

Fundamentals of Cybersecurity/CIIP

Awareness raising: The role of 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.



Copyright 2009, CTP, Inc. All rights reserved.

Objectives of this Presentation

- Review the Problem
- Review the origins of the national strategy and self-assessment approach
- Provide an overview of the national strategy and self-assessment approach

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?

“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*

- Call them “the Participants.”

What Action must Participants 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?

A Self-Assessment
Leading to
A National
Cybersecurity/ciip
Strategy

origins of national strategy and self-assessment approach

International and Regional Efforts:

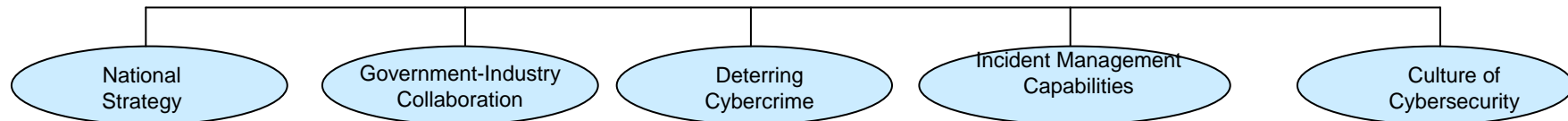
- United Nations General Assembly (UNGA)
 - Resolutions (57/239 & 58/199)
- Organization for Economic Cooperation and Development (OECD)
- G8
- Council of Europe (CoE)
- Asia Pacific Economic Cooperation (APEC)
- Organization of American States (OAS)
- World Summit on the Information Society (WSIS)
-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

origins of national strategy and self-assessment approach

National Efforts:

- Australia
- Germany
- Japan
- New Zealand
- Singapore
- United Kingdom
- United States

Framework for National Cybersecurity Efforts



POLICY: *Protection of cyberspace is essential to national security and a nation's economic well-being. Cyberspace interconnects industry sectors and crosses national borders. Coordinated national action by government, the private sector, and citizens/users is required for the prevention of, preparation for, response to, and recovery from incidents. Cooperation and coordination with international partners are also required.*

A. – Overview of Goals:

- I.A.1. Create awareness at national policy level about cybersecurity and the need for national action and international cooperation.
- I.A.2. Develop a national strategy to enhance cybersecurity to reduce the risks and effects of cyber disruptions.
- I.A.3. Participate in international efforts for the prevention of, preparation for, response to, and recovery from incidents.

B. – Specific Steps to Achieve Goals:

- I.B.1. Persuade national leaders in government of the need for national action to address threats to and vulnerabilities of the national cyber infrastructure through policy level discussions.
- I.B.2. Identify a lead person and institution for the overall national effort; determine where within the government a Computer Security Incident Response Team with national responsibility (N-CSIRT) should be established, and identify lead institutions for each element of the national strategy.
- I.B.3. Identify the appropriate experts and policymakers within government ministries, government, and private sector, and their roles.
- I.B.4. Identify cooperative arrangements for and among all participants.
- I.B.5. Establish mechanisms for cooperation among government and private sector entities at the national level.
- I.B.6. Identify international expert counterparts and foster international efforts to address cybersecurity issues, including information sharing and assistance efforts.
- I.B.7. Establish an integrated risk management process for identifying and prioritizing protective efforts for cybersecurity.
- I.B.8. Assess and periodically reassess the current state of cybersecurity efforts and develop program priorities.
- I.B.9. Identify training requirements and how to achieve them.

POLICY: *The protection of cyberspace is a shared responsibility that requires cooperation between government at all levels and the private sector, which owns and operates much of the underlying infrastructure.*

A. – Overview of Goals:

- II.A.1. Develop government-industry collaborations that work to effectively manage cyber risk and to protect cyberspace.
- II.A.2. Provide a mechanism for bringing a variety of perspectives, equities, and knowledge together to reach consensus and move forward together to enhance security at a national level.

B. – Specific Steps to Achieve Goals:

- II.B.1. Include industry perspectives in the earliest stages of development and implementation of security policy and related efforts.
- II.B.2. Encourage development of private sector groups from different critical infrastructure industries to address common security interests collaboratively with government.
- II.B.3. Bring private sector groups and government together in trusted forums to address common cybersecurity challenges.
- II.B.4. Encourage cooperation among groups from interdependent industries.
- II.B.5. Establish cooperative arrangements between government and the private sector for incident management.

