Information Security at Austin Energy

(with contribution from the City CISO)

Update to Austin Energy Utility Oversight Committee

5/23/18

Hacking – Some History

- 1976 - Data Encryption Standard is approved for the first time
- 1985 - The first PC virus is created. Named Brain originating in Pakistan
- 1988 - Robert Morris, 22, launches the Internet Worm spreading to 6,000 computers, 1/10 of all computers on the Internet; sentenced to 400 hours of community service, and a $10,000 fine.

So far in 2018

- Over 25 major incidents compromising billions of individual persons confidential data
  - Schneider Electric forced to shut down power plants in Middle East after Industrial Control Systems are infected
  - Data breach of Under Armour compromised the information of 150 million users of fitness & nutrition tracking app MyFitnessPal
  - Atlanta did not bill for water for a month and a half

Applicable Laws, Rules & Regs

- NERC CIP Reliability Standards
- HIPAA
- Payment Card Industry (PCI) rules
- Personally-Identifiable Information (PII)
- Texas State records and information management laws
- COA information protection (COA Ordinance 2-11)
- Fair and Accurate Credit Transactions Act of 2003 (FACTA)
- Privacy Act of 1974
- Clinger-Cohen Act of 1996 (IT Management Reform Act)
- Computer Fraud and Abuse Act of 1986
- Computer Matching and Privacy Protection Act of 1988
- E-Government Act of 2002
- Federal Information Security Management Act (FISMA) of 2002
- Rehabilitation Act of 1998 Section 508
- Federal Trade Commission Act

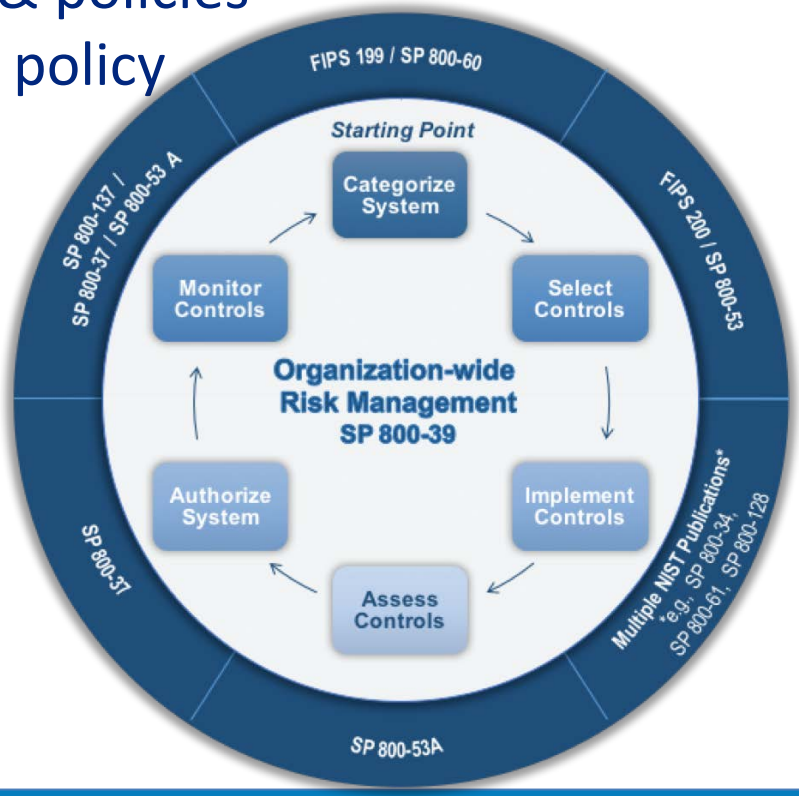
Elements of an Enterprise Security Program

- Risk Management Framework
- Data Governance
- Vendor or Partner Data Security
- Internal Controls and Vulnerability Management
- Continuous Threat Assessment

NIST Risk Management Framework

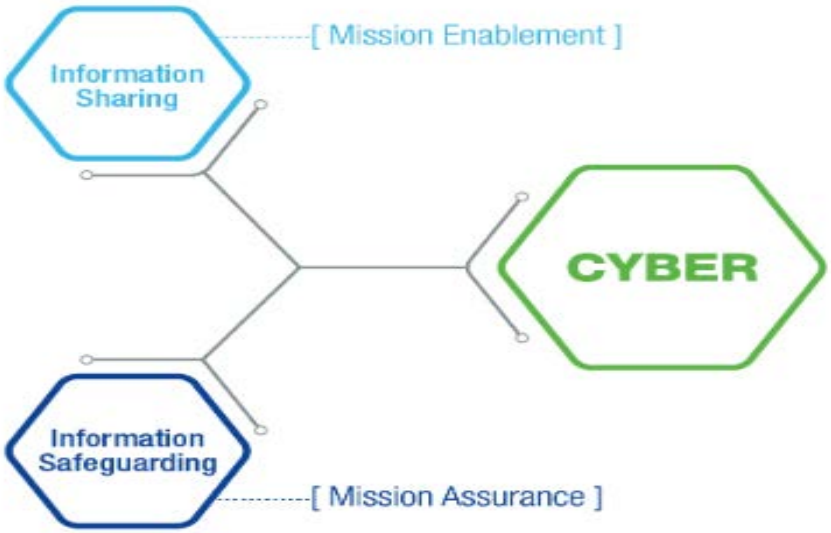
- Integrates security and risk management activities into system development life cycle
- Considers effectiveness, efficiency and constraints due to applicable laws, directives, Executive Orders, policies, standards or regulations & defines internal roles & policies
- Executive level committee in charge of policy

- Process:
  - Categorize systems
  - Select controls
  - Implement controls
  - Assess controls
  - Authorize system
  - Monitor controls



Data Governance

- Austin Energy handles confidential information at all levels of the organization and is faced with increased data interactions with systems and parties outside its network.



➢ Strengthening internal roles and responsibilities with respect to accountability and data governance

- New Data Council to evaluate/develop access policies
- Enterprise awareness of controls available/required before sharing confidential data (customer, security) and why

Vendor/Partner Data Security

- We have increased use of cloud services and third parties that access our data
  - Data Handling Controls (DHC) document spells out requirements for counterparties
  - Collaborating w/ purchasing/contracts teams to ensure DHC applied appropriately
  - Audit vendor adherence to DHC

Internal Controls & Vulnerability Management

- Business units require more and complex hardware & software which IT must monitor

- Strengthening vulnerability management practices
  - Leveraging new security monitoring tools
  - Building Security/Network Operating Center
  - Strengthening patch management procedures
  - Collaborating w/ law enforcement on industry threats

Continuous Assessments

- 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