Fundamentals of Cybersecurity/CIIP

The Role of a National Cybersecurity Strategy and National Self-Assessment

Presented to:

2009 ITU Regional Cybersecurity Forum for Americas

"Connecting the World Responsibly"

23-25 November 2009

Santo Domingo, Dominican Republic

Joseph Richardson

CTP, Inc.

Objectives of this Presentation

- Provide an Overview of the Problem
- Perspectives on Participants and Leadership
- Outline a National Response
  - self-assessment leading to
  - a national strategy

Why Worry About Cybersecurity/CIIP?

- Nation is dependent on ICTs
  - Economic wellbeing
  - National security
  - Social cohesion
- Risk is inherent in ICT use
  - Vulnerabilities
  - Threats
  - Interdependences
- Conclusion: Action is required

Who Must Take Action?

We reaffirm the necessity to further promote, develop and implement in cooperation with all stakeholders a global culture of cybersecurity…

This culture requires national action and increased international cooperation to strengthen security while enhancing the protection of personal information, privacy and data

WSIS TUNIS AGENDA FOR THE INFORMATION SOCIETY

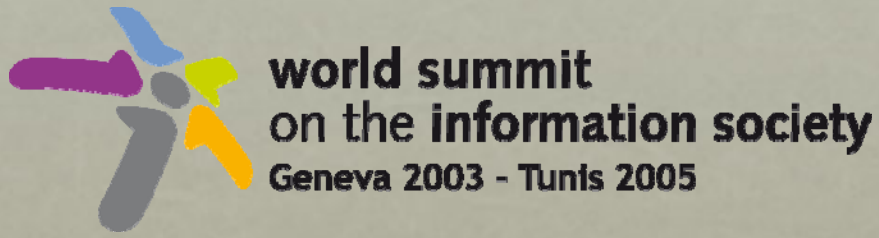
A global culture of cybersecurity requires the engagement of all stakeholders, and imply the establishment of national cybersecurity strategies within the framework of international principles.

ITU and Cybersecurity

- ITU constitutes a unique global forum to discuss cybersecurity.
- The **ITU Secretary-General has set cybersecurity as a top priority**.
- **ITU Membership has been calling for a greater role to be played by ITU** in matters relating to cybersecurity through a number of Resolutions, Decisions, Programs and Recommendations.

- ITU provides a global perspective and expertise and is promoting cybersecurity through a range of activities.

ITU Global Framework for Cybersecurity



At the World Summit on the Information Society (WSIS) in 2005, ITU was entrusted by leaders of the international community to act as the facilitator for

WSIS Action Line C5: "Building confidence and security in the use of ICTs"

ITU Global Cybersecurity Agenda

"Building confidence and security in the use of ICTs"

In 2007, ITU Secretary-General launched the **Global Cybersecurity Agenda**, an international framework for collaboration on Cybersecurity matters that addresses **five main areas**:

1. **Legal Measures**
2. **Technical and Procedural Measures**
3. **Organizational Structure**
4. **Capacity Building**
5. **International Cooperation**

What Action must Stakeholders Take?

- Actions appropriate to their roles
- Cybersecurity/CIIP is a SHARED responsibility
- All “participants” must be involved

- **Government has responsibility to lead**

Where is Government to Start?

Identify:

Best Practices

Conduct:

Self Assessment

Develop:

National Strategy

Sources of Best Practices

National Efforts:

International and Regional Efforts:

