Fundamentals of Cybersecurity/CIIP

Building Capacity:

Using a National Strategy & Self-Assessment

Presented to:

2009 ITU Regional Cybersecurity Forum for Asia-Pacific

"Connecting the World Responsibly"

23-25 September 2009

Hyderabad, India

Presenter: Joseph Richardson

CTP, Inc.

Developing a National Cybersecurity Strategy

Getting Started

Part 1: The Cybersecurity Self-Assessment

Part 2: The Statement – A National Cybersecurity Strategy

The Cybersecurity Self-Assessment

- **The Audience**
  - The target audience for National Cybersecurity Strategy
    - Government leaders (executive and legislative)
    - Business and industry
    - Other organizations and institutions
    - Individuals and the general public

The Cybersecurity Self-Assessment

- **The Audience**

  - Level of awareness and response
    - How aware are participants of cybersecurity issues?
    - What authorities are in place?
    - Who has taken action?
    - What actions have been taken?

  - Significant decisions already taken in regard to cybersecurity

The Cybersecurity Self-Assessment

- **The Case for Action**
  - Role of ICTs in the nation
    - The national economy
    - The national security
    - For national critical infrastructures
    - For national social interactions

The Cybersecurity Self-Assessment

- **The Case for Action**
  - Risks associated with ICTs
    - Vulnerabilities of ICTs
    - Threats from ICT use

The Cybersecurity Self-Assessment

- **The Case for Action**
  - Risks to be managed
    - The national economy
    - The national security
    - National critical infrastructures
    - National social interaction

The Cybersecurity Self-Assessment

- **The Case for Action**
  - Other national goals and objectives: the stage for Cybersecurity
    - Economic
    - National security
    - Critical infrastructure protection
    - Social
    - Other

The Cybersecurity Self-Assessment

- **Collaboration and Information exchange**
  - Government with Industry and other participants
    - For policy development
      - Existing mechanisms
      - Improvements needed?
    - For information sharing and operational matters
      - Existing mechanisms
      - Improvements needed?
    - For Trusted forums
      - Existing mechanisms
      - Improvements needed?

The Cybersecurity Self-Assessment

- **Collaboration and Information exchange**
  - Industry with Industry
    - Existing mechanisms
      - Within same industry
      - Among interconnected critical industries
      - Role of government in each mechanism
    - Improvements needed?

The Cybersecurity Self-Assessment

- **Incident Management**
  - Management Issues:
    - Identify **Coordinator for Incident Management (CIM)**
    - Identify roles and responsibilities of CIM
    - Identify cooperating government agencies (and points of contact for each)
    - Identify cooperating partners from other national and international participants (and points of contact for each)
    - Identify mechanisms for receiving advice from other participants on policy development
    - Identify mechanisms for information sharing and cooperation with key participants on incident management (operations)

The Cybersecurity Self-Assessment

- **Incident Management**

  - Operational and policy issues, including;
    - CSIRT with national responsibility (N-CSIRT)
    - Ensure a full range of CSIRT services are available
    - Protection plan for government operated systems
    - Tools and procedures for cybersecurity and the protection of national cyber resources
    - Integrated risk management

The Cybersecurity Self-Assessment

- **Legal Framework**
  - Policy Issues: Review and update legal authorities, including;
    - Cybercrime
    - Privacy
    - Data protection
    - Commercial law
    - Digital signatures
    - Encryption
    - Others

The Cybersecurity Self-Assessment

- **Legal Framework**

  - Management Issues
    - Identify lead ministries for reviews and update
    - Ensure outreach and awareness among participants, including in particular the judiciary and legislative branches

The Cybersecurity Self-Assessment

- **Legal Framework**

  - Operational Issues
    - Identify and train cybercrime enforcement offices
    - Ensure cooperative arrangements with N-CSIRT, international counterparts and other national participants
    - Participate in international cooperative arrangements

The Cybersecurity Self-Assessment

- **Culture of Security**
  - Develop security awareness programs for and outreach to all participants, for example, children, small business, etc.
  - Enhance science and technology (S&T) and research and development (R&D)
  - Other initiatives

The Cybersecurity Self-Assessment

- **Other considerations**
  - Budget and financing
  - Implementation timeframe and milestones
  - Review and reassessment

A National Cybersecurity Strategy

Part 2:

The Statement

A National Cybersecurity Strategy

- **Policy (goals) on cybersecurity**
- **Case for action**
  - Role of ICTs in nation
  - Risk to be managed
- **Relationship to other national goals and objectives**

A National Cybersecurity Strategy

- **Security initiatives and actions to be undertaken**
  - Collaboration and information exchange
    - Leadership, key participants and assignment of roles
    - Policy development mechanisms
    - Information sharing and operational mechanisms
    - Trusted forums and their operations
    - Industry to industry cooperation, including among interdependent critical industries

A National Cybersecurity Strategy

- **Security initiatives and actions to be undertaken**

  - Incident Management
    - Coordinator for Incident Management (CIM)
    - Roles and responsibilities of CIM
    - Establish CSIRT with national responsibilities (N-CSIRT)
    - Obtain CSIRT services
    - Key cooperating participants and roles
    - Protection for government operated systems
    - Proposals for protection of national cyber resources
    - Integrated risk management

A National Cybersecurity Strategy

- **Security initiatives and actions to be undertaken**
  - Legal Framework
    - Legal authorities for review and update
    - Lead ministries
    - For cybercrime – enforcement initiatives
    - International cooperation

A National Cybersecurity Strategy

- **Security initiatives and actions to be undertaken**
  - Culture of Security
    - Awareness and outreach programs
    - S&T and R&D
    - Other considerations

A National Cybersecurity Strategy

- **Other considerations**
  - Budget and financing
  - Implementation timeframes
  - Review and reassessment plans

Output of the Self-Assessment: A National Cybersecurity Strategy

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

Conclusion

The National Cybersecurity/CIIP Self–Assessment and Strategy 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