Government-Industry Collaboration

Bradford J. Willke
Team Lead, Information Security Assessment & Evaluation
Survivable Enterprise Management Group

Overview

Introduction to Government-Industry Collaborations in Cybersecurity

Building Government-Industry Collaborations

Connecting to a National Framework for Cybersecurity

Case Studies of Partnerships and Collaborations

Conclusions

INTRODUCTION TO GOVERNMENT-INDUSTRY COLLABORATION

Goals and Objectives

- Develop government-industry collaborative relationships to manage cyber risk and to protect cyberspace
- Provide a mechanism to bring government and industry perspectives, equities, and knowledge together in order to reach consensus and move forward to enhance security at a national level

Collaborative Activities - 1

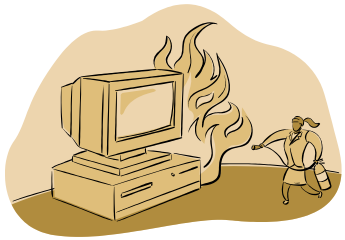
- Identify experts, resources, areas of responsibility, mutual countermeasures, best practices, and standards
- Coordinate with vendor and service provider communities on technical and procedural solutions and remedies
- Coordinate within management frameworks (such as CIP programs, national emergency response plans, etc)
- Advise government, nCSIRTs, intelligence services, and law enforcement
- Participate in planning, design, implementation, operation, and reconstitution processes with partners

Collaborative Activities - 2

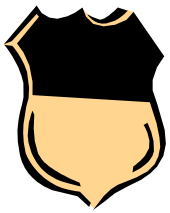
- Identify dependencies and interdependencies between critical infrastructure systems
- Identify consequences of a critical infrastructure failure
- Identify threats, risks, single points of failure, and major vulnerabilities
- Develop options for investment and other mitigation strategies
- Plan and test using evaluations and scenarios, including natural disasters, criminal actions, and acts of sabotage/terrorism, which disrupt the supply of critical infrastructure services and test business continuity and other response plans

Other G2I Activities In CIIP

- Perform research to understand aspects of the national cybersecurity environment
- Create metrics to quantify understanding
- Track the state of cybersecurity over time



- Improve the process by which cybersecurity threats, vulnerabilities, and risks are identified and addressed as a community
- Disseminate “lessons learned” from analysis of the cyber and physical environments
- Identify gaps and contention in e-laws and regulations



[GOVERNMENTS] BUILDING GOVERNMENT-INDUSTRY COLLABORATIONS

Recognize Strategic Imperatives & Impediments

Goal Orientation:

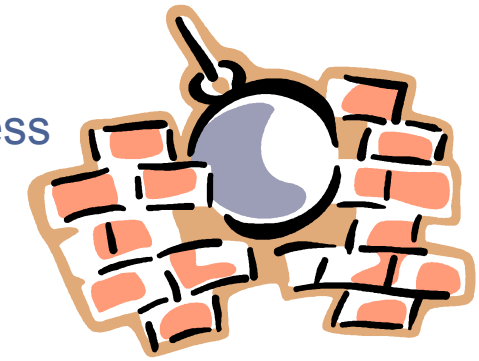
- Cybersecurity, business continuity, and ICT operations support critical information infrastructure protection (I.e., provide elements of resiliency), but are often performed independent of one another

Problem Recognition:

- The field of cybersecurity and CIIP tends to be focused on technical; managerial solutions and true process improvement are elusive

Preparation:

- Nations are tested during disruptive events; but need a good sense of readiness / preparedness



Process:

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

Measurement:

- Measurement and feedback move nations forward; but few reliable benchmarks are available for determining capacity in CIIP

Missions and Visions

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]

Gain Industry Perspectives

Engage industry early from development to implementation to maintenance

Employ different mechanisms for engagement

- Participation in government-industry working groups
- Solicitation of comments for cybersecurity policy and strategy development
- Coordination of efforts through information sharing mechanisms

Collaborate on an approach to risk management

Cooperate in research and development activities

Encourage Development of Industry Groups

Focus:

- Strategic issues
- Operational issues
- Management of security concerns

Functions:

- Enables information sharing among industry
- Helps to provide a process for government engagement

Conditions needed to enable collaboration:

- Anonymity for members
- Access to information
- Protection of proprietary/business sensitive information

Reduce Barriers to Government-Industry Collaboration

Focus on mechanisms to build trust and promote collaboration

- Utilize a written agreement that guides the collaboration and exchange between government and industry
- Define a shared vision and purpose
- Leverage strong individual and organizational leadership
- Enable participants to achieve tangible and measurable outcomes

Example: Cooperative Arrangements for Incident Management

Coordinated response efforts are key to effective incident management

- Identify procedures for rapid identification of problems, information exchange, mitigation and/or remediation to diminish the damage caused by incidents