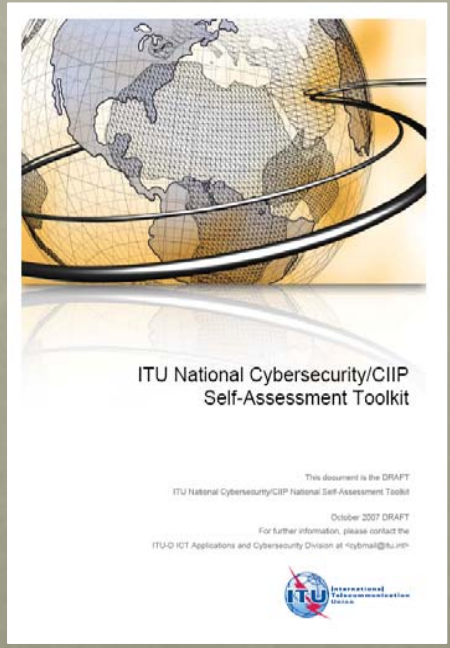
- ITU Global Cybersecurity Agenda (GCA)
- United Nations General Assembly (UNGA)
  - Resolutions (57/239 & 58/199)
- Organization for Economic Cooperation and Development (OECD)
- G8
- Council of Europe (CoE)
- Asia Pacific Economic Cooperation (APEC)
- Organization of American States (OAS)
- World Summit on the Information Society (WSIS)
- Etc.

Sources of Best Practices: ITU Efforts

The ITU Global Cybersecurity Agenda (GCA) is the reference model, from which a national strategy can be built, since in line with the international cooperation principles.

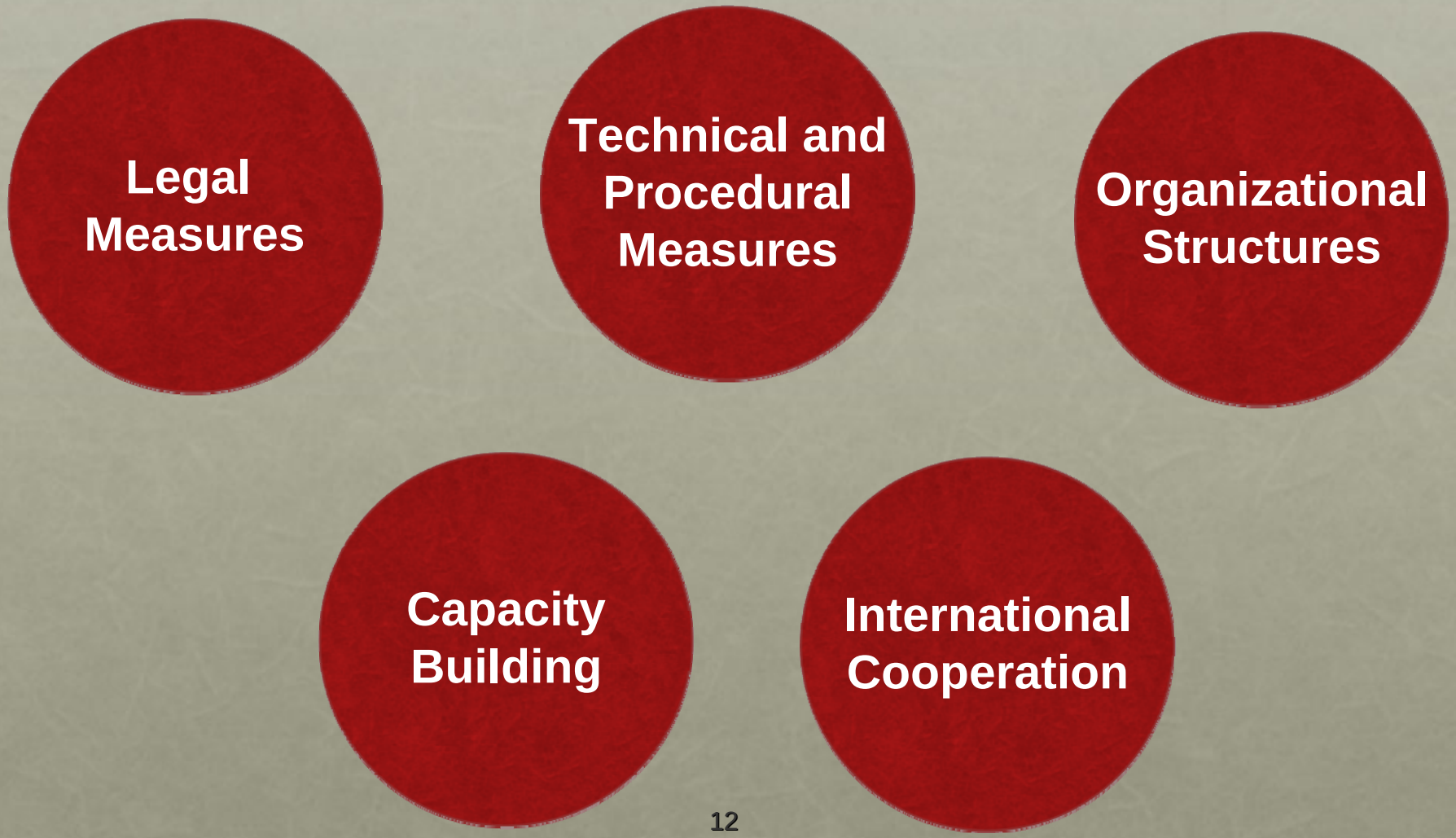
Other elements:

