Written Testimony

Hearing of the House Science, Space and Technology Committee
Subcommittees on Energy and Research & Technology

United States House of Representatives

Ms. Annabelle Lee
Senior Technical Executive – Cyber Security
Electric Power Research Institute

"Examining Vulnerabilities of America's Power Supply"

October 21, 2015

The Electric Power Research Institute (EPRI) conducts research and development relating to the generation, delivery and use of electricity for the benefit of the public. An independent, non-profit organization, EPRI brings together its scientists and engineers as well as experts from academia and industry to help address challenges in electricity, including reliability, efficiency, affordability, health, safety, and the environment. EPRI's members represent approximately 90 percent of the electricity generated and delivered in the U.S., and international participation extends to more than 30 countries.

Background

The nation's power system consists of both legacy and next generation technologies. New grid technologies are introducing millions of novel, intelligent components to the electric grid that communicate in much more advanced ways (e.g., two-way communications and wired and wireless communications) than in the past. These new components will operate in conjunction with legacy equipment that may be several decades old, and provide no cyber security controls. Traditional information technology (IT) devices typically have a life span of three to five years. In contrast, operational technology (OT) devices have a life span of up to 40 years or longer. With the constantly changing IT and threat environments, addressing potential cyber security events is a challenge.

With the increase in the use of digital devices and more advanced communications and IT, the overall attack surface has increased. For example, substations are modernized with new equipment that is digital, rather than analog. These new devices include commercially-available operating systems, protocols, and applications as an alternative to proprietary solutions that are specific to the electric sector. Many of the commercially-available solutions have known vulnerabilities that could be exploited when the solutions are installed in OT system components. Potential impacts from a cyber event include: billing errors, brownouts/blackouts, personal injury or loss of life, operational strain during a disaster recovery situation, or physical damage to power equipment.

Another change is the convergence of IT and OT. Historically IT has included computer systems, applications, communications technology and software to store, retrieve, transmit and process data typically for a business or enterprise. OT has historically focused on physical equipment-oriented technology that is commonly used to operate the energy sector. Currently, multiple groups and operators often independently gather and analyze information from isolated and "stove-piped" systems that have been developed to provide security monitoring for physical, enterprise, and control system environments. As the threat landscape has evolved, there is a greater need to have a coordinated view of all aspects of an organization's security posture (i.e., situational awareness) and events (both

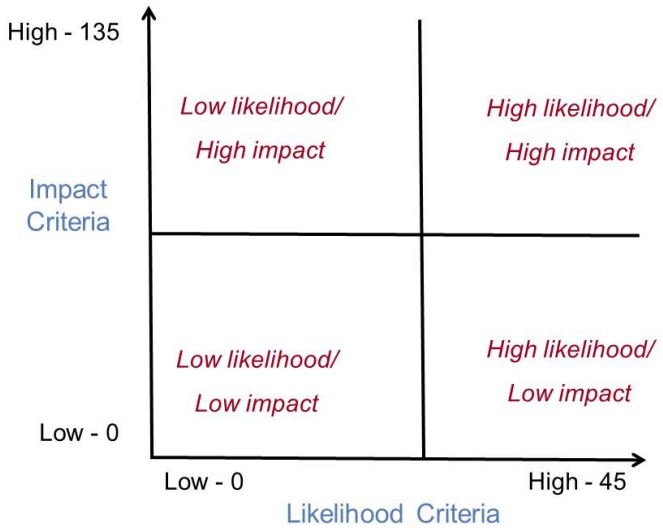
unintentional, such as a component failure; and malicious) that may impact an organization's security posture, and responses to those events.

Risk Management

Cyber security is a priority for critical infrastructures, especially electric utilities. To adequately address cyber security risks, utilities need to understand that there are some basic differences between the security requirements for IT systems and the security requirements for OT systems. In general, the focus for IT systems is confidentiality of information; for example, customer energy usage and privacy information. The focus for OT systems is availability and integrity, to ensure that the reliability of the grid is maintained even in the event of a cyber security incident. OT systems also have performance requirements and any significant delay in sending and/or receiving data and commands could adversely impact the reliability of the grid. Some typical IT security controls such as cryptography and vulnerability scanning that have been implemented in OT systems could cause systems to fail. Because of these differences, utilities need to ensure that implemented security controls do not adversely impact the reliability of the grid.