POLICY: *The protection of cyberspace requires updating criminal laws, procedures and policy to address and respond to cybercrime.*

A. – Overview of Goals:

- III.A.1. Enact and enforce a comprehensive set of laws relating to cybersecurity and cybercrime consistent with the provisions of the Convention on Cybercrime (2001).

B. – Specific Steps to Achieve Goals:

- III.B.1. Assess the current legal authorities for adequacy. A country should review its criminal code to determine if it is adequate to address current (and future) problems.
- III.B.2. Draft and adopt substantive, procedural and mutual assistance laws and policies to address computer-related crime.
- III.B.3. Establish or identify national cybercrime units.
- III.B.4. Develop cooperative relationships with other elements of the national cybersecurity infrastructure and the private sector.
- III.B.5. Develop an understanding among prosecutors, judges, and legislators of cybercrime issues.
- III.B.6. Participate in the 24/7 Cybercrime Point of Contact Network.

POLICY: *The protection of cyberspace requires an organization to serve as the national focal point for securing cyberspace, whose mission includes watch, warning, response and recovery efforts and the facilitation of collaboration between and among government entities at the national, state and local levels; the private sector; academia; and the international community.*

A. – Overview of Goals:

- IV.A.1. Develop a coordinated national cybersecurity response system to prevent, detect, deter, respond to and recover from cyber incidents.
- IV.A.2. Establish a focal point for managing cyber incidents that bring together critical elements from government (including law enforcement) and essential elements from infrastructure operators and vendors to reduce both the risk and severity of incidents.
- IV.A.3. Participate in watch, warning and incident response information sharing mechanisms.
- III.A.4. Develop, test and exercise emergency response plans, procedures, and protocols to ensure that government and non-government collaborators can build trust and coordinate effectively in a crisis.

B. – Specific Steps to Achieve Goals:

- IV.B.1. Identify or establish a national Computer Security Incident Response Team (N-CSIRT).
- IV.B.2. Establish mechanism(s) within government for coordination among civilian and government agencies.
- IV.B.3. Establish collaborative relationships with industry to prepare for, detect, respond to, and recover from national cyber incidents.
- IV.B.4. Establish point(s) of contact within government agencies, industry and international partners to facilitate consultation, cooperation, and information exchange with the N-CSIRT.
- IV.B.5. Participate in international cooperative and information sharing activities.
- IV.B.6. Develop tools and procedures for the protection of the cyber resources of government entities.
- IV.B.7. Develop a capability through the N-CSIRT for coordination of governmental operations to respond to and recover from large-scale cyber attacks.
- IV.B.8. Promote responsible disclosure practices to protect operations and the integrity of the cyber infrastructure.

POLICY: *Because personal computers are becoming ever more powerful, technologies are converging, the use of ICTs is becoming more and more widespread, and connections across national borders are increasing. All participants who develop, own, provide, manage, service and use information networks must understand cybersecurity and take action appropriate to their roles to protect cyberspace. Government must take a leadership role in bringing about this Culture of Cybersecurity and in supporting the efforts of other participants.*

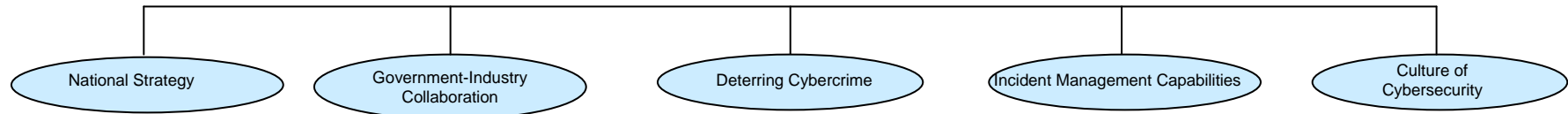
A. – Overview of Goals:

- V.A.1. Promote a national Culture of Security consistent with UNGA Resolutions 57/239, *Creation of a global culture of cybersecurity*, and 58/199, *Creation of a global culture of cybersecurity and the protection of critical information infrastructures.*

B. – Specific Steps to Achieve Goals:

- V.B.1. Implement a cybersecurity plan for government-operated systems.
- V.B.2. Implement security awareness programs and initiatives for users of government systems and networks.
- V.B.3. Encourage the development of a Culture of Cybersecurity in business enterprises.
- V.B.4. Support outreach to civil society with special attention to the needs of children and individual users.
- V.B.5. Promote a comprehensive national awareness program so that all participants – businesses, the general workforce, and the general population – secure their own parts of cyberspace.
- V.B.6. Enhance Science and Technology (S&T) and Research and Development (R&D) activities.
- V.B.7. Review existing privacy regime and update it to the online environment.
- V.B.8. Develop awareness of cyber risks and available solutions.

