International Telecommunication Union

Australian Government

Department of Broadband, Communications and the Digital Economy

ITU Regional Cybersecurity Forum for Asia-Pacific and Seminar on the Economics of Cybersecurity

15-18 July 2008
Brisbane, Australia

Draft Forum Agenda

Description: At the start of the 21st century, modern societies have a growing dependency on information and communication technologies (ICTs) that are globally interconnected. This interconnectivity creates interdependencies and risks that must be managed at national, regional and international levels. At the national level, each nation should consider organizing itself to take coordinated action related to the prevention of, preparation for, response to, and recovery from cyber incidents. Such action requires coordination and cooperation among national participants, including, those in government, business, and other organizations, as well as individual users, who develop, own, provide, manage, service and use information systems and networks. The formulation and implementation by all nations of a national framework for cybersecurity and critical information infrastructure protection (CIIP) represents a first step in addressing the challenges arising from globally interconnected ICT infrastructures.

This Regional Cybersecurity Forum for Asia-Pacific, hosted by the Department of Broadband, Communications and the Digital Economy (DBCDE), Government of Australia, aims to identify the main challenges faced by countries in the region in developing frameworks for cybersecurity and CIIP, to consider best practices, share information on development activities being undertaken by ITU as well as other entities, and review the role of various actors in promoting a culture of cybersecurity. This forum, one in a series of regional events organized by ITU-D, is being held in response to *ITU Plenipotentiary Resolution 130: Strengthening the role of ITU in building confidence and security in the use of information and communication technologies* (Antalya, 2006) and the 2006 World Telecommunication Development Conference Doha Action Plan establishing *ITU-D Study Group Question 22/1: Securing information and communication networks: Best practices for developing a culture of cybersecurity*. As part of this activity, ITU is developing a *Report on Best Practices for a National Approach to Cybersecurity* which outlines a *Framework for Organizing a National Approach to Cybersecurity* identifying five key elements of a national effort, including: 1) Developing a national cybersecurity strategy; 2) Establishing national government-industry collaboration; 3) Creating a national incident management capability; 4) Deterring cybercrime; and 5) Promoting a national culture of cybersecurity.

The first day of the event, 15 July 2008, will be dedicated to an ITU Tariff Group for Asia and Oceania (TAS) Seminar on the Economics of Cybersecurity.

SEMINAR ON THE ECONOMICS OF CYBERSECURITY	
TUESDAY 15 JULY 2008	
08:00–09:00	**Meeting Registration**
09:00–09:15	**Meeting Opening and Welcome**
	Welcoming Address: Representative from the ITU Tariff Group for Asia and Oceania (TAS) *Opening Remarks:* Seminar Chairperson
09:15–10:15	**Session 1: The Economics of Cybersecurity – An Introduction**
	Session Description: Security flaws are often due to perverse incentives rather than the lack of suitable technical protection mechanisms. Since individuals and companies do not bear the entire

