International Telecommunication Union

Australian Government
Department of Broadband, Communications and the Digital Economy

Forum Summary, Wrap-Up, and the Way Forward

ITU Regional Cybersecurity Forum for Asia-Pacific[1]

Brisbane, Australia
16-18 July 2008

Eun-Ju Kim
Head, ITU Regional Office for Asia-Pacific

Today, we are ending this three day long **ITU Regional Cybersecurity Forum for Asia-Pacific** here in Brisbane, where over 72 participants attended from 26 countries. I do not have to repeat the importance of cybersecurity and the protection of critical information infrastructures and assets for each nation's security, prosperity and economic well-being. This has been stressed by His Excellency Senator Stephen Conroy, Minister for Broadband, Communications and the Digital Economy (DBCDE), during his Ministerial Address on the first day of the Forum as well as other distinguished speakers from the Australian government and from other countries throughout the duration of this event.

Looking back at the sessions of this event we can note the following:

Session 1: Cybersecurity and Critical Information Infrastructure Protection were examined within the context of the ITU National Cybersecurity Framework

[1] See the ITU Regional Cybersecurity Forum for Asia-Pacific website at www.itu.int/ITU-D/cyb/events/2008/brisbane/

currently being developed in the ITU Development Sector's Study Group 1 under its Question 22/1 related work. In addition to an insight into the Framework and the related ITU National Cybersecurity/CIIP Self Assessment Toolkit, the participants also learned about some of the issues currently under discussion in Australia with regards to critical infrastructure protection.

The address by Senator Stephen Conroy, Minister for Broadband, Communications and the Digital Economy (DBCDE), further highlighted some of the main activities undertaken by the executing agencies in Australia in order to work towards implementing a shared vision of promoting a culture of security as well as building confidence and security in the use of ICTs.

Session 2: In promoting a culture of cybersecurity, we all learned about some of the innovative initiatives into region that aim to raise awareness of the importance of cybersecurity and educate users of all ages about how they protect themselves and stay safe online. The important and specific roles played by the different actors - i.e. the government, the private sector, academia, civil society in promoting a culture of cybersecurity - were highlighted.

Session 3: In building stronger and more effective relationships between government and industry, we learned about the benefits from engaging industry early from development to implementation of a national cybersecurity strategy. We also learned about the benefits of Cyber Storm exercises and why this is a useful exercise for both the government agencies and private sector players.

Session 4: Appropriate legislation, international legal coordination and enforcement are all important elements in preventing, detecting and responding to cybercrime and the misuse of ICTs. Discussions in this session looked at specific aspects of the Council of Europe's Convention on Cybercrime and the challenges faced by Pacific Island nations in crafting cybercrime-related

legislation. Different tools and resources are available to help Member States to better understand the challenges related to cybercrime were also shared.

Session 5: It was noted that one of the main activities for addressing cybersecurity at the national as well as regional level is preparing for, detecting, managing, and responding to cyber incidents through the establishment of watch, warning and incident response capabilities or CERT/CSIRT type of activities. It was noted that threats to cybersecurity are becoming more severe; and while it is difficult to secure our online assets today, it will be increasingly difficult to secure what we will have in the future.

Session 6: As the final pillar of ITU's national cybersecurity framework, we listened to a number of interesting presentations and country case-studies. We also understood that whatever happens in bigger countries often filter down and affect also the small countries. We learned how the ITU National Cybersecurity/CIIP Self-Assessment Toolkit can be a useful tool and benchmark for both developed and developing economies, when governments review and try to better understand their existing national approach to cybersecurity as well as when they are trying to identify areas for attention, and prioritize to address cybersecurity.

Session 7: The participants acknowledged that improving cybersecurity is a global problem and that each country must undertake action to join and support international efforts to improve cybersecurity.

Session 8 and Session 9: Increased capacity building for interested countries in the Pacific region was discussed during the two sessions dedicated to the special needs and requirements of Small Island Developing States (SIDS), when it comes to enhancing cybersecurity.

Session 10: We just concluded the event with Session 10, dedicated to Regional and International Cooperation noting that regional and international cooperation is extremely important in fostering national efforts and in facilitating interactions and exchanges, at all levels, for increased cybersecurity at the interdependent and globalized information society. The importance of regional cooperation, joint initiatives and the sharing of resources and information on best practices, training and education was noted as critical going forward.

If I may repeat what our experts have stressed in the last three days, cybersecurity is not just one specific person's responsibility, but that of all participants in the interconnected information or ubiquitous society. Therefore, we need to involve all stakeholders whether it they are in the public sector, private sector, or country citizens. Hence, public-private partnerships and raising awareness campaigns are crucial for ensuring cybersecurity. We must also apply a holistic framework and integrated approach to develop and implement a national strategy. This is why the ITU has worked, and will continue to work, with many other organizations including PITA, APT, APECTEL, as well as national and regional CERTs/CSIRTs, etc. when developing tools and guidelines related to cybersecurity and critical information to avoid any duplication of effort.

From this we can note five recommendations for concrete actions that need to be taken by countries in the region:

1) Enhance watch, warning and incident response capabilities in the Pacific Islands through the creation of a Pacific CERT with studying first the ways of creation and further maintenance of such a Computer Emergency Response Team (CERT)/ Computer Security Incident Response Team (CSIRT).

2) Encourage countries to use the ITU National Cybersecurity Framework and related tools as a structure for thinking through issues related to the creation of a national cybersecurity strategy.

3) Use available resources, toolkits and material to raise awareness amongst all stakeholder groups on cybersecurity threats as genuine security can only be promoted, when every user is aware of the possible dangers and threats online.

4) Share information on national cybersecurity best practices with other countries in the region and play an active role in the activities to finalize the report being developing in ITU-D Study Group Question 22/1: Securing information and communication networks - Best practices for developing a culture of cybersecurity.

5) Carry out study on economic aspects and indicators of cybersecurity.

6) Identify and provide ITU a focal point responsible for coordinating with ITU, particular the Regional Office for Asia and the Pacific, in activities related to cybersecurity.

As the way forward, ITU will:

1) At the international level, strengthen collaboration among its three Bureaus and its partners. The Union will also enhance its partnerships with other international organizations including standardization bodies, governments, and private sectors in areas related to cybersecurity and critical information infrastructure protection and will also continue to work closely with its regional offices to assist ITU Member States and Sector Members in related activities.

2) At the regional and national levels, the ITU Regional Office for Asia and the Pacific will work in close cooperation with the ICT Applications and Cybersecurity Division of ITU Telecommunication Bureau to assist Member States, especially the developing countries in the Asia-Pacific region in such key areas as: e.g. Providing forums for participants to learn about ITU's new products, to gain more knowledge from experts, to exchange information and practices among countries. In this regard, it is expected that a regional forum on cybersecurity will be organized again in 2009;

3) Build human capacity through training programmes and/or workshops. For instance, on-line training and/or face-to-face classroom training will be provided through five ITU Centres of Excellence in the Asia-Pacific region;

4) Provide toolkits such as the ITU National Cybersecurity/CIIP Self-Assessment Toolkit and any other available tools through close coordination between ITU Regional Office and focal points of the countries;

5) Provide ITU experts as part of direct country assistance to help countries implement activities related to cybersecurity such as development and implementation of cybersecurity strategies, cybercrime legislation and enforcement mechanism; and,

6) Facilitate the establishment of a Pacific CERT and national CERTs/CSIRTs, as and when requested.

In conclusion, all the papers and summary of each session of the Forum will be posted at the ITU website at http://www.itu.int/ITU-D/cyb/events/2008/brisbane/presentations.html