Infrastructure Dependencies: The Big Rocks Panel - Private Sector Perspective

DIB CIP Conference, 24 August 2011

Guy Copeland, Vice President, Information Infrastructure Advisory Programs and Special Assistant to the CEO, CSC
Co-Chair, Cross Sector Cyber Security Working Group (CSCSWG)
Sector Partnership Model

National Infrastructure Protection Plan (NIPP)

Critical Infrastructure Partnership Advisory Council (CIPAC)
Cross-Sector Cyber Security Working Group
CIPAC Framework and Liaison Groups

- NIPP Federal Senior Leadership Council (FSLC)
- Critical Infrastructure Protection Advisory Council Framework
- Partnership for Critical Infrastructure Security
- National Council of ISACs
- Other Ad-Hoc Groups as needed
- US-CERT
- Software Assurance Forum

Guy Copeland, CSC, Opinions in this presentation are solely those of the Presenter, not necessarily CSC. 08/24/2011
Dependencies on technology are greater then ever

- Possibility of disruption is greater than ever because hardware/software/people are vulnerable
- Economic disruption as serious as physical
- Loss of confidence alone can lead to stakeholder actions that disrupt critical business activities

Internet users in the world: 1,766,727,004
E-mail messages sent today: 215,674,475,422
Blog Posts Today: 458,972
Google searches Today: 2,302,204,936

Who is behind data breaches?
- 74% resulted from external sources (+1%).
- 20% were caused by insiders (+2%).
- 32% implicated business partners (-7%).
- 39% involved multiple parties (+9%).

How do breaches occur?
- 7% were aided by significant errors (<>).
- 64% resulted from hacking (+5%).
- 38% utilized malware (+7%).
- 22% involved privilege misuse (+7%).
- 9% occurred via physical attacks (+7%).


credit to Don Davidson, DoD
Private Sector Impact: *Interdependencies among infrastructures make a problem in one infrastructure a problem for all.*
Conclusions – We Have Known For Years Now

- National risk is growing, especially with asymmetric threats and increasing reliance on information & communications infrastructure

- Public confidence in infrastructures is critical

- Risk is shared among public & private interests

- New Thinking Required

Partnership is the Foundation for Critical Infrastructure Security
Partnership Principles

• Partnership must be voluntary
• Trust among partners is essential
• Working members must be personally responsible and accountable for their trusted behavior
• Objectives must be clearly defined and embody common goals
• Internal support and trust within each partner must exist
• Institutionalized process is important to provide lasting benefit
• Build on existing organizations first
• Working members of the partnership should frequently interact
• Partnership needs to be an evolving relationship
• Legal and liability issues can be powerful tools for aligning interests of the partners
• Partnership needs champions and institutional support
Successes and Challenges – a few examples

- National Infrastructure Protection Plan
  - Sectors, Sector Specific Plans and Risk Assessments
- National Level Exercises and Cyber Storm Exercises – joint
- Sharing through PCIS, National Council of ISACs, CSCSWG
- Private Sector Seats in NCCIC
- Cybersecurity is a Policy Concern and Priority
  - U.S. Senate: Lieberman-Collins, Rockefeller-Snow, Reid
  - Administration Legislation Proposal
  - International Strategy for Cyberspace
- Rapid Adoption of Cloud Computing
- National Broadband Plan and Public Safety
- Supply Chain and other international issues
- Telecom Energy Alliance Working Group
There are numerous successes and there remain numerous challenges!

Guy Copeland, CSC
703-876-1238, gcopelan@csc.com