International Telecommunication Union

المجلـــس الأعلـى للاتصـــالات وتكنولوجيـــا المعلومـــات
Supreme Council of Information & Communication Technology

ITU Regional Cybersecurity Forum 2008
Doha, Qatar

Document RWD/2008/02-E
20 February 2008
Original: English

ITU Regional Cybersecurity Forum Agreed Output[1]

18-20 February 2008

Doha, Qatar

An ITU Regional Cybersecurity Forum[2] was held 18-20 February 2008 in Doha, Qatar, in collaboration with the Qatar Supreme Council of Information and Communication Technology (ictQATAR) and Q-CERT. Over 80 representatives from 18 countries in the Arab region, experts from outside the region (e.g., Malaysia, USA), and representatives from key regional organizations including the League of Arab States (LAS), Gulf Cooperation Council (GCC), and United Nations Economic and Social Commission for Western Asia (UN-ESCWA), participated in the Forum.

During the three days of this event, cybersecurity and critical information infrastructure protection (CIIP) were examined within the context of the draft "ITU Cybersecurity Framework"[3] being developed in the ITU Development Sector's Study Group 1 Question 22/1. A number of interesting presentations on national experiences and regional initiatives (e.g., LAS, GCC, UN-ESCWA) addressing each element of the framework were discussed, including:

- Developing a National Strategy for Cybersecurity;
- Establishing National Government-Industry Collaboration;
- Deterring Cybercrime;
- Creating National Incident Management Capabilities; and
- Promoting a National Culture of Cybersecurity.

It was recognized that each of these elements form part of a comprehensive national approach to cybersecurity.

A related resource, the draft "ITU National Cybersecurity/CIIP Self-Assessment Toolkit"[4] was also examined. The toolkit is designed to assist national governments to review and understand their existing national approach, develop a baseline in terms of current "Best Practices", identify areas for attention, and prioritize national efforts to address cybersecurity.

The role of government in leading national cybersecurity efforts was discussed as well as the challenges faced within all governments to achieving the necessary actions. Discussions were held on the need to raise awareness among all participants, and of the need to tailor arguments to different audiences, whether they be political arguments to senior leaders, economic arguments to business, or personal safety arguments to individual users.

Discussions were held on the importance of including the private sector and other groups in the development of policy and law in this domain, and in the implementation and operation of a national cybersecurity strategy.

[1] More information about the forum can be found on event website at http://www.itu.int/ITU-D/cyb/events/2008/doha/
[2] The title of the event was "Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection (CIIP)" described at http://www.itu.int/ITU-D/cyb/events/2008/doha/.
[3] http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-draft-cybersecurity-framework.pdf
[4] http://www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html

Discussions were held on the importance of reviewing national cybercrime legislation to ensure it addresses threats in cyberspace and learned that the Convention on Cybercrime (Budapest, 2001) which offers an internationally developed basis for examining existing national cybercrime law and for determining what new substantive, procedural and mutual assistance provisions are needed in national cybercrime law.

Discussions were held on the importance of developing a national focal point for cyber incident management with the mission of watch, warning, investigation, response and recovery. Such a national focal point can serve to maintain collaboration within government, between the government and the private sector, and with international partners.

Discussions were held on the necessity of promoting a national culture of cybersecurity to ensure that all users, owners, and operators of information systems and networks know their responsibilities in regard to security and have the tools to take action appropriate to their roles.

Doha Declaration on Cybersecurity – ITU Regional Cybersecurity Forum

At the conclusion of this event, the participants agreed on the following outcomes:

- Recognized that improving cybersecurity is a global problem and that each country must undertake action to join and support international efforts to improve cybersecurity.
- Recognized the initiatives, actions and approaches that have worked in a number of countries and in other regions and the efforts of the ITU and other organizations to compile a set of "best practices" and develop tools which can support national efforts within the Arab region.
- Recognized that the ITU Cybersecurity/CIIP Framework offers a useful guide for raising awareness and initiating and/or reviewing national action as it helps to ensure consistency and compatibility of action among nations.
- Recommended that the ITU Cybersecurity/CIIP Framework and related resources and toolkits be finalized as soon as possible and made available in all ITU working languages, with particular attention to Arabic to support efforts in the region.
- Encouraged each country in the region to utilize the Framework and related ITU National Cybersecurity/CIIP Self-Assessment Toolkit as a means to develop their institutions, policies and relationships for cybersecurity and protecting critical information infrastructures.
- Recognized that some countries in the region may need support and assistance to implement the Framework and use the ITU National Cybersecurity/CIIP Self-Assessment Toolkit and requested that ITU-D consider ways to provide this support.
- Agreed that each country in the region should, if it has not already done so, develop an incident management capability (CSIRT/CERT) with national responsibility and use current examples and best practices of CSIRTs/CERTs in the region when developing national capabilities.
- Agreed that an important component of developing a national framework is joining regional and international efforts to promote a culture of cybersecurity.
- Emphasized the importance of developing regional cooperation initiatives and resources that can provide examples of best practices and training and education opportunities and develop models for capacity building that can be adapted to each country's needs in the region.
- Requested ITU-D in partnership with regional organizations and national administrations to undertake initiatives necessary to follow-up on the results of the meeting and to provide updates on progress and regional cooperation. In these follow-up initiatives, participation should be encouraged by additional participants identified in the Framework (e.g., all relevant ministries, business and other organizations).
- Expressed their appreciation to ictQATAR/Q-CERT and the ITU for their support and facilitation of the meeting.

****