A Critical Information Infrastructure Protection Approach to Multinational Cyber Security Events

Bradford J. Willke

19 September 2007

Overview

A framework for national Critical Information Infrastructure Protection (CIIP) provides a **structured view of strategic information services and infrastructure resources** for a nation state. This framework also serves as a **common lens from which to view risks, threats, vulnerabilities, and protective controls** of those resources. **Plans for national response and infrastructure protection** define the **process for risk management** and have a potential to **create stabilizing effects** both domestically and internationally.

In this overview, we will examine **best practices pervasive in CIIP frameworks**, **common intersections of CIIP practice**, **consequences of under planning or scoping of CIIP activities**, and **a practical approach to multi-national event coordination** under a CIIP framework.

Multi-National Cybersecurity Impediments

Cybersecurity, business continuity, and ICT operations support critical information infrastructure protection (I.e., provide elements of resiliency) but are often performed independent of one another

The field of cybersecurity and CIIP tends to be focused on technical not managerial solutions; true process improvement elusive

Nation's have false sense of preparedness; only tested during disruptive events

Codes of practice are numerous; however practice effectiveness is rarely measured

There are few reliable benchmarks for determining an nation's capability for protecting critical information infrastructures

Critical Infrastructure Protection (CIP) Defined

Critical infrastructures are those systems that provide the resources upon which all functions of society depend. Examples are telecommunications, transportation, energy, water supply, health care, emergency services, manufacturing and financial services

Source: IEEE-USA. Available at http://www.ieeeusa.org/policy/positions/infoinfrastructure.html

Critical Information Infrastructure Protection (CIIP) Defined

Protecting “communications or information service[s] whose availability, reliability and resilience are essential to the functioning of a modern [national] economy, security, and other essential social values”

Source: “Ensuring (and Insuring?) Critical Information Infrastructure Protection: A Report of the 2005 Rueschlikon Conference on Information Policy,” Kenneth Cukier. Available at http://www.rueschlikon-conference.org/pressdocs/56_R_05_Report_Online.pdf

CIIP Strategic Goals - Example

GOAL 1: Facilitate the development of a national Critical Information Infrastructure programme (CIIP) strategy

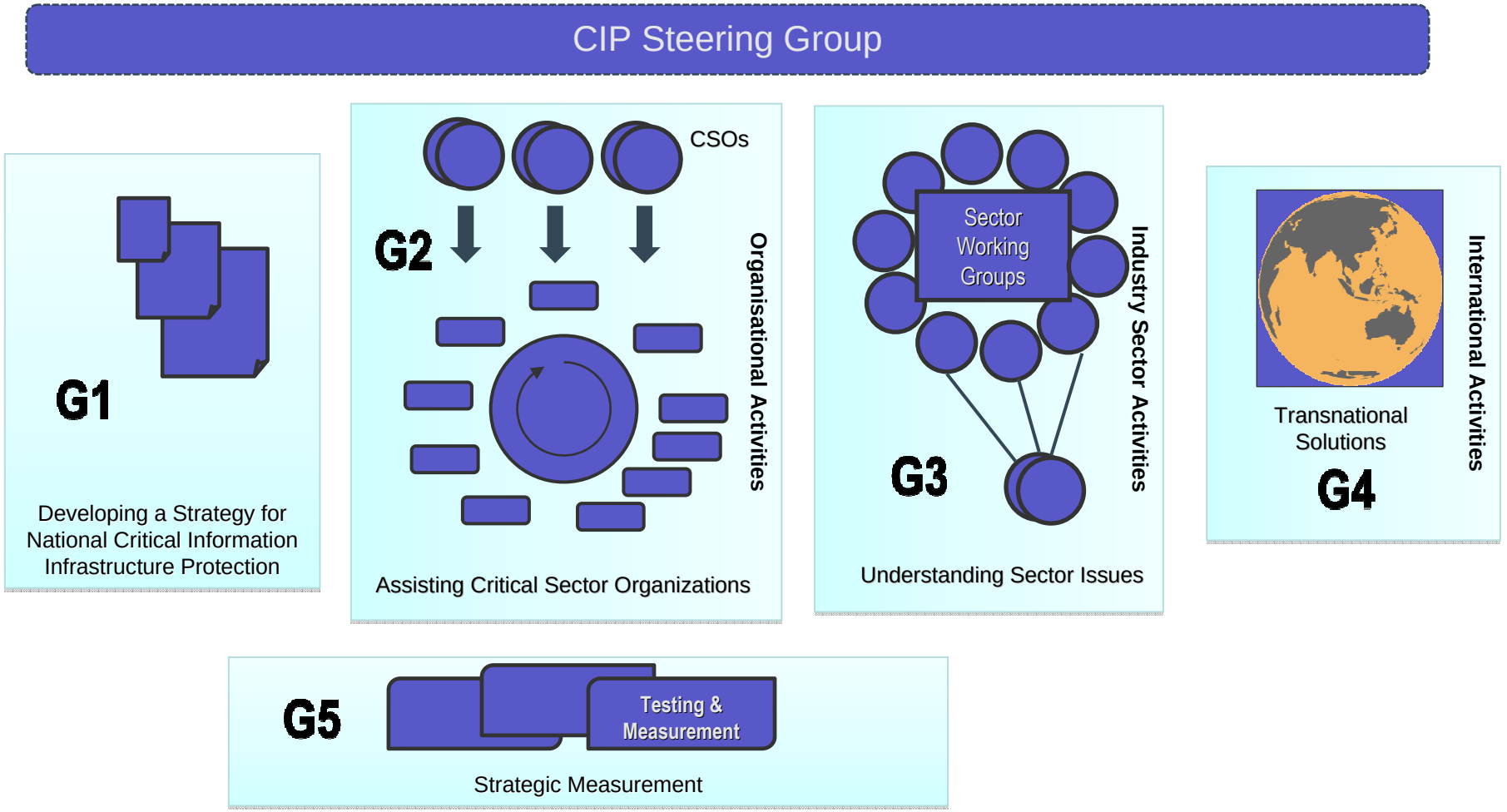
GOAL 2: Assisting owners & operators of Critical Infrastructure, (both Government and private sectors) to mitigate their information risk