	costs of cyber incidents, they do not tend to protect their system in the most efficient way. If they did support all the financial consequences, they would have stronger incentives to make their network more secure for the good of all interconnected networks. This session provides an introduction to the economics of cybersecurity and reviews some of the current leading thinking and research in this area.
10:15–10:30	**Coffee/Tea Break**
10:30–12:00	**Session 2: The Financial Aspects of Network Security: Malware and Spam**
	Session Description: The costs and revenues of all stakeholders across the value network of information services, such as software vendors, network operators, Internet Service Providers, and users are affected by malware and spam. These impacts may include, but are not limited to, the costs of preventative measures, the costs of remediation, the direct costs of bandwidth and equipment, and the opportunity costs of congestion. This is further complicated by the fact that spam and malware also create new revenue streams, both legitimate and illegitimate. They enable legitimate business models (e.g., anti-virus and anti-spam products, infrastructure, and bandwidth) as well as criminal business models (renting out of botnets, commissions on spam-induced sales, pump and dump stock schemes). Consequently, they create mixed, sometimes conflicting incentives for stakeholders, which complicate coherent responses to the problem. This session will explore the financial impacts of malware, and especially the economics of spam.
12:00–13:30	**Lunch**
13:30–14:45	**Session 3: The Botnet Economy**
	Session Description: Botnets (also called zombie armies or drone armies) are networks of compromised computers infected with viruses or malware to turn them into “zombies” or “robots” — computers that can be controlled without the owners’ knowledge. Criminals can use the collective computing power of these externally-controlled networks for malicious purposes and criminal activities, including, inter alia, generation of spam e-mails, launching of Distributed Denial of Service (DDoS) attacks (e.g., for blackmail purposes), alteration or destruction of data, and identity theft. An underground economy has sprung up around botnets, yielding significant revenues for authors of computer viruses, botnet controllers and criminals who commission this illegal activity by renting botnets. While many countries are investing a lot to deal with the problems related to malware and spam, some experts recommend countries to focus their attention on botnets in their fight against criminal online activities. This session seeks to explore the different motivators behind the botnet economy and elaborate on possible steps that countries can take to take down these botnets.
14:45–15:00	**Coffee/Tea Break**
15:00–16:30	**Session 4: Elaboration and Development of Indicators for Cybersecurity**
	Session Description: To gain an insight into the reliability of today’s ICT networks and the challenges they face (and ultimately whether any progress is being made in building confidence and security in the use of ICTs), one important requirement would be to benchmark different elements of cybersecurity (e.g. spam, viruses, phishing). This benchmarking can then be used for a more detailed analysis of cybersecurity trends, both at the level of geography (national, regional, and international) and in terms of the different threats. This session will look at the requirements behind and usefulness of a common set of metrics for cybersecurity.
16:30–17:00	**Seminar Wrap-Up and Conclusions**
	Session Description: The final session of the special seminar on the economics of cybersecurity will discuss and report on some of the main findings from the event. It will review some of the ongoing regional and international cooperation initiatives in order to encourage meeting participants to participate in further concrete actions that could be implemented in the region and internationally.

ITU REGIONAL CYBERSECURITY FORUM FOR ASIA-PACIFIC

WEDNESDAY 16 JULY 2008

08:00–09:00	**Meeting Registration**
09:00–10:15	**Meeting Opening and Welcome**
	Welcoming Address: Representative from Australia *Opening Remarks:* Representative from ITU *Presentation:* Setting the Stage — The Changing Cybersecurity Threat Environment
10:15–10:30	**Coffee/Tea Break**
10:30–12:00	**Session 1: Towards a Framework for Cybersecurity and Critical Information Infrastructure Protection**
	Session Description: The necessity of building confidence and security in the use of ICTs, promoting cybersecurity and protecting critical infrastructures at national levels is generally acknowledged. As national public and private actors bring their own perspective to the relevant importance of issues, in order to have a consistent approach, some countries have established cybersecurity/CIIP institutional framework structures while others have used a light-weight and non-institutional approach. This session will review, from a broad perspective, different approaches to such frameworks and their often similar components in order to provide meeting participants with a broad overview of the issues and challenges involved. The session will also present an overview of the ITU Management Framework for Organizing National Cybersecurity/CIIP Efforts and the ITU National Cybersecurity/CIIP Self Assessment Toolkit. The toolkit is intended to assist national governments in examining their existing national policies, procedures, norms, institutions, and relationships in light of national needs to enhance cybersecurity and address critical information infrastructure protection.
12:00–13:30	**Lunch**
13:30–15:15	**Session 2: Management Framework for Organizing National Cybersecurity/CIIP Efforts: Promoting a Culture of Cybersecurity**
	Session Description: In order to better understand the Management Framework for Organizing National Cybersecurity/CIIP Efforts and further explore how different countries are currently implementing the five pillars of the Framework, i.e. Promoting a Culture of Cybersecurity, Government — Industry Collaboration, Legal Foundation and Enforcement, Incident Management Capabilities, and Developing a National Cybersecurity Strategy, sessions 2, 3, 4, 5, and 6 are dedicated to the specific pillars and related country case studies. Session 2 looks closer at the building blocks needed to successfully Promote a Culture of Cybersecurity.
15:15–15:30	**Coffee/Tea Break**
15:30–17:00	**Session 3: Management Framework for Organizing National Cybersecurity/CIIP Efforts and Country Case Studies: Government—Industry Collaboration**
	Session Description: In order to better understand the Management Framework for Organizing National Cybersecurity/CIIP Efforts and further explore how different countries are currently implementing the five pillars of the Framework, i.e. Promoting a Culture of Cybersecurity, Government — Industry Collaboration, Legal Foundation and Enforcement, Incident Management Capabilities, and Developing a National Cybersecurity Strategy, sessions 2, 3, 4, 5, and 6 are dedicated to the specific pillars and related country case studies. Session 3 looks closer at Government — Industry Collaboration.
17:00–17:15	**Daily Wrap-Up and Announcements**
18:00–	**Welcome Reception (TBC)**

