ITU Workshop on Frameworks for National Action: Cybersecurity and Critical Information Infrastructure Protection
Geneva, Switzerland - 17 September 2007

Document CYB-WS07/3-E
17 September 2007
Original: English

ITU NATIONAL CYBERSECURITY/CIIP SELF-ASSESSMENT TOOLKIT: BACKGROUND & APPROACH

Helping the world communicate

ITU National Cybersecurity/CIIP Self-Assessment Toolkit: Background & Approach

September 2007

Joe Richardson & Robert Shaw
<cybmail@itu.int>

ICT Applications and Cybersecurity Division
Policies and Strategies Department, BDT
International Telecommunication Union

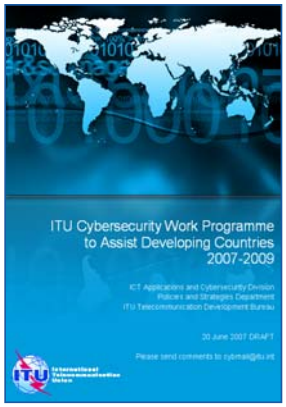
Helping the world communicate

ITU Development Sector Role

- ITU Resolution 130: Strengthening the role of ITU in building confidence and security in the use of information and communication technologies (Antalya, 2006);
- From World Telecommunication Development Conference (Doha, 2006):
  - Cybersecurity is priority in Programme 3 activities
  - ITU-D Study Group Question 22/1: Securing information and communication networks: Best practices for developing a culture of cybersecurity

ITU Cybersecurity Work Programme to Assist Developing Countries

- Most countries have not formulated or implemented strategies for cybersecurity and/or Critical Information Infrastructure Protection (CIIP)
- Work Programme scopes a set of high level assistance activities
- Also scopes detailed activities planned in the 2007-2009 period by the ITU Development Sector's ICT Applications and Cybersecurity Division
- Used to develop detailed operational plan for 2008-2009



www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-cybersecurity-work-programme-developing-countries.pdf

Cybersecurity Work Programme to Assist Developing Countries: High Level Elements

- Assistance related to Establishment of National Strategies and Capabilities for Cybersecurity and Critical Information Infrastructure Protection (CIIP)
- Assistance related to Establishment of appropriate Cybercrime Legislation and Enforcement Mechanisms
- Assistance related to establishment of Watch, Warning and Incident Response (WWIR) Capabilities
- Assistance related to Countering Spam and Related Threats
- Assistance in Bridging Security-Related Standardization Gap between Developing and Developed Countries
- Project on Enhancing Cybersecurity and Combatting Spam
- Establishment of an ITU Cybersecurity/CIIP Directory, Contact Database and Who's Who Publication
- Cybersecurity Indicators
- Fostering Regional Cooperation Activities
- Information Sharing and Supporting the ITU Cybersecurity Gateway
- Outreach and Promotion of Related Activities

Case Study: Activities Related to National Best Practices

ITU-D Study Question 22/1

- Q.22/1: Study Question adopted at World Telecommunication Development Conference (WTDC): Securing information and communication networks: best practices for developing a culture of cybersecurity
- Calls for Member States and Sector Members to create a report on best practices in the field of cybersecurity
- Four-year study cycle
- Pointer to Q.22/1 activities can be found at www.itu.int/ITU-D/cyb/cybersecurity/

ITU-D Q.22/1: 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

Q22.1 Draft Report (Sept 2007)

- 5 key elements to a good national cybersecurity programme:
  - A national strategy
  - A sound legal foundation to deter cybercrime
  - A national incident management capability
  - Collaboration between Government and Industry
  - A national awareness of the importance of a culture of cybersecurity

Self–Assessment Toolkit

- Based on Q.22/1 Framework Best Practice Documents
- Focused at national management and policy level
- Intended to assist national administrations to:
  - understand existing approach
  - compare to best practices
  - identify areas for attention
  - prioritize national efforts

Self-Assessment Toolkit cont'd

- Objective: assist nations to *organize* and *manage* national efforts to
  - *Prevent*
  - *Prepare for*
  - *Protect against*
  - *Respond to, and*
  - *Recover from* cybersecurity incidents

Self-Assessment Toolkit cont'd

- Looks at organizational issues for each element of the Framework
  - The people
  - The institutions
  - The relationships
  - The policies
  - The procedures

Considerations

- No nation starting at ZERO
- No single "right" answer or approach
- Continual review and revision necessary
- All "participants" must be involved
  - appropriate to their roles

Who are Participants?

- National "Participants" responsible for cybersecurity and/or CIIP:
  - "Governments, businesses, other organizations and individual users who develop, own, provide, manage, service and use information systems and networks"
    - UNGA Resolution 57/239 Creation of a global culture of cybersecurity

Self-Assessment Toolkit cont'd

- Examines management and policy level for each element of Framework
  - National Strategy
  - Deterring Cybercrime
  - National Incident Management Capabilities
  - Government-Private Sector Collaboration
  - Culture of Cybersecurity

National Pilot Tests

- Vietnam (2007)
- Latin America Country (2007)
- Ghana (2007)

- To express interest in participating in national pilot tests of the toolkit, please contact cybmail@itu.int

More Information

- ITU-D ICT Applications and Cybersecurity Division
  - www.itu.int/itu-d/cyb/
- ITU National Cybersecurity/CIIP Self-Assessment Toolkit: Background & Approach
  - www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-cybersecurity-national-self-assessment-toolkit.pdf
- Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection
  - www.itu.int/ITU-D/cyb/events/
- Botnet Mitigation Toolkit
  - www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-botnet-mitigation-toolkit.pdf
- Cybersecurity Publications
  - www.itu.int/ITU-D/cyb/publications/

International Telecommunication Union

Helping the World Communicate