A National Approach to Cybersecurity

ITU Regional Cybersecurity Forum for Europe and CIS
Sofia, Bulgaria
7-9 October 2008

Joseph Richardson
Joseph.Richardson@ties.itu.int
for
ICT Applications and Cybersecurity Division
Policies and Strategies Department, ITU-D
This Presentation

- Introduces the National Approach to Cybersecurity
- Identifies Issues for Implementing the National Approach
- Introduces the ITU National Cybersecurity/CIIP Self-Assessment Tool
National Approach

Why is a National Approach Needed?

- Cybersecurity and 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”
Elements of National Approach

- National Strategy
- Culture of Cybersecurity
- Public-Private Collaboration
- Incident Management Capabilities
- Deterring Cybercrime
Action Requirements

- For each of these five elements:
  
  - POLICY: to guide national efforts
  - GOALS: to implement the policy
  - SPECIFIC STEPS: to achieve goals
Implementing the National Approach

- Actions required of Government
- Collaboration among participants
Actions for Government

- 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 Tool

- Intended to assist national authorities review their domestic situation in context of policies, goals and actions identified in National Approach

http://www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html
National Cybersecurity/CIIP Self-Assessment

- Focused at national management and policy level
- Intended to assist national governments:
  - Understand existing national approach
  - Develop “baseline” report on best practices
  - Identify areas for attention
  - Prioritize national efforts
Considerations for Using Self-Assessment

- 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

- Examines each **Element** at management and policy level:
  - National Strategy
  - Public-Private Sector Collaboration
  - Deterring Cybercrime
  - National Incident Management Capabilities
  - Culture of Cybersecurity
The Self-Assessment

- Looks at organizational issues for each **Element**:
  - The people
  - The institutions
  - The relationships
  - The policies
  - The procedures
  - The budget and resources
The Self-Assessment

- 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 National Approach and Self-Assessment Tool

Objective: assist nations organize and manage national efforts to

- Prevent
- Prepare for
- Protect against
- Respond to, and
- Recover from cybersecurity incidents.
National Approach to Cybersecurity

- What are the next steps
  - for your nation?
  - for your region?
International Telecommunication Union

Committed to connecting the world