NextGrid: Utility of the Future Study
Reliability, Resiliency, and Cyber Security Working Group Meeting No. 3
May 11, 2018

Working Group Leaders:
Manimaran Govindarasu
Dominic Saebeler

MEETING SUMMARY

[Note: descriptions of comments and discussion are condensed summaries and paraphrases]

Agenda Item I: Presentations

Presentations were given by the following:

1.) EPRI - Galen Rasche – Sr. Program Manager, Cyber Security
2.) Ameren Illinois - Eric Herr - director cyber security operations
3.) NERC – Bill Lawrence – Director of the Electronic Information Sharing and Analysis Center

Please refer to the slide deck presentations for additional information.

Agenda Item 2: Discussion "People" (commonly the weakest link in a security chain)

- *Challenge 1 "Ensuring a collaborative and consistent approach towards achieving a higher level of cyber and physical security"*
    - Opportunities - Building resiliency throughout ecosystem; growing employee skillset
    - Solutions - Capability measurement:
        - a. Baseline and advanced capabilities
        - b. Drivers' license type certification
    - Education - Achieving a baseline level of cyber and physical security competency among all personnel.
    - Comments:
        - We strive to mitigate risks, but understand we are not able to mitigate all risks. Should also focus on how do we respond and recover from an attack.

            - Military – view grid as a critical infrastructure that if affected, will severely affect the economy. Want everyone input on mitigation of risks, response, and recovery. Ex. - Grid X exercise.

- Working Group Leader (WGL)– want ideas put it matrix of recommendations on how to solve solutions. Is it appropriate to have some sort of minimum certification program? Ex. Driver license – certification required to operate vehicle.
    - Wouldn't recommend certification route, but list refences for readers to obtain some level of baseline knowledge.
- WGL- how many people would engage and how would we measure such engagement?
    - There could be privacy concerns or privacy issues if require driver's license and other sensitive information to measure participation.
    - When hear about some type of regulatory driver license certification, have red flags. If path were decided, we need to take into account the industry training we are already doing within the utilities to prevent redundancies.
- recommend having frequent collaborative type meetings amongst stakeholders throughout Illinois.

- *Challenge 2 "Improve mindset and institutional culture to optimize problem solving capabilities and avoid the "failure of imagination""*
    - Opportunities - Growing security subject matter expertise, aging workforce/turnover
    - Solutions - Avoid sensory data overload through use of tools like machine learning, data visualization
    - Comments:
        - Traditionally, there has been a barrier between operational technology (OT) & Information Technology (IT). Lays foundation for more integrated model for cybersecurity. Capacity is not there for OT teams to keep up with the fast changes in technology. There is not awareness that once make OT devise "smart", you just made on OT device an IT. Just because it's then an IT device doesn't mean it has to be IT managed, but still comes with vulnerabilities and risks as well.

- *Challenge 3 "Streamlining data sharing, security clearance, access to necessary intelligence while balancing the need to protect critical infrastructure information"*
    - Opportunities - Expedite security clearances (which currently take 18+ months to process) and real-time intel sharing.
    - Solutions - Expedite credible and accurate threat intel sharing through:
        - (1) improvement of government declassification of information and
        - (2) improvement of processes for sharing of information
    - Comments:

- DHS is now offering 1-day read ins on information to governors and secretary of states. May be good for commission and other agencies and groups to reach out for these read-ins.
- There are other opportunities to sit down and get read-in on what adversaries are doing now and what actions we should or should not take.
- There is a lag to get that information. Maybe educate stakeholders on reasons why this information should be shared sooner than later and where to readily find this information.
- EPRI currently allow utilities access to their labs to acquire best practices and knowledge to bring back in house to utilities across the nation.
- Education with cybersecurity habits start forming before high school and university level. With users using internet at very young age, we should look at elementary school and tech students what to look for when receive emails and such.

- *Challenge 4 "Fully understanding adversary behavior: tactics, capabilities, tools, strategies, growing sophistication, identity of the adversaries; including insider threats"*

- *Challenge 5 "Fully understanding stakeholder expectations"*
  - Opportunities - Engaging all customers in addressing security challenges, community buy-in.
  - Solutions - Defining customer role in ensuring security; understanding true customer reliability expectations and cost sensitivity, including among different customer types (e.g. residential, business, CI)
  - Comments:
    - Should there be more ownership pushed to the customer to avoid putting more risks to the grid? Any thoughts or examples?
      - Not sure on what customer could do to affect our grid. But when have DERs connected to the grid and the programs that come along with them could affect the reliability and resiliency of the grid itself.
      - Ameren has worked with ComEd to come up with smart inverter specification we will require customers to install to be able to control DER devices linked to the grid.
    - Have a security appliance that is built into each endpoint that is on the AMI networks. Even if hack one endpoint, cannot use that information to hack other endpoints.
    - Thinking of two stakeholders that may have an impact in this opportunity – (1) telecom and (2) national labs provide recommended specifications stakeholders can use.