GOAL 3: Identify and understanding sector issues and cross-sector dependencies

GOAL 4: Working with international CIP/CIIP organizations for determining transnational solutions

GOAL 5: Testing and measuring CIP/CIIP maturity over time and guiding strategy based on measurement

CIIP Strategies - How It Is Organised



Developing a National Strategy

Formalise the nation's recognition of cybersecurity as an imperative

- Policy goals for CIIP/Cybersecurity
- Understanding of risks associate with CII/Cyber
- Recognition of roles and responsibilities (of all parties)

Formalise the structure of CIIP as a function of government

- Placement of national programme
- National agenda vehicle
- Relationship to existing capabilities (I.e., National CSIRT, Information Sharing and Analysis Centres, etc)

Formalise the national policy

Developing a National Strategy (Cont.)

Formalise the relationship of partners

- Public-Private partnerships (government-to-business, government-to-Subject-Matter-Experts, government-to-academic/research)

Create a risk management process for prioritizing and examining protective measures

Assess and re-assess the national state of cybersecurity (periodically)

Identify requirements:

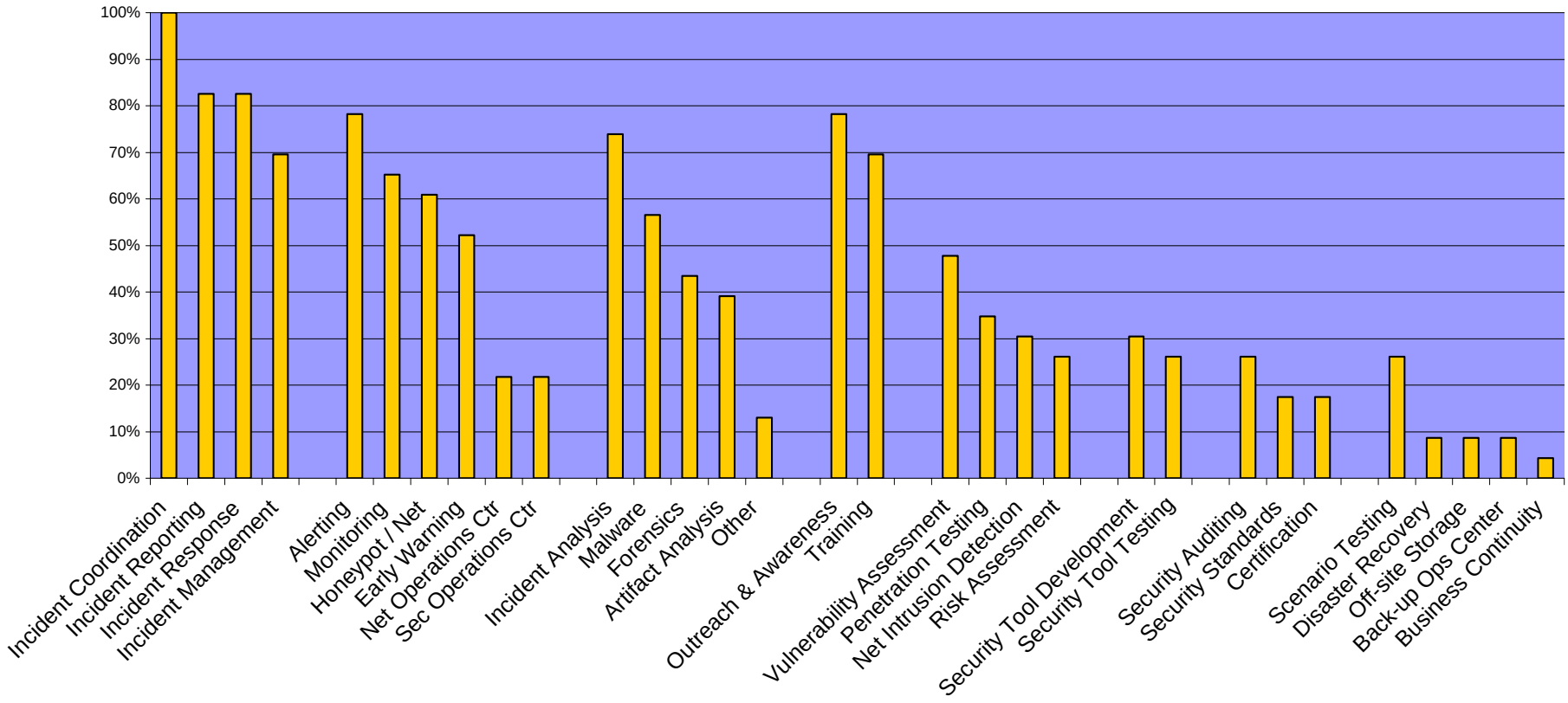
- Training requirements
- Process requirements
- Data sources
- Information channels
  - Distribution of urgent, normal, or informative communications

What is Required to Do this Efficiently and Effectively

Requirements:

- Common risk framework (risks based on the potential negatives impacts to critical information infrastructures caused by threats and vulnerabilities)
  - Common or comparable definitions and risk articulation
  - Valuation of the CII
  - Common understanding of negative impact and areas of impact (economy, psychology, safety, …)
- Understand how mature your CII programme is, what goals have been met, and what capabilities exist
- Understand ‘trusted’ sources of information and mutual capabilities/functions

Services Offered by CERTs with National Responsibility (Many related to CIIP)



CSIRT Activities In CIIP