- Reference material and training resources, toolkits and guidelines
- Targeted workshops and events
- ITU-D Study Group Q 22/1
- ITU-T Study Group 17
- ITU National Cybersecurity/CIIP Self-Assessment Tool



See website for more information: www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html

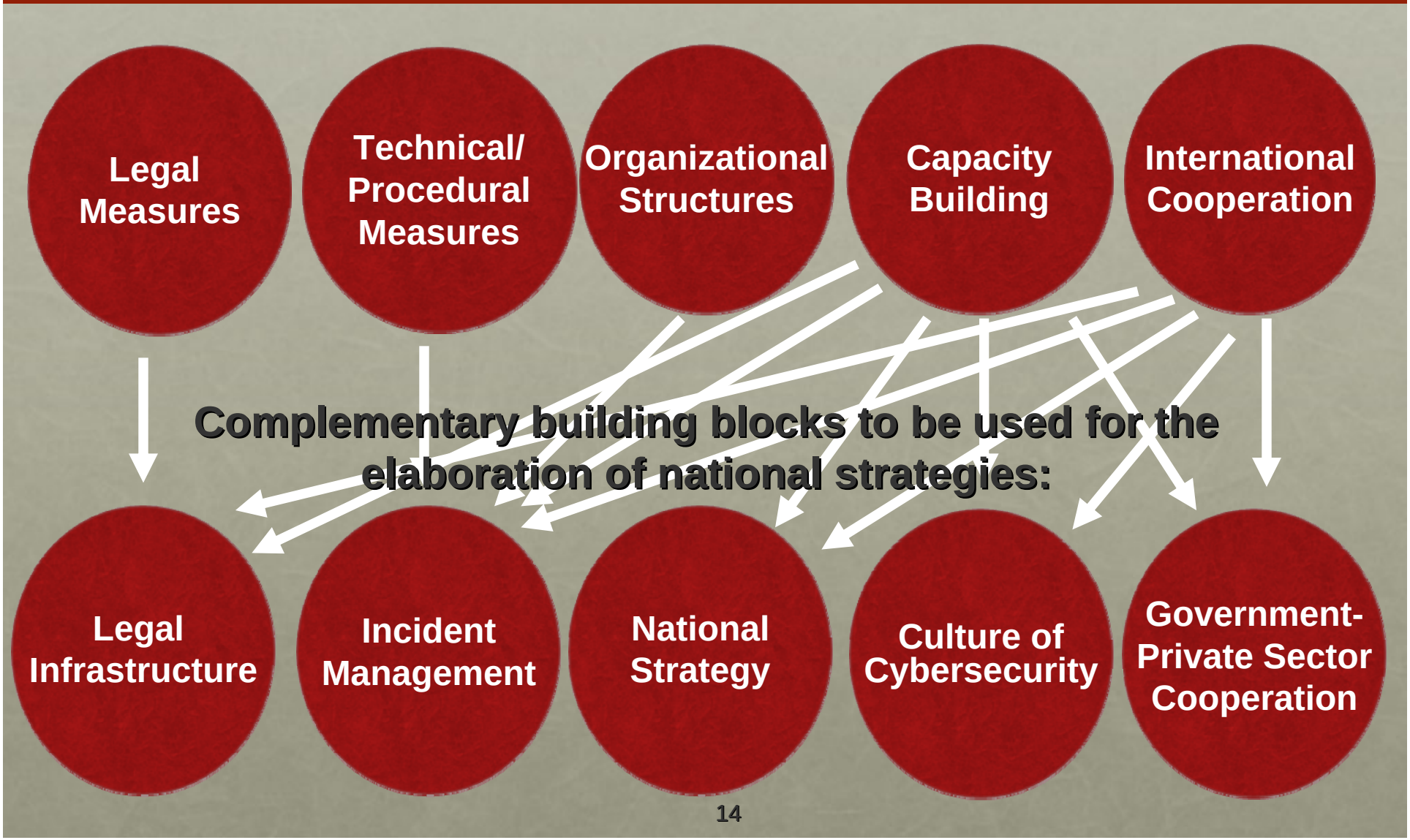
The Five Pillars of the ITU Global Cybersecurity Agenda



