CERT

Engineering National Cybersecurity and Critical Information Infrastructure Protection

Bradford J. Willke, CISSP

16 October 2007

ITU Regional Workshop
Buenos Aires, Argentina

© 2007 Carnegie Mellon University

Overview

Purpose: This session seeks to explore in more detail various approaches, best practices, and identify key building blocks that could assist countries in the Americas region in establishing national strategies for cybersecurity and CIIP.

To address these threats and protect infrastructures, each country needs a comprehensive action plan that addresses technical, legal and policy issues, combined with regional and international cooperation.

Issues, actors, and frameworks that should be considered in a national strategy for cybersecurity and critical information infrastructure protection

© 2007 Carnegie Mellon University

Preface on National Cybersecurity Efforts

“If you don’t know where you are, a map won’t help”

-- Watts Humphrey, Software Engineer

© 2007 Carnegie Mellon University

National and Multi-National Cybersecurity Impediments

Goal Orientation: 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

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

Preparation: Nation’s have false sense of preparedness; only tested during disruptive events

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

Measurement: There are few reliable benchmarks for determining an nation’s capability for protecting critical information infrastructures

© 2007 Carnegie Mellon University

National Cybersecurity Goals

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

© 2007 Carnegie Mellon University

Getting Started

Self-assessment against a common framework can provide a place to start building a national cybersecurity programme

But you have to know

- What is the route (a framework)
- What is the destination (how far you must implement the framework)
- Where you are (how far you have implemented the framework)

The destination is determined by the capabilities and the maturity of processes you must have in place to manage unacceptable risks

© 2007 Carnegie Mellon University

National Risks and Risk Tolerance

National risks to cybersecurity involve conditions where negative consequences and events can possibly harm the assets required to implement, sustain, and protect critical infrastructure

- Risks are comprised of assets, threats, vulnerabilities, consequences, and probability and/or impacts

Risk tolerance must be put in terms of CIIP and National Cybersecurity

- The degree of uncertainty a government can accept regarding potential negative impacts to community indicators of health and stability
- The threshold for negative consequences and events deemed as unacceptable community impacts of risks

© 2007 Carnegie Mellon University

Setting National Risk Tolerance

Risk tolerance is decide in the ‘public interest’ and not for the needs of single organizations or even industries

- Governments, because of the responsibility and duty they have for citizens and businesses, set the thresholds for acceptable and unacceptable risks
  - Enumerated areas of health and wellness
    - Public safety
    - Psychology
    - Economy

© 2007 Carnegie Mellon University

Best Practices for Engineering CIIP - 1

“Plan your work for today and every day, then work your plan”

-- Norman Vincent Peale, Author

Simplified:

Plan the work, Work the plan

© 2007 Carnegie Mellon University

Best Practices for Engineering CIIP - 2

Project Management Perspective

1. Establish a national-level philosophy, set of goals and objectives, and policy for cyber security
2. Plan the process of conducting cybersecurity and CIIP
3. Provide resources, assign responsibilities, and train people
4. Manage configurations
5. Identify and involve relevant stakeholders
6. Monitor and control the process
7. Objectively evaluate adherence to the process
8. Review status with governance leaders

[Adapted From: *CMMi v1.2 - Generic Goals and Practices*, Software Engineering Institute, Carnegie Mellon University.]

© 2007 Carnegie Mellon University

Best Practices for Engineering CIIP - 3

Process Control Perspective

1. Treat national strategies for cybersecurity and CIIP as a process
2. Monitor and control the plan, design, and implementation
3. Focus on building a national-level, highly visible process
4. Develop and manage requirements
5. Measure and analyze, where appropriate
6. Perform validation and verification of assumption, requirements, and solutions
7. Define trusted, reliable sources of information and the means for information sharing

© 2007 Carnegie Mellon University

Sponsors, Stakeholder, & Actors - 1
[What are their responsibilities]

	Define the CIIP Process	Implement the CIIP Process	Review the CIIP Process
Government Agencies & Regulators	X	X	X
Private Industry Sectors	X	X	X
Public-Private Partnerships	X	X	X
International Partnerships	X	X	X

© 2007 Carnegie Mellon University

Sponsors, Stakeholder, & Actors - 2
[Who are they]

	Controls and Monitors Risks	Controls and Monitors Process	Controls and Monitors Plan
Government Agencies & Regulators	Generally All Departments / Regulators	Specialists within Agencies	One Agency, or Small Group of in Collaboration
Private Industry Sectors	Generally All Sectors	Sector leads and Specific CI/KR Owners	[Account & Assist Only]
Public-Private Partnerships	Some Partnerships	Working groups and Teams	[Account & Assist Only]
International Partnerships	Some Partnerships	Standards, Working & Study Groups	[Observe and Assist Only]

© 2007 Carnegie Mellon University

Final Words on National Frameworks

"All models are wrong, some models are useful"

-- George Box, Industrial Statistician

© 2007 Carnegie Mellon University

Questions and Discussion

Contact Information:

Bradford Willke

Email: bwillke@cert.org

Phone: +1 412 268-5050

Postal Address:

CERT Survivable Enterprise Management Group
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, Pennsylvania 15213-3890
USA

© 2007 Carnegie Mellon University