THURSDAY 17 JULY 2008	
09:00–10:30	**Session 4: Management Framework for Organizing National Cybersecurity/CIIP Efforts and Country Case Studies: Legal Foundation and Enforcement**
	Session Description: In order to better understand the Management Framework for Organizing National Cybersecurity/CIIP Efforts and further explore how different countries are currently implementing the five pillars of the Framework, i.e. Promoting a Culture of Cybersecurity, Government — Industry Collaboration, Legal Foundation and Enforcement, Incident Management Capabilities, and Developing a National Cybersecurity Strategy, sessions 2, 3, 4, 5, and 6 are dedicated to the specific pillars and related country case studies. Session 4 looks closer at the need for Legal Foundation and Enforcement.
10:30–10:45	Coffee/Tea Break
10:45–12:00	**Session 5: Management Framework for Organizing National Cybersecurity/CIIP Efforts and Country Case Studies: Incident Management Capabilities**
	Session Description: In order to better understand the Management Framework for Organizing National Cybersecurity/CIIP Efforts and further explore how different countries are currently implementing the five pillars of the Framework, i.e. Promoting a Culture of Cybersecurity, Government — Industry Collaboration, Legal Foundation and Enforcement, Incident Management Capabilities, and Developing a National Cybersecurity Strategy, sessions 2, 3, 4, 5, and 6 are dedicated to the specific pillars and related country case studies. Session 5 looks closer at developing Incident Management Capabilities.
12:00–13:30	Lunch
13:30–15:00	**Session 6: Management Framework for Organizing National Cybersecurity/CIIP Efforts and Country Case Studies: Developing a National Cybersecurity Strategy**
	Session Description: Increasingly, electronic networks are being used for criminal purposes, or for objectives that can harm the integrity of critical infrastructure and create barriers for extending the benefits of ICTs. To address these threats and protect infrastructures, each country needs a comprehensive action plan that addresses technical, legal and policy issues, combined with regional and international cooperation. What issues should be considered in a national strategy for cybersecurity and critical information infrastructure protection? Which actors should be involved? Are there examples of frameworks that can be adopted? This session seeks to explore in more detail various approaches, best practices, and the key building blocks that could assist countries in establishing national strategies for cybersecurity and CIIP.
15:00–15:15	Coffee/Tea Break
15:15–17:00	**Session 7: Review and Discussion: Management Framework for Organizing National Cybersecurity/CIIP Efforts**
	Session Description: Session 7 seeks to review and further discuss the Management Framework for Organizing National Cybersecurity/CIIP Efforts and related toolkit, identifying some of the main takeaways from the presentations on the Framework and the country case studies in preparation for the concluding meeting discussions.
17:00–17:15	Daily Wrap-Up and Announcements
18:00-	Social Event (TBC)

FRIDAY 18 JULY 2008	
09:00–10:30	**Session 8: Cybersecurity and Small Island Developing States (SIDS)**
	Session Description: SIDS and Pacific Island countries are faced with unique challenges posed by their small size and remoteness. This session will review some of the ongoing initiatives in the Pacific and would deliberate on the possible cooperation model.
10:30–10:45	**Coffee/Tea Break**
10:45–12:30	**Session 9: Cybersecurity and Small Island Developing States (SIDS) (Continued)**
	Session Description: SIDS and Pacific Island countries are faced with unique challenges posed by their small size and remoteness. This session will review some of the ongoing initiatives in the Pacific and would deliberate on the possible cooperation model.
12:30–14:00	**Lunch**
14:00–15:30	**Session 10: Regional and International Cooperation**
	Session Description: Regional and international cooperation is extremely important in fostering national efforts and in facilitating interactions and exchanges. This session will review some of the ongoing regional and international cooperation initiatives in order to inform meeting participants and to further these regional and international efforts.
15:30–15:45	**Coffee/Tea Break**
15:45–16:45	**Session 11: Wrap-Up, Recommendations and the Way Forward**
	Session Description: The final session of the meeting reports some of the main findings from the event, and aims to elaborate recommendations for future activities in order to enhance cybersecurity and increase protection of critical information infrastructures in the region.
16:45–17:00	**Meeting Closing**
	Closing remarks: Representative from Australia *Closing remarks:* Representative from ITU