EPRI

SUCCESS STORY

EPRI'S POWER DELIVERY CYBER SECURITY RISK ASSESSMENTS HELP REDUCE OUTAGES AND IMPROVE SAFETY

Electric generating utilities are seeking to increase their cyber security program maturity beyond regulatory compliance. Their goals include reducing the likelihood and consequence of cyber attacks. A robust operation technology (OT) cyber security program can mitigate cyber risks that may impact grid operations and cause unplanned outages, reputational damages, lost revenue, and/or personnel safety. EPRI's *Power Delivery Cyber Security Tailored Assessment for Utility Transmission and Distribution Operations* (3002022419) project delivers focused assessments to help utilities identify opportunities for operational, tactical, and strategic actions that may mitigate cyber risks. Cyber security assessments serve the public good by offering new insights and recommendations that enhance existing utility cyber security programs and practices and help ensure grid reliability.

EPRI recently completed work with the New York Power Authority (NYPA) to assess its transient cyber asset, patching and vulnerability management, and training programs. The first two assessment topics focused on how NYPA manages security procedures for specific grid operations. The third assessment topic examined NYPA's cyber security training for all resources and for cyber security professionals. These analyses identified strengths and opportunity areas in the program capabilities and documented actionable recommendations bolstered by EPRI research.

OBJECTIVE THIRD PARTY EXPERT PERSPECTIVE

Utilities must objectively understand their cyber security posture and capabilities within their OT environments to develop the most effective cyber security plans that help ensure continued grid reliability and resiliency. Some utilities conduct their own internal assessments based on existing models like the National Institute of Standards and Technology's (NIST) Cybersecurity Framework (CSF) or the Department of Energy's (DOE) Cybersecurity Capability Maturity Model (C2M2) to provide that information. However, they may benefit from an objective outside perspective on specific emerging topics or their internal assessment processes.

EPRI's tailored cyber security assessment methodology for power delivery systems looks closely at specific areas of a utility's cyber security program instead of the entire program. The research team may take the results from previous examinations, such as a NIST CSF or Department of Energy Cybersecurity Capability Maturity Model (C2M2) assessment and focus on select areas of concern or look at aspects of the program that have not been examined.

> *"Third party assessments are powerful tools to assess the security posture of an organization. EPRI's experience and research in the utility sector and operational technology adds insights that generic cyber assessments may miss or overlook. EPRI's specific and actionable recommendations both showed that NYPA's cyber security program is on the right track and highlighted valuable opportunities for improvement."*
>
> – **NEZIR FETAHAJ**
> *Director of Operations Technology*
> New York Power Authority

Each tailored EPRI power delivery cyber security assessment starts with identification of the module(s) that will be applied to the project scope. Additional assessment modules may be added based upon participant requirements. The assessment methodology may request specific data furnished by utilities and may include surveys and other tools to collect that data. These assessment modules cover programmatic and performance areas including:

- Internal assessment and audit process
- Engineering design process
- Patch management and testing
- Transient cyber asset program
- Wireless access
- Remote access
- Tamper indication program
- Cyber security training
- GPS and precision timing

VALUE REALIZED

EPRI's assessment approach produces recommendations for improvements that may include goals, plans, and timelines. EPRI identified recommendations to improve NYPA's cyber security program. These recommendations were specific, rated by priority, and given estimated timeframes for completion. NYPA tailored the recommendations to meet internal security goals and incorporate them into work plans. EPRI also provided a detailed discussion of the program components, regulatory requirements, industry best practices, and relevant EPRI research. NYPA derived added value from EPRI membership by using the organization's research in targeted action plans.

FOR MORE INFORMATION

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

Christine Hertzog	*Principal Project Manager*
Program	Cyber Security for Power Delivery
Phone	650.314.8111
Email	chertzog@epri.com

3002025993 January 2023

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