Information Security at Austin Energy

Update to Electric Utility Commission

12/11/2017

Information Security Challenges

- Risk management process
- Data Governance
- Vendor data security and handling
- Internal controls
- Continuous assessments

Risk Management

- AE faces information security concerns at all levels of the organization and across all business units, with risks to all major strategic goals:

- Implementing industry best-practices from DOE and NIST for managing cyber security risk
  - Ensuring correct internal organization/roles/policies
  - Coordinating executive level committee in charge of policy and decision making that meets quarterly
  - Leveraging existing staff committees to support the information security risk management

Data Governance

- AE handles confidential information at all levels of the organization and is faced with constant outside requests for information and increasing interactions with systems and parties outside our network.
- Strengthening internal roles and responsibilities with respect to accountability and data governance
  - Established a new Data Council to evaluate/develop access policies
  - Ensuring enterprise awareness of what data we are required to keep confidential (customer, security) and why, and controls available/required before sharing

Vendor/Partner Data Security

- Business increasingly uses/gets value from cloud services and third parties that access our confidential information
- Managing the risk of data security with our vendors
  - – Developed a standard Data Handling Controls (DHC) document that spells out standard requirements for each counterparty
  - – Collaborating with purchasing and contracts teams to ensure DHC considered
  - – Ensuring checks/balances in place so appropriate contract terms are used w/o limiting competition

Internal Controls

- Business units require increasingly more and complex hardware and software that must be monitored
- Strengthening our vulnerability management practices
  - – Leveraging new system security monitoring tools
  - – Building a new Security and Network Operating Center
  - – Collaborating with federal and local agencies including law enforcement on imminent industry threats

Continuous Assessments

- Measuring how “well” we manage information security across the enterprise in a dynamic threat environment
- Leveraging available industry-best practice cybersecurity maturity assessments
  - Current posture is good relative to industry averages
  - Identified areas for improvement including asset and data inventories