Do You Need to Dust off Your ERP?

Michael Goodroe, Sawnee EMC
Elaine Johns, EnerVision

NRECA TechAdvantage Conference
Nashville, TN
February 27, 2018
Today’s Speakers

Mike Goodroe
President/CEO
Sawnee EMC

Elaine Johns
President/CEO
EnerVision, Inc.
Emergency Response Planning and Tabletop Testing

- Introductions
- ERP + Tabletops Background
- The Document
  - Vulnerability Risk Assessment
- Tabletop Exercises
- Closing Thoughts
Sawnee EMC

- Headquarter in Cumming, Ga.
- Serves 176,000 meters
- Has 142,000 members
- 12,000 miles of physical plant
- 245 employee
- 80th anniversary
EnerVision, Inc.

- Management and technical consulting firm, specializing in electric cooperatives
- Came out of Oglethorpe Power Corporation 1997 restructuring
- Services over 130 cooperatives in over 35 states
- Sawnee EMC is one of our first clients

😊
Objectives

Leave today with the following:

- **Emergency Response Planning** = Disaster Response + Business Continuity
- **Components of an Emergency Response Plan (ERP)**
  - Supply chain planning
  - Redundancies for critical systems
- **Importance of Tabletop Exercises**
ERP Background

- Not just Disaster Recovery, it’s also Business Continuity
- FEMA, DHS, RUS, PCI
- Tabletops

“Tabletop exercises are table-based activities typically held in an informal setting and presented by the Facilitator. There is no hands-on practice or field work. This type of exercise is intended to generate discussion of various issues regarding a hypothetical, simulated emergency.” FEMA, 2013
ERP Document

- A Manager’s Must Have’s
  - Chain of Command
  - Board Communication
  - Emergency Levels and Activation Plan
Chain of Command

- In the event, CEO is not available
- SEMC Chain of Command Policy
  - Definitions
    - “not available”
    - “disaster”
  - Defined chain of command
  - Conditions of Succession
Board Communication

- Throughout the entire document
- Specifically in Communications and Public Relations section
- CEO determined
- Board members kept abreast of key issues, restoration efforts and possible advocacy
Emergency Levels and Activation Plan

- **Emergency Activation Levels**
  - Level 1: Weather or Hazard Alert
  - Level 2: Partial ERP Activation
  - Level 3: Complete ERP Activation

- **Calling Internal Emergency Meetings**
SEMC’S ERP DOCUMENT
## Requirements/Objectives of RUS

### Vulnerability and Risk Assessment (VRA)
- Critical facilities and business functions:
  - National security
  - Reliability and security of grid
  - Significant risk to safety and health of public
- Criticality and risk level associated with assets
- External impact (interdependency)
- Threats and vulnerabilities
- Existing & additional mitigation procedures

### Emergency Restoration Plan (ERP)
- Procedures for response and restoration efforts in event of major system outage
- Key contact information
- Key utility management and other personnel
- Chain of command and delegation of authority responsibility
- Recovery procedures in case of loss of power to headquarters, key offices, or operation center facilities
- Business Continuity section
- ERP available to key personnel

### Annual ERP Exercise*
- Verify, at least annually*:
  - Operability of alert and notification systems
  - Efficacy of ERP
  - Employee competency with ERP procedures
  - Points of Contact (POC) of key personnel – internal and external
  - Contact numbers for POCs

*Per RUS, a borrower may exercise its ERP in a number of ways:
- After natural event that requires utilization of ERP
- Participation in joint exercises with other utilities
- Tabletop exercise
Vulnerability and Risk Assessment (VRA)

Recognized by *RUS Bulletin 1730B-2* as an effective decision supporting tool for prioritizing and determining sites and functions within a business in need of security investment and development of a meaningful ERP

\[ \text{Risk} = \text{Threat} \times \text{Vulnerability} \times \text{Asset Value} \]
VRA Objectives

- Understand the utility’s critical facilities and business functions
- Identify threatening vulnerabilities of critical facility systems
- Understand system design and operations in order to determine likelihoods of failure
- Identify consequences of system failures
- Recommend facility improvements to reduce vulnerability
Core of the VRA Methodology

Risk Assessment
- Universe of Potential Threats
- Likelihood of Event/Attack
- Infrastructure Interdependencies
- Existing Asset Protection
- Prioritization of Critical Facilities and Business Functions

Risk Mitigation
- Incremental Cost of Best Practices to Reduce/Limit:
  - Vulnerability
  - Damage/Consequences
  - Restoration Time

Mitigation Priorities
- Existing Asset Protection/Mitigation

= Gap Analysis and Cost/Benefit

Screen

Potential Debilitating or Material Financial Impacts on:
- National Security
- Mission Critical Operations
- Stakeholders Deemed to be Critical
SEMC ERP Table of Contents

1. Electric Distribution System
2. Corporate Campus
3. Key Business Assets
4. Communications and PR
5. Cybersecurity
6. Pandemic
7. FEMA and GEMA
Examples of Supply Chain Planning

