kulanthaivelu**, from the Malaysian Communications and Multimedia Commission, discussed Malaysia's national strategic objectives for cybersecurity and capacity building, which include: *i*) develop, foster, and maintain a national culture of security; *ii*) standardize and coordinate education programs, *iii*) establish effective mechanisms for cyber knowledge dissemination at the national level, *iv*) identify minimum requirements. He highlighted recent initiatives, including its Klik Dengan Bijak (Click Wisely) program, which leverages existing initiatives and partnerships to raise cybersecurity awareness, and an initiative to ensure that its Critical National Information Infrastructure agencies are Information Security Management System certified, among others.

NEXT STEPS

30. The workshop outcomes as outlined in this report will be presented at the 35th Meeting of the OECD WPISP in Paris, France in December 2013.These elements will serve as input to the review of the 2002 OECD Security Guidelines. The next stage of the review will be discussed at the same WPISP meeting as well as the following day by its parent body, the Committee for Information, Computer and Communications Policy (ICCP).

31. In the APEC TEL context, the United States, in its role as Convenor of the APEC TEL Security and Prosperity Steering Group, plans to circulate a short questionnaire to APEC membership about various aspects (building on the themes of the themes of the Symposium) of the TSSOE, which will inform its review. The questionnaire will be circulated prior the 49th Meeting of the TEL, which will take place in spring 2014. APEC TEL plans to share the results of the questionnaire with OECD membership.

APEC-OECD SYMPOSIUM ON SECURITY RISK MANAGEMENT IN THE INTERNET ECONOMY
18 SEPTEMBER 2013
HAWAII, UNITED STATES

FINAL LIST OF SPEAKERS

Nur Sulyna Abdullah
APEC TEL

Laurent Bernat
OECD

Chris Boyer
AT&T

Duangthip Chomprang
Internet Society

Chris Drew
Department of Broadband, Communications, and the Digital Economy, Australia

Matthew Healy
Macquarie Telecom

Yurie Ito
Asia-Pacific Computer Emergency Response Team

Dmitri Kostrov
Ministry of Communications and Mass Media, Russia

Saravanan Kulanthaivelu
Communications and Multimedia Commission, Malaysia

Peter Lord
Oracle

Kai Koon Ng
Symantec

Audrey Plonk
Intel

Kiyomi Sakamoto
Ministry of Economy, Trade, and Industry, Japan

Thongchai Sangsiri
Electronic Transactions Development Agency, Thailand

Estelle Moungseob Shim
Center for Asia-Pacific ICT Development, Republic of Korea

Jordana Siegel
Department of Homeland Security, United States

Jürgen Treib
Federal Ministry of the Interior, Germany

John Weigelt
Microsoft Canada

Jaesuk Yun
Korea Internet & Security Agency, Republic of Korea