ITU National Cybersecurity Framework – Overview

ITU Regional Cybersecurity Forum for Eastern and Southern Africa

Lusaka, Zambia
25–28 August 2008

Joseph Richardson
Joseph.Richardson@ties.itu.int
for
ICT Applications and Cybersecurity Division
Policies and Strategies Department
ITU Telecommunication Development Bureau

This Presentation

- Introduce the ITU National Cybersecurity Framework
- Identify Issues for Implementing the Framework Nationally
- Introduce the ITU Self–Assessment Toolkit

This Presentation

Based on:

Study Group Q 22/1: Report on Best Practices for a National Approach to Cybersecurity: A Management Framework for Organizing National Cybersecurity Efforts

Why a Framework?

- Why is a National Strategy needed?
- Cybersecurity/Critical Information Infrastructure Protection (CIIP) is a SHARED responsibility
- All “participants” must be involved
  - Appropriate to their roles

Participants

- "Participants" responsible for cybersecurity:
  - *"Government, business, other organizations, and individual users who develop, own, provide, manage, service and use information systems and networks"*
    - From "UNGA Resolution 57/239 Creation of a global culture of cybersecurity"

ITU Framework for National Action

Framework for Action

- For each of these five elements, the Framework recommends:
  - POLICY: to guide national efforts
  - GOALS: to implement the policy
  - SPECIFIC STEPS: to achieve goals

