BEST PRACTICES FOR ORGANIZING NATIONAL CYBERSECURITY EFFORTS

James G. Ennis
Rapporteur, ITU-D Q22/1 on Cybersecurity

ITU-D Q22: History

- Created by WTDC at its meeting in Doha in 2006
- Three meetings: September 2006, May 2007, and September 2007
- Next meeting: April 21-22, 2008 in Geneva

ITU-D Q22: Purpose

- To survey, catalogue, describe and raise awareness of :
  - The principal issues faced by national policy makers in building a culture of cybersecurity
  - The principal sources of information and assistance related to building a culture of cybersecurity
  - Successful best practices employed by national policy-makers to organize for cybersecurity
  - The unique challenges faced by developing countries
- To examine best practices for watch, warning, and incident response and recovery capabilities.

What is Cybersecurity?

- "Cybersecurity" is the prevention of damage to, unauthorized use of, exploitation of, and – if needed – the restoration of electronic information and communication systems, and the information they contain, in order to strengthen the confidentiality, integrity and availability of these systems.

Why is cybersecurity important?

- All critical sectors of a nation's economy today rely upon IP networks for transacting business, including energy, transportation, water, banking, agriculture and food, essential government services, etc.
- To achieve maximum economic benefit from the use of IP networks, they need to be reliable, secure, and trusted.
- Today, these networks, which were not originally designed with security in mind, face increasing threats from cyber attacks.

Five Keys to a Good National Cybersecurity Program

- A national strategy
- Collaboration between Government and Industry
- A sound legal foundation to deter cybercrime
- A national incident management capability
- A national awareness of the importance of cybersecurity

A National Strategy

- A government needs to understand the importance of cybersecurity for the national economy
- A national strategy should have an international component. Because cybersecurity is a global problem, national cybersecurity will only be achieved when international cybersecurity is achieved.

Collaboration between Government and Industry

- It is very important for governments to collaborate with industry in the cybersecurity area for a number of reasons:
  - Industry owns most of the IP network structure.
  - Industry has the expertise to find solutions to cyber incidents.
  - Industry is usually the first to be aware of a cyber attack or incident.
  - Industry knows what can and cannot be done.

A sound legal foundation to deter cybercrime

- Enact and enforce a comprehensive set of laws relating to cybersecurity and cybercrime consistent with the provisions of the 2001 Convention on Cybercrime
- The advantage to using the Cybercrime Convention as a starting point is one of flexibility. The Convention lays out specific principles and capabilities that each country should have without prescribing language. As a result, the Convention can be adapted to all legal systems.
- About 40 countries have either signed, or signed and ratified the Convention

National Incident Management Capability: Watch, Warning, Response & Recovery

- Governments need to develop a government-wide system to counter cyber attacks
- It is recommended that governments establish a focal point, often known as a "national computer security incident response team", or "N-CSIRT"
- A role for the focal point is information sharing
- Another role for the focal point is to develop procedures, security controls, and tools to protect government systems.

A national awareness of the importance of cybersecurity

- Many information system vulnerabilities exist because of a lack of cybersecurity awareness.
- Government needs to take a leadership role in creating a culture of cybersecurity awareness in their countries.
  - E-government
  - Education and training
  - Financial assistance & tax incentives
  - Research & Development
  - Guidance on privacy issues; secure collection & management of personal information
- International and regional forums generate additional ideas

Q22 Draft Report

- Annex A: Spam and Associated Threats
- Annex B: Identity Management

Q22

- Draft Report is available on ITU-D website at http://www.itu.int/md/D06-RGQ22.1-C/e/e if you have an ITU TIES account

- You are invited to participate in the next meeting of Q 22 and to contribute to the development of the draft report in order to improve its usefulness for national administrations