Framework for coordination

- Construct for information sharing that includes focal points for policy-related issues and operational information exchange
- Identify policies and procedures for sharing and reporting incidents
- Establish policies for protecting and disseminating sensitive (government and industry) proprietary information
- Create mechanisms for communicating and disseminating information

Exercise coordination mechanisms

- Test government-industry information sharing and coordination to identify gaps and improve preparedness activities

CONNECTING TO A NATIONAL FRAMEWORK FOR CYBERSECURITY

Relationship to a National Framework

- A national strategy
- Legal foundations
- Incident response capability
- Government-industry partnerships
- A culture of security
- Information sharing mechanisms
- Risk management approach

Develop a National Strategy

Formalize 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)

Formalize the structure of CIIP as a function of government

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

Formalize the national policy framework

Develop a National Strategy (Cont.)

Formalize 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

Set 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

Engineer CIIP

Use a 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

Identify Sponsors, Stakeholder, & Actors

	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]

CASE STUDIES OF GOVERNMENT-INDUSTRY COLLABORATION

G2I Case Study - Malaysia

Information Sharing Forum (ISF)

- Formed in June 2004 by the Malaysian Communications and Multimedia Commission (MCMC)
- Forum for Internet Service Providers (ISP) and other agencies to address Malaysian information and network security issues

Goals:

- Encourage cooperation between different network owners, operators, and other agencies
- Enable the sharing of experience and expertise for the benefit of the Malaysian network infrastructure
- Elaborate guidelines and best practices

G2I Case Study - Republic of Korea

Financial Information Security Alliance (Established in October 2002)

- 87 members: 20 banks, 27 security corporations, 30 insurance companies, and 10 non-bank financial institutions

Goals:

- Protect financial information security systems from cyber-terror and hacking
- Implement changes in international information protection policies such as the Banking Industry Technology Secretariat (BITS)
- Develops information protection standards and policies for the financial sector as well as assessments and certifications
- Perform research in information security and provides education

Information Security Practice Alliance (Established in July 2002)

- Voluntary alliance of private and public sector organizations

Goals:

- Increase information protection activities in the private sector, in cooperation with various security companies and associations and with the help of the Korean Information Security Alliance (KISA)

G2I Case Study - Australia

Critical Infrastructure Protection Modeling and Analysis (CIPMA) Program

Goals:

- Enhance the protection of Australia's critical infrastructure and improve the resilience of our economy and society
- Build technology for modeling and analyzing relationships and dependencies between Australia's critical infrastructure systems
- Build a capability to model and report on the likely impacts when networks in one or more sectors are affected by failures (caused by nature or people) in another sector

Partners:

- Australian Federal Government's Attorney-General's Department (lead organization)
- Commonwealth Scientific and Industrial Resource Organization (CSIRO)
- Trusted Information Sharing Network for Critical Infrastructure Protection (TISN)
- Australian Government agencies, state and territory governments, the Infrastructure Assurance Advisory Groups of the TISN and critical infrastructure owners and operators

Sectors covered (to date) include:

- Energy
- Telecommunications
- Banking and Finance

G2I Case Study - Singapore

National Infocomm Competency Centre (NICC)

- Industry-led and government-supported organization created to assist individuals and organizations in reaching and maintaining a high level of ICT competence
- Main accreditation body for ICT certifications
- Works closely with the Ministry of Manpower (MOM) and the Infocomm Development Authority (IDA) to promote knowledge and skills

Goals:

- Develop and maintain ICT skills, standards, and knowledge
- Facilitate the development and implementation of certification programs
- Promote activities to increase the certification of IT professionals and users
- Collaborate with international certifying bodies for the accreditation of certifications
- Promote competence and learning management practices

CONCLUSIONS

Getting Started - 1

Self-assessment against a common framework can provide a place to start building a government-industry collaborations

Use tools, such as the ITU Self-Assessment Toolkit, to:

- Identify the route (a framework)
- Identify the destination (how far you must implement the framework)
- Identify 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

Getting Started - 2

Identify national risks in cybersecurity, especially negative consequences and events that will harm the national interest (those assets that are required to implement, sustain, and protect critical infrastructure)

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

Identify risk tolerance and put it 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

Use Available Resources

ITU Study Group Q.22/1 Report on Best Practices for a National Approach to Cybersecurity: A management Framework for Organizing National Cybersecurity Efforts, ITU-D Secretariat DRAFT, January 2008

- Available at: http://www.itu.int/ITU-D/cyb/

2007 Report on Policies to Protect the Critical Information Infrastructure (Australia, Canada, Japan, Korea, The Netherlands, United Kingdom, United States)

- Available at: www.oecd.org/sti/security-privacy

International CIIP Handbook 2006:

- Volume I: An Inventory of 20 National and 6 International Critical Information Infrastructure Protection Policies
- Volume II: Analyzing Issues, Challenges, and Prospects
- Available at: http://www.crn.ethz.ch/publications/crn_team

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