CSIRT Contributions to National Efforts in Critical Information Infrastructure Protection

Bradford J. Willke, CISSP

17 October 2007

ITU Regional Workshop
Buenos Aires, Argentina

Overview

This presentation examines **best practices pervasive in CIIP frameworks related to CSIRTs**, **common intersections of CSIRT-to-CIIP practice**, and **benefits of planning or scoping of CSIRT-to-CIIP activities** and **multi-national event coordination** under a CIIP framework

Culture of Cybersecurity

A Focus on security in the development of information systems and networks and the adoption of new ways of thinking and behaving when using and interacting within information systems and networks

[OECD Council definition, July 2002]

… factor[ing] security into design and use of all information systems and networks by promoting consideration of security as an important objective when thinking about, assessing and acting…

[OECD Guidelines, Aug 2007]

Components of the Culture

Awareness, Training, and Education

Assigned Responsibility

Responsiveness

Ethics

Neutrality

Risk Attentiveness

Planning and Design

Management

Assessment

National and Multi-National Cybersecurity Culture 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

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

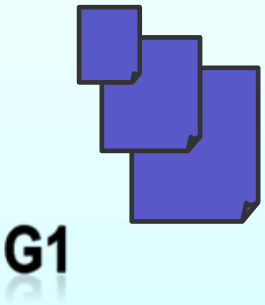
GOAL 3: Identify and understanding sector issues and cross-sector dependencies

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

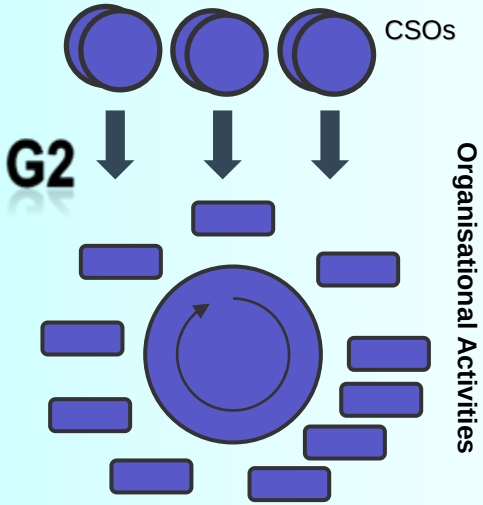
GOAL 5: Testing and measuring CIP/CIIP maturity over time and guiding strategy based on measurement

CIIP Strategies - How It Is Organised

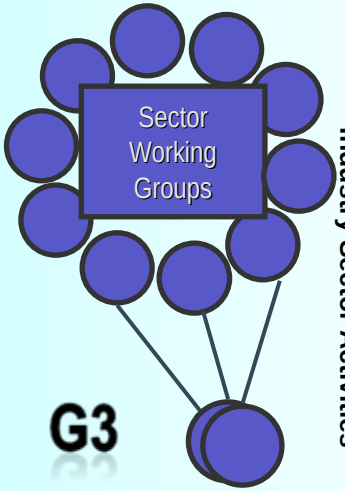
CIP Steering Group



Developing a Strategy for National Critical Information Infrastructure Protection