Framework for National Cybersecurity Efforts



C. – Reference Material & Training Resources:

(available from the U.S. or internationally)

I.C.1. Awareness raising (I.B.1., I.B.2.)*
UN World Summit on the Information Society, <http://www.itu.int/WSIS/index.html>
ITU Development Bureau Cybersecurity webpage <http://www.itu.int/ITU-D/cyb/>
ITU Cybersecurity Gateway, <http://g4chat.itu.ch/cybersecurity/gateway/index.html>
OECD Guidelines and Culture of Security: <http://www.oecd.org/sti/cultureofsecurity>
UNGA Res. 55/63, 56/121, 57/239, 58/199; <http://www.un.org/Depts/dhl/resguide/gares1.htm>
"Information Society in an Enlarged Europe," Budapest, 2/26/04, http://ec.europa.eu/archives/commission_1999_2004/liikanen/media/speeches/index_en.htm
"i2010: How to Make Europe's Information Society Competitive," Brussels, 2/22/05, <http://europa.eu.int/rapid/pressReleasesAction.do?reference=SPEECH/05/107&type=HTML&aged=0&language=EN&guiLanguage=en>
European Network and Information Security Agency, <http://www.enisa.europa.eu/>
Meridian Conference, www.meridian2007.org/
I.C.2. National Strategy (I.B.2., I.B.3., I.B.4., I.B.5., I.B.7.)
U.S. National Strategy to Secure Cyberspace <http://www.whitehouse.gov/pcipb/>
National Implementation Strategies of 11 OECD members: http://www.oecd.org/document/63/0,2340,en_21571361_36139259_36306559_1_1_1_1,00.html
UK Centre for Protection of National Infrastructure (CPNI): <http://www.cpni.gov.uk/>
New Zealand: www.digitalstrategy.govt.nz
Canada: www.psepc-spccc.gc.ca
I.C.3. Assessment and Program Development (I.B.5., I.B.7., I.B.8)
Self-Assessment Tool
NIST Special Publications 800-26 (2001), 800-30 (2002), 800-50 (2003), &

C. – Reference Material and Training Resources:

(available from the U.S. or internationally)

II.C.1. Structures for Government-Industry Collaboration (II.B.1., II.B.2., II.B.3., II.B.4., II.B.5.)
United States Information Sharing and Analysis Centers (ISACs) & Coordinating Councils:
Financial Services ISAC <http://www.fsisac.com/>
Electric Sector ISAC <http://www.esisac.com/>
Information Technology ISAC <http://www.it-isac.org>
Telecommunications ISAC <http://www.ncs.gov/ncc/>
Network Reliability and Interoperability Council (NRIIC) <http://nriic.org/>
National Security Telecommunications Advisory Committee (NSTAC) <http://www.ncs.gov/nstac/nstac.html>
United States Sector Specific Plans: http://www.dhs.gov/xprevprot/programs/gc_11798661976_07.stm
ITAA White Paper on Information Security: <http://www.itaa.org/eweb/upload/ITAA%20Infosec%20White%20Paper.pdf>
Industry-Government Cooperation on Standards: American National Standards Institute-Homeland Security Standards Panel: http://www.ansi.org/standards_activities/standards_boards_panels/hssp/overview.aspx?menuid=3
National Telecommunications and Information Administration: <http://www.ntia.doc.gov/>
IT Sector Coordinating Council (SCC): www.it-sec.org
II.C.2. Cybersecurity Information Sharing (II.B.1., II.B.2., II.B.3., II.B.4., II.B.5.)
National Information Assurance Council (NIAC) report on sector partnership model working group: http://itaa.org/eweb/upload/NIAC_SectorPartModelWorkingGrp_July05.pdf
US-CERT alerts: <http://www.us-cert.gov/cas/>
National Institute of Standards and Technology, Computer Security and Research Center, <http://csrc.nist.gov/>
Internet Engineering Task Force: www.ietf.org
World Wide Web Consortium: www.w3c.org
Institute of Electrical and Electronics Engineers: www.ieee.org
Messaging Anti-Abuse Working Group: www.maaawg.org
II.C.3. Awareness Raising and Outreach: Tools for Business and Home Use
Information for technical and non-technical users: <http://www.us-cert.gov/>
StaySafeOnline: <http://www.staysafeonline.org/>
Federal Trade Commission: Onguard Online www.ftc.gov/infosecurity and www.OnguardOnline.gov
U.S. CERT posters and information sheets: http://www.uscert.gov/reading_room/distributable.html
OECD's Anti-Spam Toolkit: <http://www.oecd-antispam.org>
London Action Plan: www.oecd-antispam.org