Framework for National Cybersecurity Efforts

	National Strategy	Government-Industry Collaboration	Deterring Cybercrime	Incident Management Capabilities	Culture of Cybersecurity
Policies	Developing and implementing a national cybersecurity plan requires a comprehensive strategy that includes an initial broad review of the adequacy of current national practices and consideration of the role of all stakeholders (government authorities, industry, and citizens) in the process.	Protecting critical information infrastructure and cyberspace is a shared responsibility that can best be accomplished through collaboration between government at all levels and the private sector, which owns and operates much of the infrastructure. It is important to recognize that although the world's information security systems have largely become an interoperable and interconnected whole, the structure of this network can vary greatly from country to country. Therefore, an effective and sustainable system of security will be enhanced by collaboration among owners and operators of these systems.	Cybersecurity can be greatly improved through the establishment and modernization of criminal law, procedures, and policy to prevent, deter, respond to, and prosecute cybercrime.	It is important to maintain a national organization to serve as a focal point for securing cyberspace and the protection of critical information infrastructure, whose national mission includes watch, warning, response and recovery efforts and the facilitation of collaboration between government entities, industry, academia, and the international community.	Considering that personal computers are becoming ever more powerful, that technologies are converging, that the use of ICTs is becoming more and more widespread, and that connections across national borders are increasing, all participants who develop, own, provide, manage, service and use information networks must understand cybersecurity issues and take action appropriate to their roles to protect networks. Government must take a leadership role in bringing about this Culture of Cybersecurity and in supporting the efforts of other participants.
Goals	I.A.1. Create awareness at a national policy level about cybersecurity issues and the need for national action and international cooperation. I.A.2. Develop a national strategy to enhance cybersecurity to reduce the risks and effects of both cyber and physical disruptions. I.A.3. Participate in international efforts to promote national prevention of, preparation for, response to, and recovery from incidents.	II.A.1. Develop government-industry collaborative relationships that work to effectively manage cyber risk and to protect cyberspace. II.A.2. Provide a mechanism for bringing a variety of perspectives, equities, and knowledge together to reach consensus and move forward together to enhance security at a national level.	III.A.1. Enact and enforce a comprehensive set of laws relating to cybersecurity and cybercrime consistent with the provisions of the Convention on Cybercrime (2001).	IV.A.1. Develop a coordinated national cyberspace security response system to prevent, detect, deter, respond to, and recover from cyber incidents. IV.A.2. Establish a focal point for managing cyber incidents that bring together critical elements from government (including law enforcement) and essential elements from infrastructure operators and vendors to reduce both the risk and severity of incidents. IV.A.3. Participate in watch, warning, and incident response information sharing mechanisms. IV.A.4. Develop, test, and exercise emergency response plans, procedures, and protocols to ensure that government and non-government collaborators can build trust and coordinate effectively in a crisis.	V.A.1. Promote a national Culture of Security consistent with UNGA Resolutions 57/239, Creation of a global culture of cybersecurity, and 58/199, Creation of a global culture of cybersecurity and the protection of critical information infrastructures.
Steps	I.B.1. Persuade national leaders in the government of the need for national action to address threats to and vulnerabilities of the national cyber infrastructure through policy-level discussions. I.B.2. Identify a lead person and institution for the overall national effort; determine where within the government a Computer Security Incident Response Team with national responsibility should be established; and identify lead institutions for each aspect of the national strategy. I.B.3. Identify the appropriate experts and policymakers within government ministries, government, and private sector, and their roles. I.B.4. Identify cooperative arrangements for and among all participants. I.B.5. Establish mechanisms for cooperation among government and private sector entities at the national level. I.B.6. Identify international expert counterparts and foster international efforts to address cybersecurity issues, including information sharing and assistance efforts. I.B.7. Establish an integrated risk management process for identifying and prioritizing protective efforts regarding cybersecurity. I.B.8. Assess and periodically reassess the current state of cybersecurity efforts and develop program priorities. I.B.9. Identify training requirements and how to achieve them.	II.B.1. Include industry perspectives in the earliest stages of development and implementation of security policy and related efforts. II.B.2. Encourage development of private sector groups from different critical infrastructure industries to address common security interests collaboratively with government. II.B.3. Bring private sector groups and government together in trusted forums to address common cybersecurity challenges. II.B.4. Encourage cooperation among groups from interdependent industries. II.B.5. Establish cooperative arrangements between government and the private sector for incident management.	III.B.1. Assess the current legal authorities for adequacy. A country should review its criminal code to determine if it is adequate to address current (and future) problems. III.B.2. Draft and adopt substantive, procedural and mutual assistance laws and policies to address computer-related crime. III.B.3. Establish or identify national cybercrime units. III.B.4. Develop cooperative relationships with other elements of the national cybersecurity infrastructure and the private sector. III.B.5. Develop an understanding among prosecutors, judges, and legislators of cybercrime issues. III.B.6. Participate in the 24/7 Cybercrime Point of Contact Network.	IV.B.1. Identify or establish a national CSIRT (N-CSIRT) capability. IV.B.2. Establish mechanism(s) within government for coordination among civilian and government agencies. IV.B.3. Establish collaborative relationships with industry to prepare for, detect, respond to, and recover from national cyber incidents. IV.B.4. Establish point(s) of contact within government agencies, industry and international partners to facilitate consultation, cooperation, and information exchange with the N-CSIRT. IV.B.5. Participate in international cooperative and information sharing activities. IV.B.6. Develop tools and procedures for the protection of the cyber resources of government entities. IV.B.7. Develop a capability through the N-CSIRT for coordination of governmental operations to respond to and recover from large-scale cyber attacks. IV.B.8. Promote responsible disclosure practices to protect operations and the integrity of the cyber infrastructure.	V.B.1. Implement a cybersecurity plan for government-operated systems. V.B.2. Implement security awareness programs and initiatives for users of systems and networks. V.B.3. Encourage the development of a culture of security in business enterprises. V.B.4. Support outreach to civil society with special attention to the needs of children and individual users. V.B.5. Promote a comprehensive national awareness program so that all participants—businesses, the general workforce, and the general population—secure their own parts of cyberspace. V.B.6. Enhance Science and Technology (S&T) and Research and Development (R&D) activities. V.B.7. Review existing privacy regime and update it to the online environment. V.B.8. Develop awareness of cyber risks and available solutions.

