CYBERSECURITY IN A DISTRIBUTED ENERGY FUTURE

Addressing the Challenges and Protecting the Grid from a Cyberattack

By Advanced Energy Economy Institute

January 18, 2018

AEE INSTITUTE

San Francisco | Washington D.C. | Boston
aee.net | powersuite.aee.net | @aeenet

ABOUT ADVANCED ENERGY ECONOMY INSTITUTE

The Advanced Energy Economy Institute (AEE Institute) is a 501(c)(3) charitable organization whose mission is to raise awareness of the public benefits and opportunities of advanced energy. AEE Institute provides critical data to drive the policy discussion on key issues through commissioned research and reports, data aggregation and analytic tools. AEE Institute also provides a forum where leaders can address energy challenges and opportunities facing the United States. AEE Institute is affiliated with Advanced Energy Economy (AEE), a 501(c)(6) business association, whose purpose is to advance and promote the common business interests of its members and the advanced energy industry as a whole. Visit www.aee.net/aeei for more information.

ABOUT THE 21ST CENTURY ELECTRICITY SYSTEM (21CES) INITIATIVE

Through its 21CES initiative, Advanced Energy Economy is helping to accelerate the transition to a high-performing, customer-focused electricity system that is secure, clean, and affordable. The three primary activities of the initiative are:

Convening forums that bring together utility executives, policymakers, and advanced energy companies to develop a vision for reform that is responsive to the needs of each state and drives towards concrete action.

Participating in key regulatory proceedings in targeted states to provide leadership and input to policymakers and regulators on electric utility industry changes required to support a viable utility business model that allows a high degree of distributed energy resources and empowers customers to become more engaged in their energy use to the benefit of the whole grid.

Facilitating detailed discussions and collaboration among diverse stakeholders who are interested in working together to accelerate reforms that lead to win-win outcomes.

Background

The energy sector is entering a period of significant change, driven by new technologies, evolving customer needs, environmental imperatives, regulatory drivers, and an increasingly complex set of requirements. Amongst a range of stakeholders, there is mutual interest in moving the industry towards a secure, clean, affordable, and prosperous future. The industry has a unique opportunity to modernize infrastructure and facilitate industry evolution and the deployment of advanced technology solutions, creating economic opportunity and an improved customer experience. The grid of the future will have many more interconnected distributed energy resources and devices. Connecting these systems that are out of the control of the Utility with distributed energy resource technologies in a secure manner is pivotal to the transition process.

This paper arises out of an informal Working Group, convened by AEE Institute, that met over a several-month period to address cybersecurity concerns in the electric power sector as a starting point for further discussion with stakeholders, including regulators, policymakers, utilities, advanced energy companies, and others.

The views and opinions expressed in this white paper are those of the AEE Institute and do not necessarily reflect the official policy or positions of the Contributors or their organizations.

Contributors

- Lisa Frantzis, Coley Girouard, Ryan Katofsky, and Benjamin Stafford, Advanced Energy Economy
- Chris Bleuher, Jay Taylor, Joao Souza, and William Romero, Schneider-Electric
- Chris King, Siemens
- Jeff Smith, Direct Energy (Centrica)
- John Berdner, Enphase Energy
- Ken Lotterhos and Doug Morrill, Navigant Consulting
- Richard Jones, BRIDGE Energy Group
- Michael Demeter, Michael Vecchi, Todd Wiedman, Wim Ton, and Steven Chasko, Landis+Gyr
- Wilson Rickerson and Michael Wu, Converge Strategies, LLC
- Richard W. Caperton, Oracle Utilities
- Varun Mehra, EnergyHub
- Jeff Moe, Ingersoll Rand

TABLE OF CONTENTS

SUMMARY

Cybersecurity is a growing issue for the global economy. As new technologies and communications become widespread, cybersecurity[1] is an issue for the critical infrastructure that keeps our energy system going – not just the electricity grid, but the highly interconnected and interdependent natural gas, water, communications, and fuel distribution systems.

This paper focuses specifically on the highly dynamic electricity sector and on the opportunities and challenges created by the widespread introduction of advanced and intelligent energy technologies.

