Cyber Security: From “The Grid Edge” to “The Grid on Edge”

EPRI is assessing how to best address the range of cyber security challenges across the electric power system. Our aim is to inform cohesive, enterprise-level strategies from utilities and others in the electricity sector.

Along with the ranks of cyber criminals and saboteurs, the power system’s threat landscape and attack vectors are expanding and shifting daily. Utilities see this most dramatically at the “grid edge,” with rapid growth in the numbers and kinds of connected sensors, controllable loads, electric vehicles, and distributed generation and energy storage.

Absent effective strategies and well targeted R&D, this ever-shifting threat could put the grid “on edge”—a figure of speech meaning tense or apprehensive. Clearly there is an undercurrent of this everywhere cyber threats are perceived.

Mike Howard, President and Chief Executive Officer, EPRI

At EPRI, we focus both on the information technology (IT) and the grid’s operational technology. For operational technology, we need to address existing systems that predate cyber protection and to mitigate risks associated with the projected long-term life of new devices coming into service.

Many of the grid’s existing operational digital assets are communicating with distributed energy resources already, but R&D must anticipate and address much greater automation and connectivity—including connections among electricity customers, utilities, and third parties in the Cloud. As networks become more complicated at the grid's edge, we must continually address cyber security vulnerabilities and risks at the device, system, and aggregator (third-party) levels.

To enhance cyber security R&D, EPRI will identify where relevant work is happening—whether it be the national laboratories, manufacturers, or universities. Drawing on our deep expertise in cyber security and diverse aspects of the power system, we will transfer key insights and results of this work to the electric power industry, helping companies to apply them in their operational systems.

We are looking also at training. Those who are responsible for deploying and using digital and operational technology in power generation, delivery, and use generally are not cyber security experts. Training that targets this audience and focuses on utilities' unique operations is not readily available, and EPRI is proposing to fill this growing need.

For operational technology as elsewhere in the electricity sector, we characterize the adoption of cyber security metrics as "early stage." We see important opportunity to establish standard metrics to help quantify the effectiveness of a utility's cyber security program, justify investments, and support benchmarking.

Given all of the points above, here are four priorities we are discussing and pursuing:

1. **Security Standardization and Reference Communication Architectures for the Integration of Distributed Energy Resources**

    - Cyber security and risk analysis frameworks to support a complex, multi-party grid that involves large numbers of assets owned by customers and third-parties
    - Develop commonly accepted communication and operational cyber security solutions for customer, utility, or third-party-owned assets/systems
    - Develop practices and solutions for the secure integration and continued operation of utility, customer, and third party-owned devices

2. **Advanced Research in Supply Chain Vulnerabilities**

    - Develop near-term guidance on mitigating vulnerabilities of deployed technologies and service providers
    - Leverage EPRI's Technical Assessment Methodology to develop standardized procurement language and vendor specifications with greater transparency and consistency

3. **Security Metrics and Industry Benchmarking**

    - Common set of metrics for leaders to communicate security status to stakeholders
    - Measure the effectiveness of security controls and operations through performance metrics
    - Industry-level statistics on cyber security performance for benchmarking
    - Reliable historical data for establishing long-term strategic goals

4. **Identify Critical Research and Technologies, Transfer to Industry, and Apply to Operational Systems**

    - Develop a process to vet and disseminate emerging security solutions
    - Expedite technology development through deployment and demonstrations
    - Create advisory structure to prioritize cyber security research

Even as the scale and complexity of cyber threats can sometimes put us "on edge," EPRI believes it is most useful to offer a cyber security R&D portfolio that combines leadership, collaboration, expertise, and focus. We expect continual change and adaptation by the electricity sector and its stakeholders, and we expect that virtually everyone will have a contribution to make at the "cutting edge" of progress.

Mike Howard

President and Chief Executive Officer, EPRI