C. – Reference Material and Training Resources:

(available from the U.S. or internationally)

III.C.
Convention on Cybercrime (2001) (COE website): <http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm>
G-8 High-Tech Crime Principles and 24/7 information assistance mechanism: http://www.usdoj.gov/criminal/cybercrime/g82004/g8_background.html
UNGA Resolutions 55/63, 56/121: <http://www.un.org/Depts/dhl/resguide/gares1.htm>
U.S. DOJ CCIPS website: <http://www.cybercrime.gov>
APEC TEL Cybercrime-related documents: http://www.apec.org/apec/apec_groups/working_groups/telecommunications_and_information.html

Culture of Cyber Security, continued

V.C.3. Individuals and Civil Society (V.B.4., V.B.6., V.B.7.)
Stay Safe Online: <http://www.staysafeonline.info/>
OnGuard Online: <http://onguardonline.gov/index.html>
U.S. CERT: <http://www.us-cert.gov/nav/n01/>
OECD's Anti-Spam toolkit, www.oecd-antispam.org
The OECD questionnaire on implementation of a Culture of Security (DSTI/ICCP/REG(2004)4/Final). Available together with responses from other OECD countries at <http://webdomino1.oecd.org/COMNET/STI/ICCP/Secu.nsf/OpenDatabase>
New Zealand: www.netsafe.org.nz
Canada: www.psepc-spccc.gc.ca

C. – Reference Material and Training Resources:

(available from the U.S. or internationally)

IV.C.1. National Response Plan (IV.B.4.)
National Response Plan: http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0566.xml
StaySafeOnline <http://www.staysafeonline.info/>
Information Security and Privacy Advisory Board <http://csrc.nist.gov/ispub/>
NIST: <http://csrc.nist.gov/>
IV.C.2. National CSIRT (IV.B.1., IV.B.2., IV.B.7.)
US CERT: <http://www.us-cert.gov/>
NIATEC training courses: <http://niatec.info>
Carnegie Mellon University/CERT Coordination Center: <http://www.cert.org/csirts/>
European Network and Information Security Agency (ENISA): A Step-by-Step Approach on How to Set up a CSIRT (http://www.enisa.europa.eu/pages/05_01.htm)
India: [www.cert-in.org.in](http://cert-in.org.in)
Australia: www.auscert.org.au
IV.C.3. Cooperation and Information Sharing (IV.B.3., IV.B.4., IV.B.5., IV.B.8.)
OECD's Anti-Spam toolkit: <http://www.oecd-antispam.org>
IT-ISAC: <http://www.it-isac.org/>
IT Sector Coordinating Council <http://www.itaa.org/infosec/docs/ITSSCResponsestoGAO.pdf>
International Standards Organization, Joint Technical Committee 1, Subcommittee 27 (ISO/JTC1/SC27) <http://www.iso.org/iso/en/CatalogueListPage.CatalogueList?COMMID=143&scopelist=CATALOGUE>
IV.C.4. Vulnerability Information /Tools and Techniques (IV.B.6.)
National Vulnerability Database (NVD) – <http://nvd.nist.gov/nvd.cfm>
Open Vulnerability Assessment Language (OVAL) – <http://oval.mitre.org/>
Build Security In - Collection of software assurance and security information to help software developers, architects, and security practitioners create secure systems - <http://buildsecurityin.us-cert.gov/daisy/bsi/home.html>
Common Vulnerabilities and Exposures List (CVE) <http://www.cve.mitre.org/about/>