Develop and sustain an understanding of national cybersecurity environment

Create metrics to quantify understanding

Track the state of cybersecurity over time

Assist critical information infrastructure providers and government regulatory bodies in identifying and addressing information security vulnerabilities and threats

Disseminate “lessons learned” from analysis of the cyber environment and information gained from the various sectors in to expand and improve the overall state of security within the nation

Liase with law enforcement, regulators, subject matter experts, … on the technical solutions and implications

National Cybersecurity Goals Intersect with CSIRT Responsibilities

1. Develop National Strategy for Cybersecurity and Critical Infrastructure Protection
2. Establish National Government-to-Industry Collaboration
3. Deter Cyber Crime
4. Operate National Incident Management Capability
5. Promote National Culture of Cybersecurity

International Cybersecurity Goals Require CSIRT Facilitations

To Identify experts

To Identify resources

To Identify mutual countermeasures and areas of responsibility

To coordinate the vendor and service provider communities on technical and procedural solutions and remedies

To coordinate within management frameworks (such as CIP programmes, national emergency response plans, etc)

To advise government and industry on steps to take, and actions not to take

To participate in planning, design, implementation, operation, and reconstitution processes with partners

How is CII Information Used in National / Multi-National Cybersecurity?

What would your answer be?

What is the state of your relationship (CSIRT-to-CII Programme)?

How would you understand the state of readiness, preparedness, and competency in CII within your nation?

Do you have a formal role and set of responsibilities in national response plans, national crisis, etc?

- Is there a threshold for your participation?

Do you design or assist in national preparedness studies, scenario planning, and table-top exercises and simulations?

Questions and Discussion