Responding to High Impact Cyber Security Events (RHISE)

Reducing operational impacts and costs from cyber events

- **Cross Area Tabletop Exercises:** Document how an organization would currently respond to a high impact cyber event to understand the level of impact and opportunities for improvement.
- **Operational Incident Response Playbooks:** Develop Incident Response playbooks for select high impact use cases that can be used to help bridge the response between cyber security and operations.
- **Best Practices for Preventing the Spread of Malware in Operation Technologies (OT):** While responding to attacks that affect OT is important, not losing sight of preventing the impact of these attacks is important. So as part of this effort we will also detail industry best practices to preventing the spread of malware in OT.

Background, Objectives, and New Learnings

With ransomware perpetrators carrying out over 4,000 attacks daily, companies of all shapes and sizes are being significantly affected by this new scourge of malware. The impacts of these attacks are well documented by media, having led to everything from the payment of hefty ransoms, train station closures, to the shutdown of critical pipelines. Critical infrastructure appears to be targeted more than ever before as ransomware groups recognize the pressure these organizations feel to recover from attacks as fast as possible.

While the world is still searching for a final solution to the issue of malware such as ransomware and extortion ware there are significant activities utilities can take to help protect their operational environments from attack.

As important as prevention is, the ability for utilities to efficiently and intelligently respond if they do become the victim of a significant attack is increasingly important. In fact, organizations with a mature incident response plan and defined incident response team saved over $2 million on average when recovering from an incident compared to organizations without these capabilities. EPRI aims to take its decades of experience in helping utilities respond to critical events and protecting them from cyber attacks to help define best practices and novel approaches toward preventing and responding to high impact cyber attacks.

Benefits

With the rapidly changing landscape in the electric industry that is grappling with the introduction of a multitude of technologies, such as renewable power, storage, etc. Protecting these new technologies, along with the existing systems that have provided decades of reliable power, is more important than ever before. The public benefits of this project include providing guidance on the most effective and beneficial way to prevent and recover from high impact cyber events. Utilities will gain a greater understanding into their own current capabilities to respond to these high impact events. Additionally, utilities will gain an understanding into how their current response capabilities compare to their peers in the electric industry. Finally, utilities will have a document to use as a basis for the deployment of preventative measures that the industry agrees are the current best practices.

Project Approach and Summary

The RHISE project is focused on advancing the ability for utilities to protect and recover from high impact cyber events. The approach taken will include:

- Cross Area Semi-Live Tabletop Exercises: Documents how an organization would currently respond to a high impact cyber event to understand the level of impact and opportunities for improvement.

- Operational Incident Response Playbooks: Develops Incident Response playbooks for select high impact use cases that can be used to help bridge the response between cyber security and operations.
- Best Practices for Preventing the Spread of Malware in OT: While responding to attacks that affect OT is important, not losing sight of preventing the impact of these attacks is also critical. This task will detail industry best practices and novel approaches to preventing the spread of malware in OT.

Deliverables

The following deliverables will be available to members of this project:

- Detailed report from individual utility tabletop exercises structured around cross organizational collaboration during cyber events that impact operations (GEN, TX, DX, ICT):
  - Tabletop will be a semi-live exercise involving the multiple incident responders that would be participating in the recovery
  - Anonymized report covering the state of response capabilities from all member utilities, including best practices, and industry opportunities for improvement
- Incident Response Playbooks for Select Use Cases
- Preventing Malware in OT: Guidance and Industry Best Practices
- Role-Based Training:
  - Training modules based around different domains (GEN, TX, DX, ICT)

Price of Project

The price to join this project is $125,000 per utility, and the project requires a minimum of four utilities. The cost to participate can be spread out over the duration of the project. Funding qualifies for tailored collaboration (TC) or self-directed funding (SDF).

Project Status and Schedule

The project will begin upon reaching the minimum number of four funders. Once initiated, the project will run 18 months. Variability in the duration will depend upon the availability of funding utilities for participation in tabletop exercises.

Who Should Join

Transmission, Distribution, and Generation asset owners/operators who want to increase their ability to prevent and respond to high impact cyber events.

Contact Information

For more information, contact the EPRI Customer Assistance Center at 800.313.3774 (askepri@epri.com).

Technical Contact

Ben Sooter, PDU Cyber Security at 865.218.8108 (bsooter@epri.com)

Jason Hollern, Generation Cyber Security at 704.595.2579 (jhollern@epri.com)

Brian Deaver, PDU Distribution Ops at 443.910.2553 (bdeaver@epri.com)

Vikas Singhvi, PDU Grid Ops & Planning at 865.218.8144 (vsinghvi@epri.com)

Technical Advisor Contacts:

Central: Chuck Wentzel at 618.320.0011 (cwentzel@epri.com)

Northeast: Tim Anderson at 704.595.2054 (tanderson@epri.com)

Southeast: Barry Batson at 704.595.2879 (bbatson@epri.com)

West: Brian Dupin at 650.906.2936 (bdupin@epri.com)

EPRI

3420 Hillview Avenue, Palo Alto, California 94304-1338 • USA • 800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com