The global market for advanced energy was estimated to be $1.4 trillion in 2016. The U.S. was at the forefront of the market as a result of its support for grid modernization and advanced energy innovation. The U.S. advanced energy market was $200 billion in 2016, of which advanced electricity generation, electricity delivery and management, and building efficiency accounted for 70%.[2]

It is projected that the transition to advanced and intelligent energy technologies will create a wide range of security[3] and economic benefits for the energy system and for consumers.[4] The National Academies, for example, recently found that advanced controls and a more distributed energy generation architecture have the potential to prevent or limit widespread electric grid outages by enhancing power quality and allowing problematic components to be isolated.[5]

At the same time, the modern grid will open new modes of communication and interaction between increasingly diverse and numerous participants and devices. For this reason, modern grid technologies expose existing security vulnerabilities in new ways, as well as introduce new benefits. That said, protections that are practical and currently available or under development will be able to make an increasingly complex, interactive, and distributed electricity system more resilient against cyberattacks.

This whitepaper is intended to inform decision-makers about cybersecurity for advanced energy technologies by highlighting:

- Cybersecurity threats to the economy and to the energy sector;
- Emerging cybersecurity best practices for a distributed, intelligent grid;
- Policy and regulatory frameworks on cybersecurity that are in place at the global level, national level and in some states; and,
- Specific protective measures and protocols that can make a power grid characterized by abundant advanced energy technologies secure against cyberattack.

INTRODUCTION

Cyberattack is a growing threat to the economy and the grid

Cybersecurity threats to the grid have increased in the United States and around the world; not only are the threats becoming more common, a few have demonstrated that they can be successful. The landscape of potential attackers is broad, ranging from individuals to nation-state and terrorist actors. Cybercrimes involving fraud and theft for monetary gain continue to be a prevalent and persistent drag on national economies.[6] There is also an increasing number of attacks designed to disrupt or destroy physical assets.

The energy industry is learning important lessons from the high profile, and high impact, attacks that have affected a large number of users in the United States during the past two years. Several of these recent attacks, for example, have used internet-connected devices (also called "internet of things", or IoT) such as baby monitors, webcams, and other smart home devices. These attacks have been built using some of the same malware code found in the Mirai IoT botnet.[7] The attacker developed code to continuously scan the internet for the IP address of IoT devices with security vulnerabilities such as unchanged factory default passwords. Once a device is found, the bot malware silently installed itself and waited for a command. Once a large number of IoT devices had been compromised, the hacker used his command and control server to send out instructions to flood the target with malformed packets. The attack on the internet service provider Dyn caused widespread disruption for many of the most popular sites in the U.S. Flooding the target with large numbers of malformed packets that were generated by thousands of compromised IoT devices resulted in one of the biggest distributed denial of service (DDos) attacks in history.[8] BrickerBot malware used the same method of locating unsecured IoT devices on the internet. Instead of taking control of those devices to launch wider DDoS attacks, the BrickerBot malware installed a package which caused the device to become permanently disabled (or "bricked"). The author of this malware claims to have disabled more than 2 million devices since the beginning of the year.[9]

The recent WannaCry ransomware[10] attack did not depend on unsecured IoT devices; instead, it exploited a flaw in a protocol used by Windows machines to share files. Once the malware is delivered, the affected machine is locked. The affected machine then uses the same vulnerability to infect and lock any remote machine it can detect, thus triggering an exponential number of attacks. Any machine that was vulnerable during the initial WannaCry attack, whether on a corporate network or using wi-fi in a café, was compromised within minutes. A patch for this vulnerability was available from Microsoft for over a month before these attacks began. Users who had their "automatic update"

settings turned on were unaffected. The botnet and ransomware attacks illustrate how virtually connected technologies - upon which our economy now relies - contain vulnerabilities that can be exploited to rapidly disrupt the "real world" across a broad geographic area.

Alongside the broader trends in cybercrime, an increasing number of attacks designed for espionage and physical damage targeting national governments and critical infrastructure have been noted.[11] These attacks can be broadly divided into those that focus on information technology (IT), with the goal of gathering sensitive data (i.e., industrial and defense secrets, medical records, personal information), and those that focus on Operation Technology (OT), with the goal of manipulating industrial control systems (ICS) (i.e., hardware, switches, relays, motors).

The energy sector around the world has seen attacks that have focused on both IT and OT vulnerabilities. The recent and repeated HAVEX and BlackEnergy malware attacks have exploited OT vulnerabilities of thousands of ICS in the electricity[12] and petrochemical industries. These attacks have mapped devices on the ICS networks and learned detailed information about the processes that the ICS systems govern.[13] In 2016, the first ever malware designed specifically to target electric grids, CRASHOVERIDE, was used in an attack in Ukraine. CRASHOVERIDE triggered an electric power outage over a wide area in the Ukraine by leveraging its ability to speak ICS protocols directly to field devices in order to disable operating technology.[14] In the United States, the federal government's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) has responded to between 50-150 cyber emergency incidents within the U.S. energy sector during 2013-2016.[15]

ADDRESSING THE CYBERSECURITY CHALLENGE

Current Regulations, Standards, and Guidelines

A number of national and state-level regulations, standards, and guidelines address the challenge of cybersecurity to varying degrees. Efforts to understand the risks and provide appropriate security against cyberattack are active in and across various domains, and involve commercial and industry groups, as well as policy and regulatory decision-makers.