- **Off Site Facility**
  1. Location
  2. Space requirements
  3. Parking facilities
  4. Phone system
  5. Computer network
  6. Lease requirements
  7. Others
     - Fenced area for vehicles and supplies
     - Cubicles and office space
     - Conference rooms
     - Restrooms
     - Breakroom (desirable)
Examples of Supply Chain Planning

- **Emergency Outage Shift Procedures**
  - Objectives
    1. Establish a rotation of staff schedules
    2. Obtain efficiency and effectiveness during major disruptions
  - Work schedules
    1. Call Center and Non-Operational Support Staff
    2. Operational and Operational Support Staff
    3. Contract Personnel
Examples of Critical Systems

- Phone System – PRIORITY 1
  - Primary Contacts
  - Risk Mitigation
  - Key Restoration Procedures
    - Land line failure
    - Phone switch failure
    - Internal wiring failure
Examples of Critical Systems

- **OMS – PRIORITY 4**
  - Primary Contacts
  - Risk Mitigation
  - Key Restoration Procedures
    - Main OMS server failure
    - File corruption
    - Network or local system failure
Evaluation of Emergency Response

- Post-event observation/Self-critique
- Revise the ERP
- Staff meetings
- Annual testing of ERP
TABLETOP EXERCISES
SEMC’s Tabletop Exercises 2017

- **Two Scenarios**
  1. Active Shooter
  2. Social Media and Hacktivism

- **Two Observers**
  - DHS Protective Security Advisor, Georgia
  - DHS Cyber Security Advisor, Region 4
Scenario 1: Active Shooter

How to Respond When an Active Shooter Is in Your Vicinity

Quickly determine the most reasonable way to protect your own life. Customers and clients are likely to follow the lead of employees and managers during an active shooter situation.

1. Run
   - Have an escape route and plan in mind
   - Leave your belongings behind
   - Keep your hands visible

2. Hide
   - Hide in an area out of the active shooter’s view.
   - Block entry to your hiding place and lock the doors

3. Fight
   - As a last resort and only when your life is in imminent danger.
   - Attempt to incapacitate the active shooter
   - Act with physical aggression and throw items at the active shooter

Call 911 when it is safe to do so.
Location

- Sawnee EMC
- Headquarters Building
 Inject #1

- Date: Friday, February 9
- Time: 10:30 am EST

- A member of your finance department, who has been with your company for eight years, has just been terminated. As he is escorted out of the building by security, he tells them they will regret treating him like this.
Inject #2

- Date: Monday, March 12
- Time: 9:00 am EST

- A popping sound is heard within the building.
- An employee runs into your office shouting that there is a man firing a gun in the hall.
Inject #3

- You decide to shelter in an office, and secure the immediate area.
- The popping noises seem to be coming from your floor.
- There is yelling and screaming outside your door.
- A woman knocks frantically on your door pleading to be let in.
ETC.
Scenario 2: Social Media and Hacktivism

- **Materials – Cyber Incident Response Plan**
  - Incident Management Policy
  - Components of Training
  - Components of Incident Response Plan
    - Incident Preparedness
    - Incident Detection and Analysis
    - Containment, Eradication and Recovery
    - Post-Incident Analysis and Forensic

- **Review ERP document for process and editing**

- **Review Tabletop Exercise**
A SEMC employee sends the following email to the HR Department:

Subject: Official complaint

I want to register an official complaint and make you aware of a situation involving Mr. X.

Shortly after Mr. X joined the organization, we became Facebook friends. Recently, Mr. X has posted some very offensive opinions regarding women in the workplace. It not only upsets me, it has a lot of other people worked up on Facebook. You need to look at Mr. X’s Facebook page.

Please advise and address. Thank you!
Inject #2

- Two days later, HR discovers that Mr. X’s inflammatory comments have been posted on LinkedIn.

- Furthermore, one person commented, “How can a person like this even find a job?”

- Others have doxed him and linked him to SEMC as his employer.
Inject #3

- The next morning, SEMC’s website is taken down for 10 minutes due to a Distributed-Denial-of-Service (DDoS) attack.
- SEMC’s hosting company re-routed traffic and got them back online, but not before there were customer complaints about accessing their accounts.
- The hosting company tells SEMC they are being heavily scanned from dozens of source IP’s.
- Review of social media sites indicate that SEMC is being targeting by a large hacktivists group. They are demanding the immediate firing of Mr. X and an apology on the SEMC website.
Later in the day, many employees report receiving phishing emails.

On further analysis, it is discovered that several employees have provided their network credentials.

Compromised credentials appear to have been used prior to IT blocking the phishing emails and resetting passwords.

A local news channel has contacted SEMC.
ETC.
Hotwash

- How do you think it went overall?
- What did you learn from this exercise?
- What are the areas of concern at this point?
- What action steps are needed/changes to ERP, based on lessons learned?
  - Plans
  - Procedures
  - Training
  - Other Suggestions
- Who has responsibility for each action step?
Closing Thoughts

- Be Effective
  - Thorough
  - Practice
  - Use
  - Update

- Use What You Have
  - Neighboring coops
  - Other coops
  - Statewide

- It’s a Living Document
Thank You!

Booth #1518