To adequately address potential threat agents and vulnerabilities, cyber security must be included in all phases of the system development life cycle - from the design phase through implementation, operations and maintenance, and sunset. Cyber security must address deliberate attacks launched by disgruntled employees and nation-states as well as non-malicious cyber security events (e.g., user errors, incorrect documentation, etc.). Currently, the majority of cyber security events are non-malicious. Because organizations, including utilities, do not have unlimited resources, including personnel and funds, cyber security must be prioritized with the other components of enterprise risk. *Risk* is the potential for an unwanted impact resulting from an event. Enterprise risk addresses many types of risk such as investment, budgetary, program management, legal liability, safety, and inventory risk, in addition to cyber security. A cyber security risk management strategy should be a component within an organization's enterprise risk management strategy.

One phase within risk management is risk assessment. Risk assessment is a key planning tool for implementation of an effective cyber security program and involves identifying threats, vulnerabilities, and the potential impact and risk associated with the exploitation of those vulnerabilities. Risk assessments are performed on systems. Once the risk is determined, the organization needs to determine a course of action. This could be accept, avoid, mitigate, share, or transfer the risk. Risk assessments are not one-time activities. Rather, organizations should perform risk assessments on an ongoing basis throughout the system life cycle. The two criteria used in a risk assessment are impact and likelihood. EPRI, in conjunction with utilities, academia, researchers, and vendors developed a risk assessment methodology that is based on a typical IT methodology with impact and likelihood criteria that are specific to the electric sector. This work was performed as part of the National Electric Sector Cybersecurity Organization Resource (NESCOR) project – a DOE funded public-private partnership. Some of the NESCOR impact criteria include: system scale, safety concern, ecological concern, restoration costs, negative impact on generation capacity, and negative impact on the bulk transmission system. Some of the NESCOR likelihood criteria include: skill required, accessibility (physical), accessibility (logical), and attack vector. A score of 0, 1, 3, or 9 is determined for each criterion then a sum is calculated for impact and likelihood. The resulting score can be displayed on a graph, as shown below. The systems that fall in the upper right quadrant, high likelihood/high impact, are the highest priority for the organization as are the mitigation strategies for these systems.



Mitigation Strategies

Utilities, government agencies, academia, research organizations, and vendors are collaborating on many projects to develop tools and techniques to address cyber security threats and vulnerabilities. This collaboration is important to ensure that the unique cyber security requirements of the electric sector are addressed. Summarized below are several applicable cyber security research efforts.

To address current and emerging cyber security threats and vulnerabilities, several utilities are implementing mitigation strategies at the enterprise level. One example is an Integrated Security Operations Center (ISOC) that includes corporate systems, control systems, and physical security. Currently, multiple groups and operators independently gather and analyze information from datacenters, substations, networks, physical security and field equipment. Data is also collected and analyzed from external sources. Correlating this data to find suspicious activity can be extremely challenging and often only occurs long after an incident happens.

An ISOC is designed to collect, integrate, and analyze alarms and logs from these traditionally *siloed* organizations, providing much greater situational awareness to the utility's security team. Additionally, an ISOC allows utilities to transition to an intelligence-driven approach to incident management, which is much more effective for handling advanced threats.

Several requirements documents that specifically address the electric sector provide mitigation strategies. Two of these documents are highlighted below.

- The first document is the National Institute of Standards and Technology Interagency Report (NISTIR) 7628, *Guidelines for Smart Grid Cyber Security*, initially published in 2010. The development was led by NIST with a team of volunteers from the private sector, academia, research organizations, and government. Roughly 150 individuals volunteered their time to author this document. This is the first document that focused on the electric sector and it has been distributed and used worldwide.

- A second document is the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), which allows electric utilities and grid operators to assess their cybersecurity capabilities

and prioritize their actions and investments to improve cybersecurity. The maturity model was developed as part of a White House initiative led by DOE in partnership with the Department of Homeland Security (DHS) and involved close collaboration with industry, other Federal agencies, and other stakeholders. This document is also used worldwide.