C. – Reference Material and Training Resources:

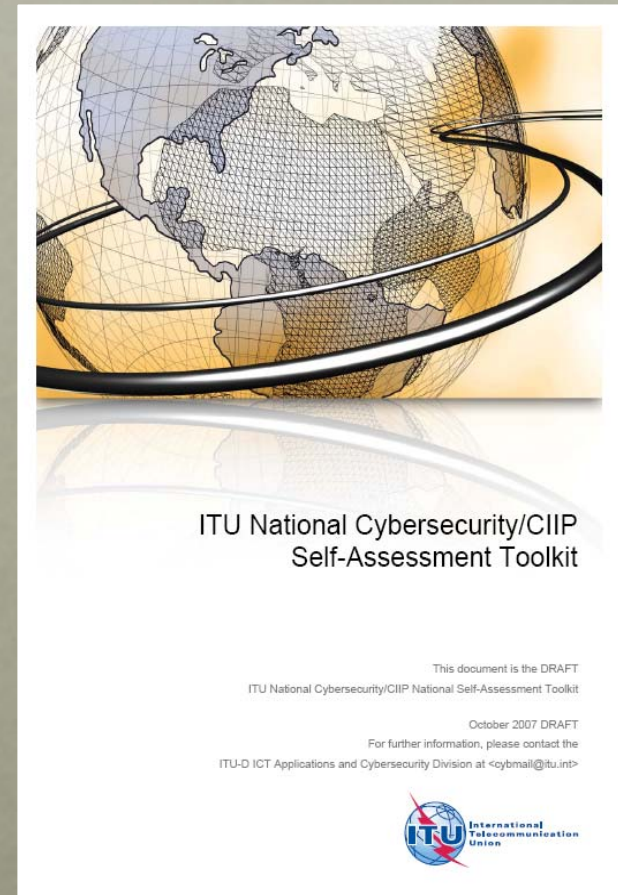
(available from the U.S. or internationally)

V.C.1. Government systems and networks (V.B.1., V.B.2., V.B.7.)
UNGA RES 57/239 Annexes a and b. <http://www.un.org/Depts/dhl/resguide/gares1.htm>
OECD "Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security" [2002] http://www.oecd.org/document/42/0,2340,en_2649_34255_15582250_1_1_1_1,00.html
OECD "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" (Adopted Sept. 23, 1980): http://www.oecd.org/document/20/0,2340,en_2649_34255_15589524_1_1_1_1,00.html
OECD Ministerial Declaration on the Protection of Privacy on Global Networks (1998), (DSTI/ICCP/REG(2005)1/Final).
Multi State Information Sharing and Analysis Center : Main Page: <http://www.msiscac.org/>
The U.S. Federal Information Security Management Act of 2002 (FISMA) <http://csrc.nist.gov/policies/FISMA-final.pdf>
U.S. HSPD-7, "Critical Infrastructure Identification, Prioritization and Protection" <http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html>
U.S. Federal Acquisition Regulations (FAR), parts 1.2,7.11, and 39. <http://www.acqnet.gov/FAR/>
[The U.S.] National Strategy to Secure Cyberspace: <http://www.whitehouse.gov/pcipb/>
U.S. CERT site: <http://www.us-cert.gov/>
U.S. NIST site: <http://csrc.nist.gov/> and <http://csrc.nist.gov/ispub/>
V.C.2. Business and Private Sector Organizations (V.B.3., V.B.5., V.B.7.)
National Cyber Security Partnership: www.cyberpartnership.org
U.S. CERT: <http://www.us-cert.gov/>
U.S. DHS/Industry "Cyber Storm" exercises: http://www.dhs.gov/xnews/releases/pr_11583409_80371.stm
U.S. DHS R&D Plan: <http://www.dhs.gov/xres/programs/>
U.S. Federal Plan for R&D: http://www.nitrd.gov/pubs/csia/FederalPlan_CSI_A_RnD.pdf
U.S. President's Information Technology Advisory Committee report on Cyber Security research priorities: http://www.nitrd.gov/pitac/reports/20050301_cyb_research_priorities.pdf

* Parenthetical references in each column, e.g., (I.B.1., I.B.2.), identify associated Specific Steps in Part B., on page 1.

ITU National Cybersecurity/CIIP Self-Assessment Tool

- Intended to assist national authorities to review their domestic situation related to goals and actions identified in:
- Study Group Q 22/1:
Report on Best Practices for a National Approach to Cybersecurity



What Does a Self-Assessment Do?

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

What Does a Self-Assessment Do?

- **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**

Self-Assessment Addresses

**Collaboration
and Information
Exchange**

**Incident
Management**

**Legal
Framework**

**Culture of
Cybersecurity**

**Key Elements of a National
Cybersecurity/CIIP Strategy**

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 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**