TEXAS UTILITIES

Cybersecurity Monitor Outreach Program

2023

Managed By

PARAGON SYSTEMS

Program Overview & History

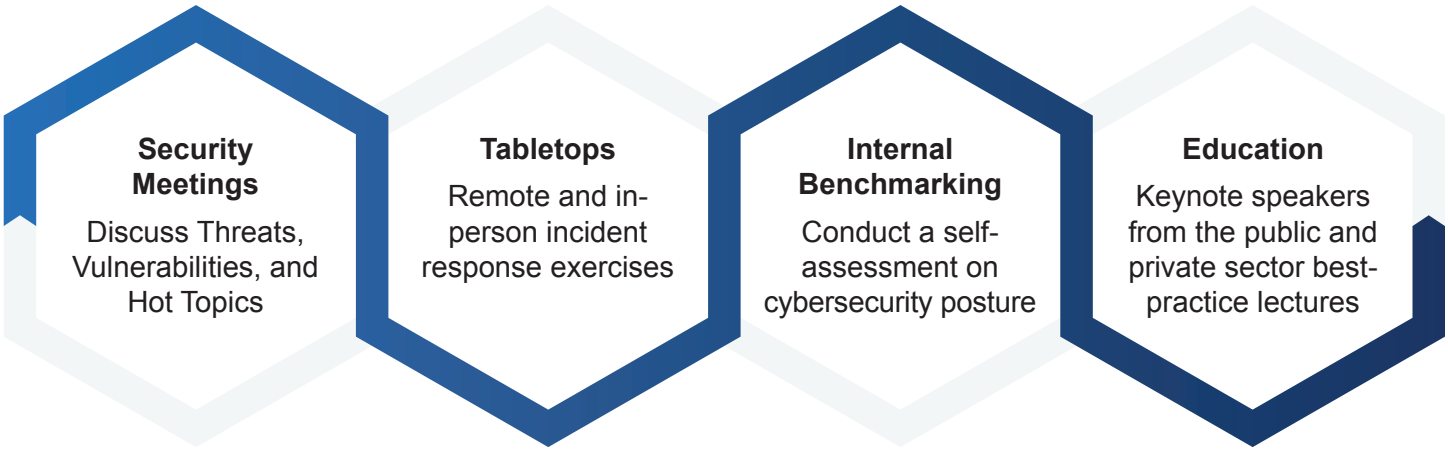
Background

In May 2019, Texas State Senate Bill 936 was passed, which required that the Public Utility Commission of Texas (PUCT) and the Electric Reliability Council of Texas (ERCOT) foster a more collaborative, strategic approach to identifying vulnerabilities and finding areas to improve security measures across Texas's critical electric infrastructure.

Our Role

Paragon Systems was selected as an independent agency by the PUCT to serve as the state's Cybersecurity Monitor. The purpose of the Cybersecurity Monitor is to develop a voluntary Outreach Program to promote collaborative discussion on cyber and physical security between the Public Utility Commission of Texas (PUCT), Electric Reliability Council of Texas (ERCOT), and participant Monitored Utilities (MUs) by which Monitored Utilities can express awareness and preparedness through their governance, practices, and training.

Program Components



Program Goals

1. Independent Self-Assessment & Recommendation's Report
    - Not a compliance exercise
2. Information Sharing
    - Examples include: Threat's & Trends, Statewide Resource Needs, etc.
3. Cybersecurity Training
    - Provide recommendations and identify available resources related to self-assessment identified focus areas
    - Biennial Incident Response Tabletop Exercise

Security Meetings

Security Meetings are held quarterly between Paragon Systems and participating utilities to provide opportunities for utilities to interact with one another to discuss concerns, emerging threats, and trends facing Texas electric utilities. These meetings also include industry specific security briefings and training sessions, designed to inform and educate.

Purpose

The purpose of Quarterly Security Meetings are to provide a secure environment for utilities to share information regarding threats and best practices.

Participants

Participants include a variety of technical and non-technical analysts and decision makers, e.g., CISOs, Cybersecurity Analysts, City Managers, General Managers.

Time & Place

Security Meetings are quarterly affairs held in March, June, September, and December. They are virtual meetings and participants are pre-screened prior to entry.

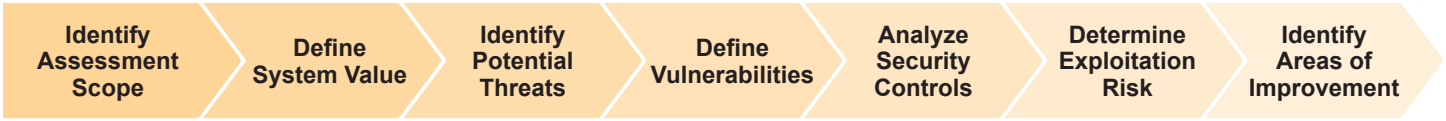
Keynote Speakers

Security Meetings are forums for expert speakers to delineate valuable information and resources. Past speakers include:

- Leach Strategic Partners
  - » Counter Unmanned Aircraft Systems
- Michael Best, LLP
  - » Top Ten Steps to Building a Cyber Incident Response Plan and Procedure

Self-Assessments

Self-assessments are comprehensive surveys designed to evaluate a utility's cyber and physical security efforts. The average time to complete and submit a self-assessment is expected to be one to two weeks of part-time work. The Cybersecurity Monitor is available to assist utilities with the self-assessment should they run into any issues, however, the process is intended to be completely self-sufficient. Self-assessments and any related information will be kept secure and confidential. They are submitted to the Cybersecurity Monitor through secure means and individual assessments will be kept secure and confidential.



