Fundamentals of Cybersecurity/CIIP

Building Capacity:

Using a National Strategy and Self-Assessment

Presented to:

2009 ITU Regional Cybersecurity Forum for Americas

"Connecting the World Responsibly"

23-25 November 2009

Santo Domingo, Dominican Republic

Presenter: Joseph Richardson

CTP, Inc.

Developing a National Cybersecurity Strategy

Getting Started: The ITU National Cybersecurity/CIIP Self-Assessment Tool:

Part 1: Cybersecurity/CIIP in the National Agenda

Part 2: Key Components to be Addressed

Part 3: The Statement – A National Cybersecurity/CIIP Strategy

Preliminary Considerations

1. Target audience and their level of awareness
   - Government leaders (executive and legislative)
   - Business and industry
   - Other organizations and institutions
   - Individuals and the general public
2. Significant decisions already taken
   - What authorities are in place?
   - Who has taken action?
   - What actions have been taken?

Preliminary Considerations

Who prepares the strategy?

Drafters from government

- Entity with authority to lead effort
- Entities with lead responsibility for the different building blocks
  - Government-private sector collaboration
  - Incident management
  - Legal infrastructure
  - Capacity building and developing a culture of security

Preliminary Considerations

Who prepares the strategy?

Advisors from government

- National security
- Critical infrastructures
- Democratic and ethical principles
- Other

Preliminary Considerations

Who prepares the strategy?

Advisors from private sector

- Industry associations from
  - CII and ICTs
  - Critical infrastructures
  - Business and economic
- Key companies
- Civil society
- Other significant voices

Cybersecurity/CIIP in the National Agenda

The Case for National Action

1. Role of ICTs in the nation
   a. In the national economy
   b. In national security
   c. For national critical infrastructures
   d. For national social interactions

Cybersecurity/CIIP in the National Agenda

The Case for National Action

2. Risks and ICTs in the nation:
   a. Vulnerabilities of ICT use
   b. Threats via ICTs
   c. Risks to be managed:
      - The national economy
      - National security
      - Critical infrastructure
      - Social interaction

Cybersecurity/CIIP in the National Agenda

The Case for National Action

3. The place of cybersecurity/CIIP in other national goals and objectives
   - Economic, National security, Critical infrastructure protection, Social and Other

4. Policy on cybersecurity/CIIP
   - Goals
   - Implementation

Cybersecurity/CIIP in the National Agenda

Participants in the National Response

1. Government:
   - Identify each entity
   - Its roles
   - Point of contact
2. Private sector
   - Identify each relevant entity
   - Describe roles
   - Identify point of contact

Cybersecurity/CIIP in the National Agenda

Organizing for Cybersecurity/CIIP

1. Identify Government leads
2. Review existing forum/structures
   a. Policy development
   b. Operations
3. For each forum/structure, identify
   - Role
   - Government lead
   - Participants (government and private sector)
   - Whether it is a trusted forum
   - Assess adequacy

Initial Building Blocks of a National Strategy

Key Building Blocks in National Strategy

1. Government-Private Sector Collaboration

1. Private sector input in policy development
2. Operational forums
   a. For information sharing and incident management
   b. Trusted forums
   c. Industry sector groups
   d. Interdependent critical industry sector groupings
3. For each forum, identify
   - Objectives
   - Government role
   - Participants (government and private sector)
   - How it operates
   - Assess for adequacy

Key Building Blocks in National Strategy

2. Incident Management

- Coordinator for Incident Management (CIM) -- CIRT with national responsibility
- Roles and responsibilities; access to CIRT services
- Cooperating government agencies (points of contact)
- Cooperating private sector partners (points of contact)
- Mechanisms for receiving advice on policy from private sector
- Mechanisms for information sharing on operations
- Protection of government operated systems
- Protection of national cyber resources
- Integrated risk management
- Funding

Key Building Blocks in National Strategy

3. Legal Measures

1. Review and update legal authorities, including;
    - Cybercrime, Privacy, Data protection, Commercial law, Digital signatures, Encryption, Others

2. Management Issues
    - Identify lead ministries for each
    - Ensure outreach and awareness among participants, including the judiciary and legislative branches

3. Operational Issues
    - Identify and train cybercrime enforcement offices
    - Cooperative arrangements with CIRT, private sector
    - Participate in international cooperative arrangements

Key Building Blocks in National Strategy

4. Capacity Building and Culture of Cybersecurity

- Security for government-operated systems
- National awareness program for all participants
- Outreach to users, including children
- Enhance science and technology (S&T) and research and development (R&D)
- Training requirements
- Other initiatives

Drafting a National Cybersecurity/CIIP Strategy

Prepare the National Strategy:

- **Review responses on self-assessment to prepare**
- **Policy on cybersecurity/CIIP**
- **Case for action**
- **Goals, objectives and means to achieve for each key element**
- **Other considerations**
  - Budget and financing
  - Implementation timeframe and milestones
  - Review and reassessment

Output of the Effort

- Summary of key findings from national self-assessment
  - Input from all participants
- Program of Actions and Recommendations
  - Promulgated at a level to ensure action by all participants

Conclusion

The ITU National Cybersecurity/CIIP Self–Assessment Tool and Best Practices document can assist governments to:

- Understand existing national approach
- Develop “baseline” on best practices
- Identify areas for attention
- Prioritize, coordinate and manage national efforts
- Get all participants involved
  - Appropriate to their roles.

- Using regional and international norms facilitates necessary cross border cooperation

Questions?

Thank You

Joseph Richardson
CTP, Inc.
300 N Lee St, 3rd floor
Alexandria, VA 22314
USA