NATIONAL-LEVEL RULES AND STANDARDS

The North American Electric Reliability Corporation (NERC) sets standards (Critical Infrastructure Protection, or CIPs) for the bulk

power system. These include standards on cybersecurity. NERC has issued 11 CIP standards subject to enforcement covering a wide range of concerns, including personnel, physical systems, and event recovery plans. These standards provide security measures and controls only for those assets, systems, and information that "directly" impact the operation of the Bulk Electric System (BES). Standards CIP-002 through CIP-011 and CIP-014 cover a wide range of concerns, including the operation of electronic and physical security perimeters around a class of technologies known as BES Cyber Assets, personnel record management, configuration management, substation security, and incident and event recovery. Current NERC standards, which apply to the bulk electric system, are not fully sufficient for protection from cyberattack as the grid evolves toward a more distributed and intelligent grid. A more comprehensive framework, such as the CIS Top 20 Critical Security Controls for Effective Cyber Defense could be augmented with electric grid or ICS-specific frameworks, such as the NIST Framework for Improving Critical Infrastructure Cybersecurity (NIST CSF), an updated version of 7628 Rev 1 and other frameworks to provide the "how to" of the cybersecurity program. The ES-C2M2 is a tool that can be used to measure how well a program is functioning and to develop a roadmap to address shortcomings. Additionally, supply chain requirements, such as NERC's CIP-013 and the Open Trusted Technology Provider Standard (O-TTPS), are becoming relevant for the electric grid industry since the security of the grid is only as good as the products that are procured and deployed. Mandatory standards based testing should be performed by a third party before equipment and assets can be brought to market.

NIST has also looked at cybersecurity issues well beyond the electric grid. In response to presidential Executive Order 13636 and following a collaborative process involving industry, academia and government agencies, NIST issued its Framework for Improving Critical Infrastructure Cybersecurity in February 2014. The goal was to provide a voluntary framework to help organizations manage cybersecurity risk in the nation's critical infrastructure, such as bridges and the electric power grid, but the framework has been widely adopted by many types of organizations across the country and around the world. In January 2017, NIST issued a draft Version 1.1[16] and, as of this writing, has completed review of public comments and is working to update the draft.

Future standards and frameworks must define the specific controls that will be the interface between the Utility Distribution Management System (DMS) and privately-owned dynamic random early detection (DRED) technologies. The increasingly popular OpenADR and ZigBee standards may evolve to be the standard approach to managing the edge of the Demand Response Management System (DRMS) platform. Hardware using the OpenADR standard must be independently tested and certified for physical and cybersecurity integrity; however, recognize that the challenge with any product cybersecurity certification is that it only evidences the device's security at that point in time, as new threats, vulnerabilities, and

methods of attack are being developed every day which may render a previously secure device insecure. What makes this approach incredibly appealing to the utility is that the security encryption for the devices rests with the Utility through the use of public key infrastructure (PKI) technology. In practice, this means that a homeowner or business with an IoT device that wants to interact with the DRMS system has to have a key that is provisioned by the Utility. If there are incidents with equipment, the keys can be unilaterally revoked individually or as a group.[17]

The British Department for Business, Energy, & Industrial Strategy sets standards for secure storage, transmission, access and acceptable use, from a design perspective, as well as SMETs2 (smart metering equipment technical specifications: second version) for equipment and functional design.

BOARDS, INSTITUTES, AND COUNCILS

From an industry perspective, the North American Energy Standards Board (NAESB) has developed cybersecurity standards across segments. While compliance with NAESB standards is voluntary, regulatory bodies, such as the Federal Energy Regulatory Commission (FERC), often mandate adoption of those standards.

To help industry prepare for cybersecurity threats, DOE awarded the Electric Power Research Institute (EPRI) a contract to administer a public-private partnership called the National Electric Sector Cybersecurity Organization Resource. EPRI aids in identifying vulnerabilities, assessing threats, interpreting cybersecurity standards, and validating cybersecurity attributes of technologies.[18]

Industry experts and executives have also joined the Electricity Subsector Coordinating Council (ESCC), to connect the electric power sector and the federal government. Electric company CEOs and trade association leaders engage government entities (White House, law enforcement, national security, and others) through the ESCC to share threat information, coordinate event responses and communications, drive research and development, and to develop cross-sector partnerships. A similar subsector group exists for oil and natural gas.

