Cybersecurity & Energy

Michael Goin, CISSP
michael.goin@austinenergy.com
February 8, 2017

Resilience

- Fault Tolerance
- Disaster Tolerance
- People

Resilience – Fault Tolerance

- Design systems to actively recover from a failure with no / minimal interruption to service:
  - Identify critical resources
  - N+1 configurations or greater
  - Clustering Technologies
  - Local fail-over documented, tested
  - Virtualization
  - Redundant paths (network, power, infrastructure)

Resilience – Disaster Tolerance

- Design systems to support a return to operations (RTO) within a specific timeframe.
  - Remote fail-over capabilities
  - Vendor relationships
  - Exercise:
    - Disaster Recovery Plan (and UPDATE it)
    - Alternative / Manual Process

Resilience – More

- Remember to focus on things besides Technology:
  - People (physical attack, pandemic, etc.)
  - Facilities (loss of data center, key resource, etc.)
  - Infrastructure (roadways, cell-service, Internet)

Resilience – People

- Quick Focus on People
  - Develop a culture of SAFETY
    - Corrective Action Program
    - Active Safety Education & Awareness
  - Document your processes
    - Include this action with employee reviews
  - Know you can staff critical roles

Protecting Critical Assets

- Identify your critical assets
- Incorporate security controls (huge)
  - administrative
  - technical
  - physical

Protecting Critical Assets

- Security Control Overview
  - Inventory
  - Patch Program
  - SIEM – monitor, monitor, alert
  - Incident Response Plan
  - Vulnerability / Risk Management Plan
  - Culture of Security Awareness
    - AND improved behavior

Relationships

- Vendor Partners
  - Know your vendors
  - Who to call
  - What service to expect (timelines)
  - Have a backup

Relationships

- Utilities
  - Good working relationships within organizations such as:
    - LPPC
    - APPA
    - RMEL
    - EPRI
  - Why?
    - Consistency
    - Best practices
    - Awareness

Relationships

- Government
  - DHS, FERC (NERC), FBI, PUC

- Why?
  - Cybersecurity Awareness (DHS AIS)
  - Regulatory Compliance (NERC)
  - Information Sharing / Reporting (ALL)

Relationships

- Customers
  - Be of service to the community
  - Be present (events, parades, etc.)
  - Be an asset to the community

  - Be the source for problem resolution
    - All calls are important
    - All outages must be minimized

  - Be the best stewards of rate payer dollars

Relationships

- Customers
  - Instill confidence, promote community culture
    - Green Energy
      - Solar
      - Wind
      - BioMass

Relationships

- Customers
  - Always deliver the best possible service
    - System Average Interruption Frequency Index
      - SAIFI: 0.61 (average # of interruptions)
      - Average service interruption frequency of 5 minutes or more per customer during a 12-month period
    - System Average Interruption Duration Index
      - SAIDI: 50.21 (average # of minutes)
      - Average service interruption duration per customer on the electric system during a 12-month period

UT Energy Week

- Thanks