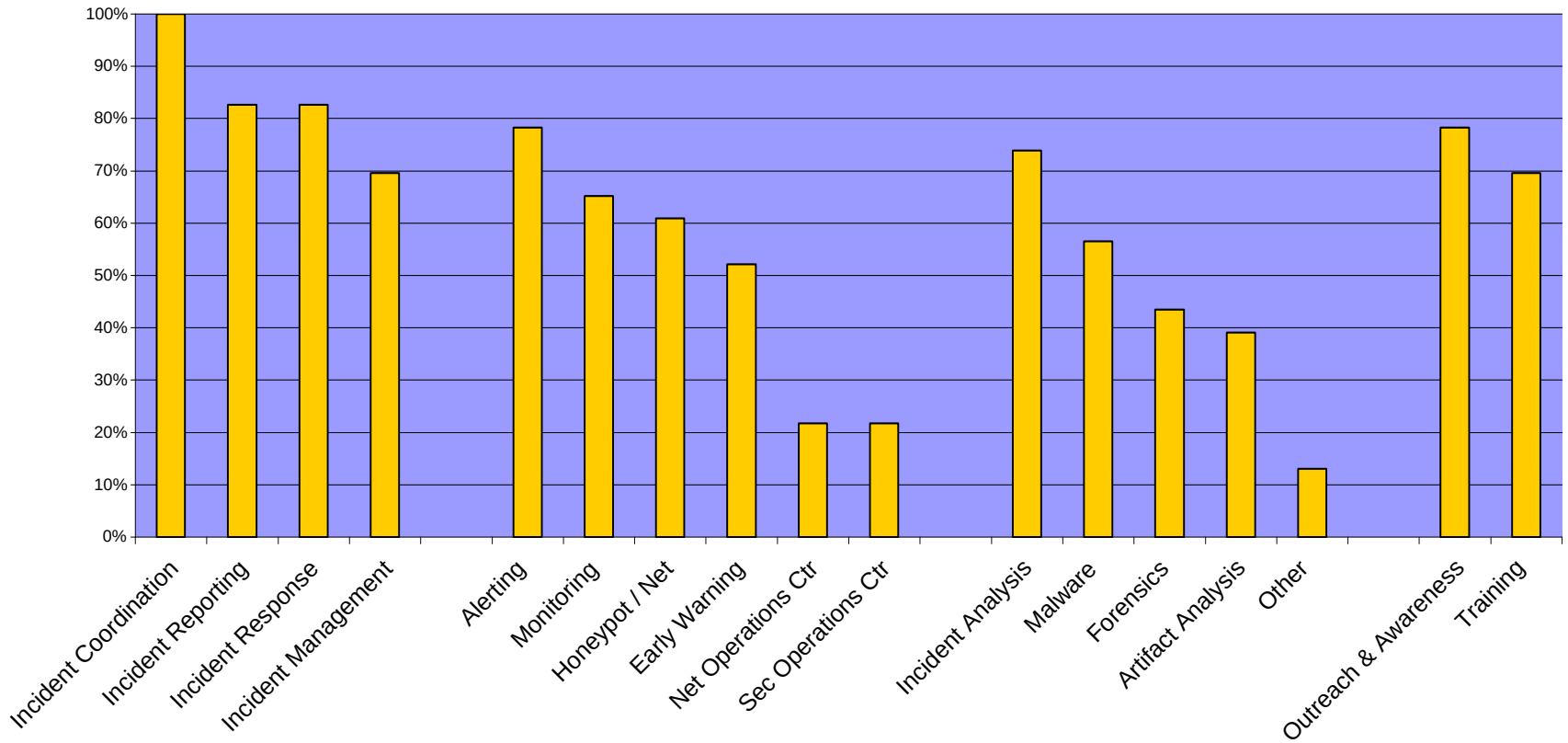
Assisting Critical Sector Organizations



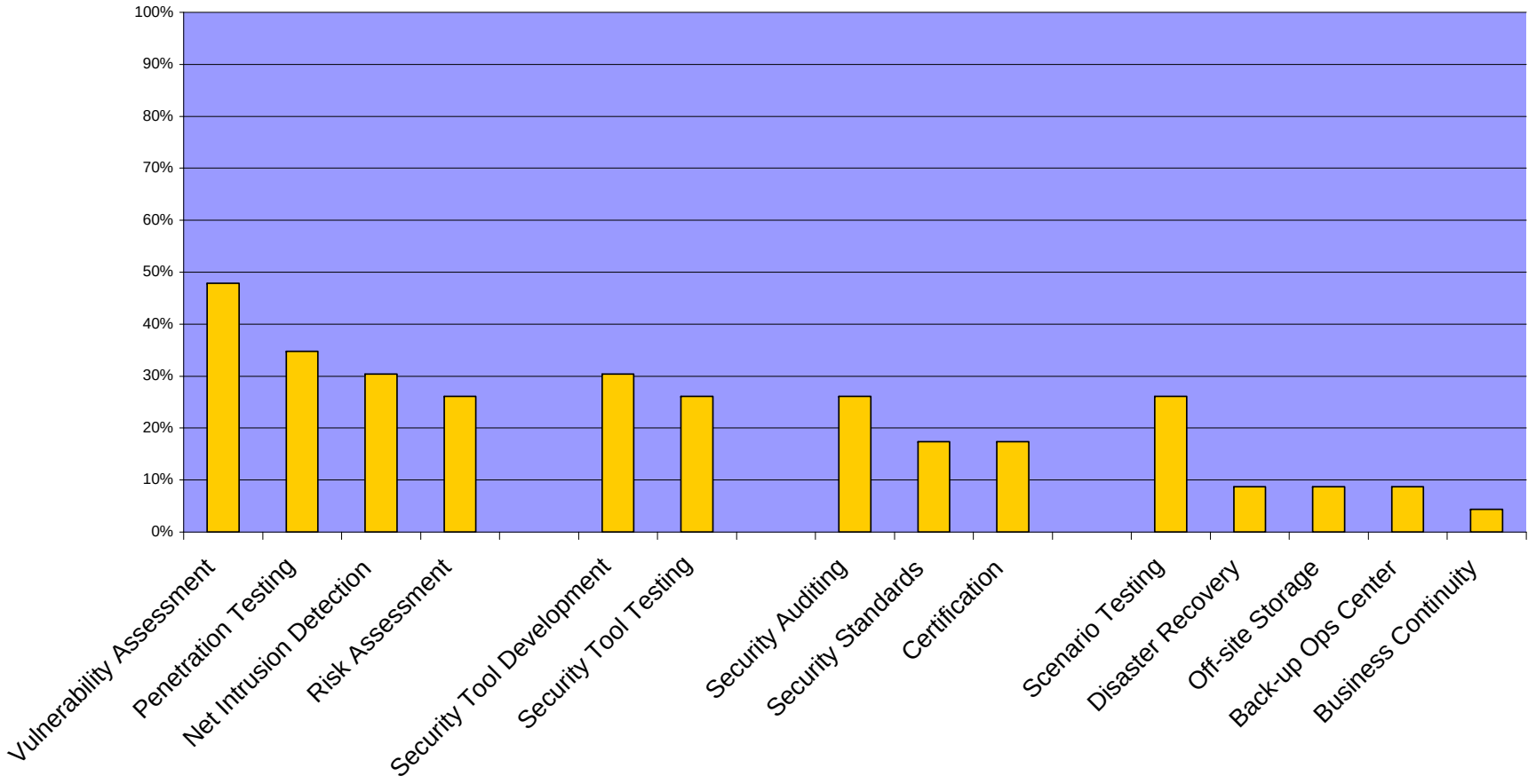
Understanding Sector Issues

Strategic Measurement

Services Offered by CSIRTs/CERTs with National Responsibility (Many related to CIIP) - 1



Services Offered by CSIRTs/CERTs with National Responsibility (Many related to CIIP) - 2



CSIRT Activities In CIIP

Develop and sustain an understanding of national cybersecurity environment

- Threats, Vulnerabilities, Risks, Capabilities, Sensitivities

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

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

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

Elements of a National Strategy Pertaining to CSIRTs

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
- Identify requirements:
  - Information channels for distribution of urgent, normal, or informative communications

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