- Challenge 6 "Overcoming inadequate cybersecurity workforce"

- Opportunities - Moving to 24/7 cybersecurity workforce
- Solutions - Attracting/retaining talent; Automation, AI, to support and enhance human capital; marketing breadth of opportunities; fully utilizing existing programs such as hackathons
- Education - Multidisciplinary approach required, educational pipeline insufficient bandwidth; university level education, short courses, summer schools
- Potential action items - Communicating an inspirational vision (e.g. how to get people excited about internship at utility v. Apple or NASA)

Agenda Item 3: Discussion "Process"

- *Challenge 1 "Encouraging industry to gravitate toward adoption of a standardized set of approaches to increase operational efficiency"*
  - Opportunities - Trend towards adopting business practices even when not required because they make sense and are effective (e.g. NERC CIP, NIST, C2M2). Maturing risk management programs. DOE cybersecurity risk management process (RMP).
  - Solutions - Formalize processes to certify people in best-practice use when interacting with OT and IT.
  - Comments:
    - A lot of information related to this challenge is covered in EPRI's presentation.

- *Challenge 2 "Effectively measuring vendor capabilities, practices, and competencies when introducing their products into grid operations (including multiple tiers in the supply chain)"*
  - Opportunities - Securing supply chain and ensuring vendors incorporate and integrate security protection capabilities.
  - Solutions - Building resiliency throughout ecosystem; Supply chain security: Cloud, 3rd Party, and Consumer-grade Products.
  - Comments:
    - Measurement of vendors and supply chain?
    - PJM in middle of supply chain effort to build security through all of their controls. Went and identified and analyzed each control (took about 3 years). Will get us started to at least identify a number of risks and new issues where you might want to or not put a lot of attention into. We are documenting control identity and will create a risk management document to go through controls to make sure still effective. Ex. Did vendors agree to safeguards by contract and ramifications if breached.
    - There are some very specific IEEE and IEC standards and requirements that are out there that vendors or utilities can use.
      - *See:*
        - Cyber Security Metrics for the Electric Sector Overview (2017)

        - https://www.epri.com/#/pages/product/000000003002011685/
    - Cyber Security Metrics for the Electric Sector: Volume 3 (2017)
        - https://www.epri.com/#/pages/product/000000003002010426/

- *Challenge 3 "Address need for metrics to quantify effectiveness of interventions"*
    - Opportunities - Adoption of risk assessment and capability maturity models. Third-party assessment and continuous improvement.
    - Solutions - Establish metrics for reliability, resiliency, and cybersecurity
    - Comments:
        - Establishing metrics is critical. Otherwise the ability to manage these systems will not be successful.
        - There are a lot of EPRI reports that you have to pay, but some reports are free for download, including reports on how to calculate the metrics.

- *Challenge 4 "Promoting an integrated return on investment strategy that includes physical and cyber security management (workforce, technology, process)"*
    - Opportunities - Ensuring security planning is incorporated in strategic planning and business processes; Potential valuation of resilience attributes in transmission planning
    - Solutions - Incorporating change management into overall project plans

- *Challenge 5 "Harmonizing framework adoption for: information sharing, incident response management, and contingency planning/analysis criteria"*
    - Opportunities - Promote increased cross-utility information sharing with regard to threat identification and incident response, complimentary to role of ISACs. Define need for information. Recognizing differing needs and goals.
    - Solutions - Increased public private partnerships to facilitate information and best practices sharing. Enhancing operations across RTO seams (processes and tools); Responsive congestion management across RTO seams. Integrating emerging technologies to improve process.
    - Comments:
        - When talking about harmonizing framework – seems like pointing to cybersecurity framework – would be really good recommendation on going forward so that conversation around tech and specifications would be easy to understand and talk about.
- Challenge 6 "Prioritizing effective, regular, and consistent evaluation and testing of core capabilities"
    - Opportunities - Testing and exercising crisis and incident management capabilities across multiple jurisdictions
    - Solutions - Exercise response capabilities through local, regional, and national coordinated exercises (CSIRT, GridEx, etc.)

- Potential action items - Continued development of ESCC Cyber Mutual Assistance program to coordinate between utilities in the event of an attack

Agenda Item 4: Next Steps

The working group discussed next steps and adjourned the meeting.