Management Framework
for Organizing National Cybersecurity Efforts:

National Strategy
&
Self-assessment tool

Prepared by
Joseph P. Richardson

Why a National Strategy?

- Cybersecurity 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.

“UNGA Resolution 57/239 Creation of a global culture of cybersecurity”

Goals of National Strategy

- Create awareness
  - of need for national action
  - of need for international cooperation
- Reduce risk and effects of disruptions
- Provide basis for cooperation
  - among parties responsible to prevent, prepare for, respond to and recover from incidents

Steps to National Strategy

- Commitment to policy development
  - Recognize importance of CII
  - Identify risk
  - Establish cybersecurity policy goal(s)
  - Identify implementation approach
- Identify roles, responsibilities and relationships
- Define processes and mechanisms for cooperation

Government Actions

- Provide leadership, guidance and coordination for national effort and international cooperation
  - Identify lead person and institution for national strategy
  - Identify lead persons and institutions for each element of national strategy
  - Develop computer security incident response team with national responsibility (N-CSIRT)
  - Identify cooperative arrangements and mechanisms for cooperation among all participants

Government Actions

- Provide leadership, guidance and coordination for national effort and international cooperation (continued)
  - Identify international counterparts and relationships
  - Identify experts
  - Establish integrated risk management process
  - Assess and periodically reassess cybersecurity
  - Identify training requirements

Getting Started on a National Strategy

- Cybersecurity Self–Assessment Tool

Self – Assessment Tool

- Based on *Best Practices* document
- Focused at 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 Tool

- 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 Tool

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

The 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 Pilot Tests

- ITU-D is sponsoring pilot tests of the self-assessment tool
  - Vietnam (August 2007)
  - Argentina (2007)
  - Ghana (2007)
  - 2008 – to be determined
- For information on pilot test program
  - contact cybmail@itu.int

ITU
Self-Assessment Toolkit

- Additional and updated information at

  http://www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html

Management Framework for Organizing National Cybersecurity Efforts:

National Strategy

Prepared by
Joseph P. Richardson
Joseph.richardson@ties.itu.int
202-258-9278