American Electric Power

CSOC Threat and Information Sharing

H Kevin Stogran
Director – IT Risk Services
Risk and Compliance Management
Information Technology
American Electric Power

At AEP, we dedicate ourselves to providing reliable, affordable service and shareholder value, with a continued focus on safety.

Headquartered in Columbus, Ohio, AEP is one of the largest electric utilities in the U.S., serving over 5 million customers in 11 states.
Our major businesses include:

- **Regulated Utility Operations**
  Seven regional electric utilities serving customers across 11 states.

- **Transmission**
  The nation's strongest transmission network, with a national vision for the nation's power grid.
  - 39,000-mile electricity transmission
  - More 765 kilovolt extra-high voltage transmission lines than all other U.S. transmission systems combined

- **Power Generation**
  One of the nation's largest, most efficient, and most innovative generation fleets with nearly **38,000 megawatts** of generating capacity.

- **AEP Energy Partners**
  Providing electric supply to customers in deregulated electricity markets.

- **River Operations**
  One of the nation's largest barge companies, transporting coal and other cargoes.
AEP Service Territory

AEP Operates one cyber network over 11 states
Problem Statement

- Don't Re-invent the Wheel
- Improve Staff Capabilities
- Improve Situational Awareness of Attackers & Threat Vectors
- Force Multiply on the Fly
- Maintain Confidentiality of Events
- Optimize Costs

Improve Cybersecurity for Better Resiliency?
The Idea
• Leverage existing threat sharing models
• Protect the gridSMART network
• Quickly expanded to the full enterprise network
• Partnering with
  • Lockheed Martin (DIB)

Funding
• Initial 2009 AEP Ohio gridSMART Stimulus from DOE.
• On-going – Membership Dues

Pilot Demo
• Spring 2011
• Initial deployment of CSOC Portal
• 30+ companies, each with one piece of data
• Strength of Sharing

CSOC Threat & Info Sharing Portal
• Secure website
• Operational July 2012
• Membership Governed & Funded
Threat Sharing - Circles of Trust

- **General Industry**
  - DHS ICS-CERT / US-CERT (10,000’s)

- **NERC’s ES-ISAC**
  - (1,000’s)

- **CSOC TIS Members**
  - (10’s)

**Data Attributes**
- Non Attributed Data “Public”
- Utility Known & Specific Data “Trusted” & Confidential
### CSOC TIS Portal Membership Benefits

<table>
<thead>
<tr>
<th>Governance</th>
<th>• Governed by Participant Steering Committee.</th>
</tr>
</thead>
</table>
| Trust      | • Close circle of trusted peers. (Will never be large community)  
|            | • Complementary to NERC ES-ISAC.            |
| Membership | • Membership vetted by current members (Not a public organization).  
|            | • Membership list is confidential.          |
| Training   | • Monthly Analyst Training  
|            | • Twice Annual Classroom Training           |
| Funding    | • Participant funded.  
|            | • Total operating costs / active members = annual membership fee. |
| Agreements | • Participants signed standard CSOC Agreement with AEP |
| Staff Multiplier | • Allows close peers to contribute on threat analysis. |
Program Successes

- Low cost to achieve.
- Community contribution of threat vectors.
- Early identification of industry attack vectors.
- More eyes on the game.
- Advanced training for SMEs.
- Analyst peer community and outreach.