The five pillars of the GCA ITU Global Cybersecurity Agenda:

Complementary building blocks to be used for the elaboration of national strategies:

The five pillars of the GCA ITU Global Cybersecurity Agenda:



For Each Pillar

What Does a National Self-Assessment Do?

- Takes stock of existing national:
  - Policies
  - Procedures
  - Mechanisms
  - Norms
  - Institutions
  - Relationships
- Provides input for a national strategy

How is Self-Assessment Structured?

- The Audience
  - Who are they?
  - What is their level of awareness and response?
  - What decisions already taken?
- The Case for Action
  - Role of ICTs in the nation
  - Vulnerabilities of and threats from ICTs
  - Risks to be managed
- The Stage for Cybersecurity/CIIP: Other National Goals and Objectives

Who Participates in the Self-Assessment?

Government drafters:

- Entity with authority to lead effort
- Entities responsible for the different building blocks
  - International cooperation, including government-industry collaboration
  - Organizational measures, incident management
  - Technical measures and standards
  - Legislation and enforcement
  - Capacity building and developing a culture of security
- National security entities
- Other government entities with significant roles

Who Participates in the Self-Assessment?

Advisors:

- From other elements of Government
- From the Private Sector:
  - Industry associations
    - CII and ICTs
    - Critical infrastructures
    - Business and economic
    - Etc.
  - Key companies
  - Civil society
  - Other significant voices

The Self-Assessment

- Looks at organizational and operational issues for each key element:
  - The people
  - The institutions
  - The relationships
  - The policies
  - The procedures
  - The budget and resources
  - Timeframes and milestones
  - Review and reassessment requirements

Output of the Self-Assessment:

Input for a National Cybersecurity/CIIP Strategy:

- Summary of key findings
  - With input from all participants
- Program of Actions and Recommendations
  - To be promulgated at a level to ensure coordinated action by all participants

What Does a National Strategy Do?

- Provides an agreed vision for national action
- Places cybersecurity/CIIP in the national agenda
- Delineates roles, responsibility and priorities
- Focuses attention at the national management and policy level
- Assist national governments to;
  - Understand the existing national approach
  - Develop “baseline” for future reference
  - Identify and prioritize areas for attention
  - Lay out a plan of action

Conclusion

A 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 national efforts
- Develop a national plan for coordinated action

- Using a common approach can facilitate necessary regional and international cross border cooperation

Observations

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

Next Steps

- What are the Next Steps
  - for your nation?
  - for your region?

Questions?

Thank You

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