



SCADA Security

What Keeps us up at Night

**API IT Security Conference
November 11, 2009
Houston, TX**

M. E. DuBois



Nightmare Scenario

- u 4:10 AM The Wake Up Call
- u 4:30 AM SCADA Flows go to Zero
- u 4:40 AM See the Ransom Instructions
- u 5:00 AM SCADA is DARK
- u 5:35 AM Disaster Recovery Site Activated
- u 7:00 AM All systems at DR Appear to Function Normally
- u 7:30 AM THE QUESTION IS ASKED



The Good Ole Days

- u SCADA was highly segregated
- u Proprietary Equipment and Protocols
- u Specialized and Distinct Communications Channels
- u High Availability Server Environments
- u Vendors (note Plural)

- u **ISOLATION and OBSCURITY**



Modern SCADA Environment

- u Integrated into Business – Real Time Data
- u Internet T1's – Cheap and Fast
- u Windows Based Platforms
- u Consolidation of Vendors

- u Post 9/11 Awareness of Threats



Additional Sleepless Hours

Vendor and Platform Challenges

- u Patching SCADA Servers in a 24/7 Environment
- u Active Directory Management
- u Stability and Flexibility Expectations not yet met



Additional Sleepless Hours

The Information Challenge

- u Lack of Actionable Data
- u Lack of Specific Data
- u Credibility Gap Between Government and Industry



Additional Sleepless Hours

The Mis - Information Challenge

- u Infrastructure has Already Been Infiltrated
- u Hacker attack in Australia – Really Trusted Insider
- u Linking of Cyber to Past Pipeline Accidents
- u Gap Between Risk Based Thinking and Consequence Based Demands



Ambien® for the CIO Soul

- u Open Partnerships with Government
 - National Labs
 - TSA/DHS
- u Open and Honest Collaboration with Vendors
- u Disciplined Cyber Security Programs – Not a Project but a Practice



And in the End

ISOLATION of the SCADA Environment



Closing

Thanks

For your

Indulgence