CSC

Reconciling Protection and Resiliency - Information Technology Sector

Guy Copeland

Vice President

CSC

NDIA 2008
Homeland Security
Symposium & Exhibition
September 9, 2008

Protection and/or Resiliency

- **Protection and Resiliency**
  - **Not either/or**
  - **Different views of the same set of physical and cyber challenges to balance primarily on risk assessment**
- **CSC helps clients – government an private sector – achieve their strategic goals through the use of information technology, frequently as part of a solution set that also includes other technologies, management solutions, processes and deep mission or business understanding and expertise.**
- **Some of the world's most important service, financial, production and government institutions rely on CSC for continuity and availability (COOP and COG in government terms) – DHS, DoD, NASA,**

Preparation is Key

- **Risk Assessment, Priority Implementation, Training, Exercising and Feedback**

- **The communications backbone, the power distribution grid and IT functions and services are designed to be highly robust, BUT ……**

- **Specific facilities must consider site, equipment, connectivity and personnel redundancy needs – e.g., Tier III data centers must achieve 99.98 percent availability (no more than 4 hours of unplanned outage every 2.5 years)**

- **Pervasive management support and employees as the lynchpins**

- **Katrina and Rita Lessons: *"Planning and teamwork were the keys to our success. Luck alone won't take you very far when you have to go to plan B and start thinking on your feet. We learned a lot during this event, and will factor these lessons into our recovery plans for the future."***

  – *Deborah Hojem, CIO, DynMcDermott's CIO.* **a CSC subsidiary that operates and manages the US Strategic Petroleum Reserve.** *The SPR is the world's largest reserve of crude oil, which is stored in underground caverns along the Gulf of Mexico in Louisiana and Texas.*

Partnership is Key

- **President's National Security Telecommunications Advisory Committee (NSTAC)**
  http://www.ncs.gov/nstac/nstac.html

- **National Coordinating Center for Telecommunications (NCC)**
  http://www.ncs.gov/ncc/index.html

- **Network Security Information Exchanges**
  http://www.ncs.gov/nstac/reports/fact_sheet/NSTAC_08.pdf

- **Information Technology Information Sharing and Analysis Center (IT-ISAC)**
  https://www.it-isac.org/

- **ISAC Council**
  https://www.isaccouncil.org/

- **Partnership for Critical Infrastructure Security (PCIS)**
  http://www.pcis.org/

- **Cross Sector Cyber Security Working Group**
  http://homeland.house.gov/SiteDocuments/20071031154922-91266.pdf

Cyber is Critical

- **Cyber "Hurricane" is hitting us all – some more than others – 24/7**
- **Risk Assessment, Priority Implementation, Training, Exercising and Feedback all apply**
- **The communications backbone, the power distribution grid and IT functions and services are designed to be highly robust, BUT ……**
- **Consolidate for manageable span of protection and response**
  - **DoD and DHS strategy to consolidate and simplify**
  - **Reduction in Internet access points**
- **Certification and Accreditation**
- **Best Practices**
- **Education and awareness**
- **Identity, Access and Privilege Management appropriate to the assets, functions and services to protect**
  - **CSC Center of Excellence because this is critical to virtually everything**

Exercise to Verify and Learn

- **Internal**

- **External – National level (e.g., TOPOFF, Cyber Storm, NLE 2-09)**

- **CSC and other companies participated in Cyber Storm II - A national cyber security exercise to test processes and capabilities of companies and agencies in both the private and public sector.**
    - CSC Objectives
        - » Opportunity to evaluate operations in a national scenario with partners
        - » Learn lessons for needed improvement
        - » Build upon existing continuous improvement for preparation and response posture

- **The largest government-sponsored national cyber security exercise of its kind.**

- **Exercises such as Cyber Storm II are critical in maintaining and strengthening cross-sector, inter-governmental and international relationships, enhancing processes and communications linkages, as well as ensuring continued improvement to cyber security procedures and processes.**

Operational Exercise Benefits

- **Operational Exercises' Benefits Include**
  - **Experience in and development of external interaction for major incident handling**
  - **Participation with major international, national, state and local, and private sector players**
  - **Exercise, test and advance the CONOPS for the IT-ISAC**
    - **CSC is a Founding Member and part of the executive committee leadership**
  - **Exercise vendor partnerships - investigate key supply chain dependencies**
  - **Exercise NOC/SOC organizational incident response processes**
  - **Demonstrate and recognize employee skills and leadership**
  - **Support for participating clients (e.g., DHS, EPA, DoS, GETS)**
  - **Education and awareness opportunity – direct and indirect**

Learn More

- **Be active in the Critical Infrastructure Protection community**

  - **Government and private sector**

- **Join your Sector Coordinating Council**

- **Join your Information Analysis and Sharing Center**

- **Participate in exercises through the SCC and ISAC**

- **Help with your sector's risk assessment and other implementation of your sector's specific plan**

- **Participate actively**

- **Apply lessons learned internally**

- **Ask your sector's CIP leadership how you can help**

Guy Copeland

Vice President

Information Infrastructure Advisory Programs

and

Special Assistant to the CEO

CSC

3160 Fairview Park Drive

Falls Church, VA 22042

gcopelan@csc.com