DOE has been the designated Sector Specific Agency (SSA) for the energy sector since 2003 and research and development (R&D) has been identified in the Sector Specific Plan (SSP) as a key source of innovation and productivity for the Energy Sector. Since more than 80 percent of the country's energy infrastructure is owned by the private sector, DOE has initiated several collaborative research efforts. Two are highlighted below:

- A key mission of DOE's Office of Electricity Delivery and Energy Reliability (OE) is to enhance the reliability and resilience of the nation's energy infrastructure. Cybersecurity of energy delivery systems is critical for protecting the energy infrastructure and the integral function that it serves in our lives. OE designed the Cybersecurity for Energy Delivery Systems (CEDS) program to assist the energy sector asset owners (electric, oil, and gas) by developing cybersecurity solutions for energy delivery systems through integrated planning and a focused research and development effort. CEDS co-funds projects with industry partners to make advances in cybersecurity capabilities for energy delivery systems.

- DOE published a *Roadmap to Achieve Energy Delivery Systems Cybersecurity* in 2011 that provides a plan to improve the cybersecurity of the energy sector. The strategic framework within presents the vision of industry, vendors, academia, and government stakeholders for energy delivery systems security, supported by goals and time-based milestones to achieve that vision over the next decade. The vision within the roadmap states: *By 2020, resilient energy delivery systems are designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions.* The roadmap is an update to the 2006 *Roadmap to Secure Control Systems in the Energy Sector*. The 2011 roadmap addresses gaps created by the changing energy sector landscape and advancing threat capabilities, and to emphasize a culture of security.

Many utilities and EPRI map their R&D programs to the strategies defined in the *Roadmap* and to the domains specified in the ES-C2M2. These common categories are used by utilities, academia, and research organizations in the public and private sectors as they define and prioritize their research agendas. This is particularly important with the constantly changing threat environment.

Another NESCOR project focused on the development of *failure scenarios* for the electric sector. A *cyber security failure scenario* is a realistic event in which the failure to maintain confidentiality, integrity, and/or availability of sector cyber assets creates a negative impact on the generation, transmission, and/or delivery of power. Each scenario includes a title, short description, relevant vulnerabilities, impact, and potential mitigations. Failure scenarios include malicious and non-malicious cyber security events such as:

- Failures due to compromising equipment functionality,
- Failures due to data integrity attacks,
- Communications failures,

- Human error,
- Interference with the equipment lifecycle, and
- Natural disasters that impact cyber security posture.

Impacts identified in the failure scenarios include loss of power, equipment damage, human casualties, revenue loss, violations of customer privacy, and loss of public confidence.

Included below is a sample failure scenario.

> **AMI.26 Advanced Metering Infrastructure (AMI) Prepaid Billing Cards are Compromised Resulting in Loss of Revenue**
>
> **Description:** The prepaid billing cards for AMI are compromised. Example compromises include tampering with cards to change the credit amount, erasing the logic that decrements the credit amount remaining, or forging cards.
>
> **Relevant Vulnerabilities:**
>
> - *System assumes data inputs and resulting calculations are accurate* on prepaid billing cards inserted into a meter,
> - *System permits unauthorized changes* to AMI billing information on prepaid billing cards.
>
> **Impact:**
>
> - Loss of revenue.
>
> **Potential Mitigations:**
>
> - *Design for security* in the payment system,
> - *Check software file integrity* (digital signatures or keyed hashes) on the prepaid billing card contents,
> - *Authenticate data source* i.e., prepaid billing cards for AMI billing,
> - *Perform security testing* as a part of system acceptance testing.

For utilities that do not have readily available cyber security staff, the failure scenarios may be used as part of the overall risk management process to begin addressing potential cyber security events. For all utilities, the failure scenarios may be used to train new personnel and for refresher training for all staff. Finally, the failure scenarios may be used as input to tabletop exercises. Tabletop exercises are discussion-based sessions where team members meet in an informal, classroom setting to discuss their roles during an emergency and their responses to a particular situation. Many tabletop exercises can be conducted in a few hours.

The NESCOR failure scenarios have been used by researchers and utilities around the world.

Conclusion

With the modernization of the electric grid, new technologies and devices have been deployed to meet our current and future electric sector needs. These new intelligent components communicate in more advanced ways (e.g., two-way communication and wired and wireless communications) than in the past. Cyber security is important because the bi-directional flow of two-way communication and the control capabilities in the modernized grid enable an array of new functionalities and applications. With this new functionality comes new threats, including cyber security threats. To take advantage of the new technology, these threats must be addressed. Identified above are several mitigation strategies that may be used to address current and future cyber security threats and vulnerabilities. Some of these mitigation strategies will be implemented in the new advanced technology.