



# **TECHNOLOGY LEADERSHIP CONFERENCE**

March 25-27, 2008  
San Diego, CA



American Council for Technology



Industry Advisory Council

Leading the IT Community to Improve Government



TLC | 2008  
SHOWCASING  
REGIONAL  
RESILIENCY

# Disclaimer

- My comments are my own & do not necessarily reflect the opinion or position of my company



# Panel Question

*What exactly is the nature of this [cyber] threat & how are public & private organizations working to detect, respond to & mitigate cyber attacks?*

# NERC CIP

- NERC Critical Infrastructure Protection
  - Cyber security standard reflects ISO 27002
  - CIP 001 Sabotage Reporting
    - Develop recognition & reporting procedures
    - Provide employees guidelines on same
    - Report breaches to “appropriate parties” & local FBI
  - Important step for utilities, but still behind where critical infrastructure needs to be

# Beyond NERC CIP

- Move from reactive detective controls to proactive preventative ones
- Perimeters are living (moving) things. Focus on the information, not on logical lines
- Communicate better & without fear of unintended disclosure or reprisal



# Communicate Better

- Security Awareness: more than e-mail & web-based training to employees
- It's internal & external
- It's sustained behavior modification through
  - Developing relationships
  - Disparate delivery mechanisms
  - Integration into business processes
  - Fresh perspective on repetitive topics



# Informal Relationships

- Local informal relationships may provide significant value
    - Consider the value of
      - key local companies,
      - federal & local law enforcement, &
      - the city
- meeting once a month for lunch to discuss security concerns