Framework

Utilities are measured based on a modified version of the Cybersecurity Maturity Model Certification (CMMC) which comprises 17 cybersecurity domains (see graphic below). All self-assessments are distributed and collected via secure mail using two-factor authentication. To minimize complexity and the volume of questions, our modified framework utilizes three levels of increasing maturity instead of five. The assessment is mapped to the three most popular frameworks among utilities:

- NIST CSF - National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)
- NERC CIP - North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection
- C2M2 - U.S. Department of Energy (DOE) Cybersecurity Capability Maturity Model

Tools & Control

The self-assessment tool is an accessible Excel workbook developed specifically for Texas electric utilities, that emphasizes ease of use, and clarity, while ensuring it objectively captures cyber and physical security maturity. The workbook asks control questions, provides extensive help and includes a real-time implementation scorecard.

Maturity Improvement Reports

Maturity Improvement Reports (MIRs) are analytical reports that provide utilities with both a baseline analysis of the self-assessment results along with best-practice recommendations. Reports are authored and circulated to individual utilities upon completion of the self-assessment.

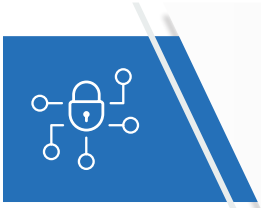
Report Components

Charted Self-Assessment Responses by Practice Area

- Control Area Scorecards
- Graphical representation of the maturity based on responses

Recommendations Based on Control Area Response

- Scorecard Result
- Recommendation
- Other Framework Mappings



General Cybersecurity Awareness Recommendations

Examples Include:

- Ransomware
- Social Engineering

Resource and Tools

Zero-cost best-practice resources for areas of improvement such as Frameworks, Tools, & Templates

Report Deliverables

- Self-Assessment Charts
- Recommendations Based on Response Thresholds
- Resources for Continuous Education
- Cross-Reference Responses to Other Frameworks
- General Recommendations
- Additional Resources & Tools to Promote Cyber Maturity

Tabletop Exercises

The Cybersecurity Monitor holds a recurring Cybersecurity Tabletop Exercise, similar in purpose to the biennial NERC Grid Security Exercise (GridEx). It is intended to be a cybersecurity-focused incident response (IR) training opportunity, designed to simulate a realistic scenario that focuses on a utility's capability to detect, identify, protect, respond, and recover from an attack.

Purpose

- Provide a forum for participants to test their incident response plan
- Provide an opportunity for utilities to work with one another on a simulated attack scenario
- Obtain documented exercise feedback that can be easily digestible across the organization

Benefits

- Identifies potential issues with IR strategy without causing any disruption to production systems
- Enables staff to better understand their individual roles and responsibilities
- Facilitate better coordination
- Help to inform decision-making

Virtual

- In April and June of 2022, we ran two exercises in collaboration with NUARI
- Participants played via the DECIDE platform which utilized email and chat functions to drive the scenario and injects
- Post-Exercise, participants were given an After-Action Report which emphasized observations at the group level and offered recommendations

In-person

- On November 9th, 2022, we hosted a tabletop exercise on the campus of Texas A&M
- Over 40 participants across dozens of utilities engaged in a progressively unfolding cyber incident scenario consisting of a phishing and ransomware attack
- Post-Exercise, an After-Action Report, which provided in-depth coverage of the scenario and questions, was circulated to participants

Participant Feedback

Program Feedback

"Learn about real world attacks and how to defend against them"

"Understand government agencies and their overlapping roles"

Tabletop Feedback

"Objectives and scenarios were realistic and applicable to what we do"

"The training was very good and always an important item to practice on a regular basis"

Self-Assessment Feedback

"Useful and easy to understand"

"The information received improved my understanding of best practices and available resources"

Texas Cybersecurity Monitor Team

TERENCE GILL
Project Manager/Business Analyst (PM/BA)

Prior experience includes: Banking, Insurance, and Information Technology

ROGER SIMMONS
Cybersecurity Subject Matter Expert (CSME)

Prior experience includes: Cooperative Utility, Department of Defense, State Government, Healthcare and Cloud Software

Paragon Systems is a subsidiary of SCIS (Securitas Critical Infrastructure Services, Inc.) with over 12,000 professionals specializing in security, fire, emergency response, investigations, inspections, cybersecurity, and mission support services to the US Federal Government and other critical infrastructure clients. Paragon Energy is the longest running specialized nuclear security provider in the industry with current contracts at operating and decommissioned plants across the country. Our clients are some of the largest utilities in the country, including Entergy, First Energy, Honeywell, and Duke Energy.

FOR MORE INFORMATION

VISIT OUR WEBSITE:
www.parasys.com/cybermonitor

SEND US AN EMAIL:
TXCSM@parasys.com

PARAGON SYSTEMS