International Telecommunication Union

Implementing the Framework Nationally

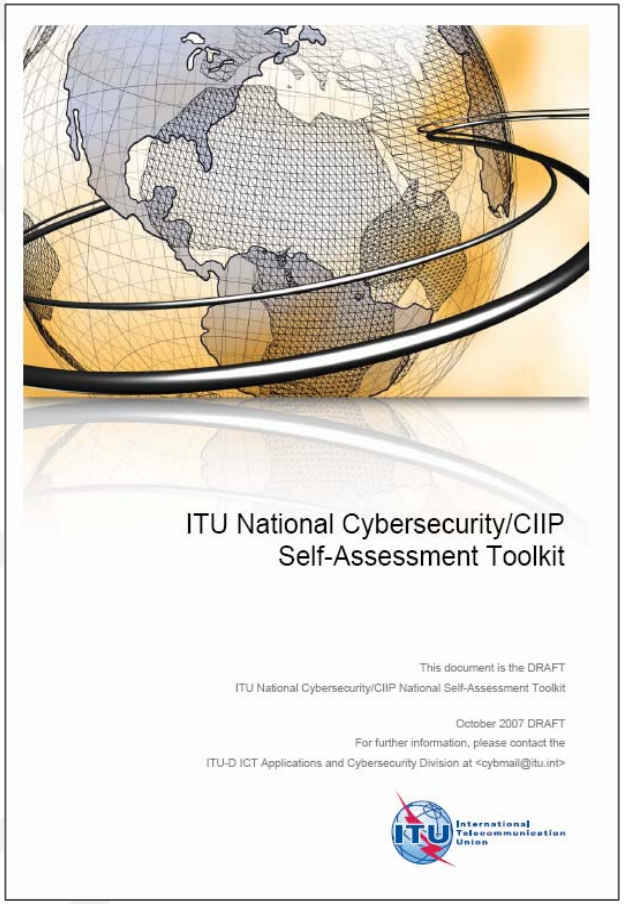
- Actions by Government
- Collaboration by other participants

Government Actions

- Provide leadership, guidance and coordination
  - Identify lead persons and institutions
  - Develop CSIRT with national responsibility
  - Identify cooperative arrangements and mechanisms among all participants
  - Identify international counterparts and relationships
  - Identify experts
  - Establish integrated risk management process
  - Assess and periodically reassess cybersecurity
  - Identify training requirements

ITU National Cybersecurity/CIIP Self–Assessment Toolkit

- Intended to assist national authorities to review their domestic situation related to goals and actions identified in:
  - Study Group Q 22/1: Report on Best Practices for a National Approach to Cybersecurity: A Management Framework for Organizing National Cybersecurity Efforts
- Adapted from work in APEC-TEL



ITU Self–Assessment Toolkit

- Focus: national management and policy level
- Intended to assist national governments:
  - Understand existing national approach
  - Develop “baseline” re Best Practices
  - Identify areas for attention
  - Prioritize national efforts

Considerations

- No nation starting at ZERO
- No “right” answer or approach
- Continual review and revision needed
- All “participants” must be involved
  - appropriate to their roles

The Self-Assessment Toolkit

- Examines each element of Framework at management and policy level:
  - National Strategy
  - Government - Industry Collaboration
  - Deterring Cybercrime
  - National Incident Management Capabilities
  - Culture of Cybersecurity

The Self-Assessment Toolkit

- Looks at organizational issues for each element of Framework:
  - The people
  - The institutions
  - The relationships
  - The policies
  - The procedures
  - The budget and resources

The Self-Assessment Toolkit

- Identifies issues and poses questions:
  - What Actions have been taken?
  - What Actions are planned?
  - What Actions are to be considered?
  - What is the Status of these actions?

The Framework and ITU National Self-Assessment Toolkit

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

Next Steps

- What are the next steps
  - for your nation?
  - for your region?

International Telecommunication Union

Committed to connecting the world