The cybersecurity strategy for designing and installing distributed energy resource (DER) systems that are resistant to cyberattacks and anomalous power systems events is being continuously discussed in various forums. IEC 62351-12, from the International Electrotechnical Commission, is a technical report that gives recommendations for DER power systems on how to withstand and recover from events such as weather, equipment failures, intermittency of DER systems, as well as malicious cyberattacks.

STATE-LEVEL RULES AND STANDARDS

State-specific efforts on sector cybersecurity are also influencing policies, regulations, and practices. For example, state utility regulators in Connecticut, Michigan, and California are building capacity and facilitating rules and regulations. The Connecticut Utility Regulatory

Authority's Cybersecurity Action Plan, issued in April 2016, "discusses standards and guidelines and the prospect of a Public Utility Company Cybersecurity Oversight Program, wherein the companies will have the opportunity to demonstrate, through annual meetings with government stakeholders, that they are adequately defending against cyber-attacks."[19]

On the state level, the National Association of Regulatory Utility Commissioners (NARUC) published the third edition of the primer *Cybersecurity for State Regulators*, representing over five years of cyber-preparedness expertise within state utility commissions. NARUC also engages regulators in training on cybersecurity, and plans to work with DOE to train in all states this year and next. The intent of the primer is to help regulators become informed, develop a strategy, and foster dialogue with industry stakeholders on cybersecurity.

In November 2016, the Michigan Public Service Commission (MPSC) began formulating rules for annual cybersecurity reporting. According to the MPSC: "The rules shall provide for an annual report that includes an overview of the electric or gas provider's cybersecurity program; a list of the company's cybersecurity departments, staffing numbers and position descriptions, and the names of key contacts; a description of any cybersecurity training and exercises undergone by employees; an explanation of any cybersecurity investment made and the rationale for such investment; a discussion of the tools and methods used to conduct risk and vulnerability assessments; and a summary of cybersecurity incidents that resulted in a loss of service, financial harm, or a breach of sensitive business or customer information."[20]

The California Public Utilities Commission (CPUC) works with the office of the Governor to coordinate responses and information sharing. Further, staff of the CPUC proposed implementing a Staff Cybersecurity Group, including four positions dedicated to assessing utility funding, coordinating with appropriate agencies on threats, and evaluating industry frameworks and practices. Further, the California Energy Systems for the 21st Century (CES-21) Program coordinates public and private research and development, including modeling attacks, testing physical systems, and enabling machine automated response systems.

PROTECTING ADVANCED GRIDS FROM CYBERATTACK

As the electricity system becomes more distributed and interconnected, the distribution grid is becoming more flexible and intelligent, with great benefit to the grid and its customers. DER installed on the grid, such as batteries, and small-scale generators (e.g., solar arrays, fuel cells), are increasingly connected online for the purposes of monitoring and control. To accommodate these new resources, utilities are adopting distributed energy resource management systems (DERMS) as ways to safely and reliably integrate them into their operations. The DERMS and DER often communicate as part of an integrated cyber-physical system.[21] Communication between DERs and the utility may also provide a potential attack vector, however.

Cybersecurity for edge devices is challenging for several reasons. Typically, edge devices are high in number and limited in bandwidth, memory, and storage space. As a result, standard industry solutions for other technology areas such as malware protection, file integrity monitoring, firewalls, and whitelisting, have not been viable for edge devices. Network infrastructure has also had similar limitations.[22]

Specialized applications for edge devices and critical network infrastructure have been developed in the past, but they have not been widely adopted. This has partly been because of the difficulty and cost of implementing these solutions, and partly because the perceived value of security has been low relative to the perceived threat, up until now.

BEST PRACTICES AND STRATEGIES

That said, new and existing best practice technologies, processes, and operational protective strategies can reduce the risks to the distribution grid – some at no or low cost. With appropriate application, the risk of a major service outage resulting from a breach within the distribution grid can be minimized, if not eliminated, by following established best- practices and protocols. The following suggested best practices and strategies are not a comprehensive list, but provide a representative sample of actions that can be taken to reduce risks.

- **Changing default passwords.** Standard protection solutions offered today on workstations and servers need to be extended to distributed energy devices. Device manufacturers should employ a technology that requires changing default passwords when a device is first connected. This requirement could also be integrated into existing standard processes, such as generator interconnection or permitting. A significant share of successful cyber incursions occur through unchanged factory default passwords.

- **Maintenance of passwords.** In addition to changing default passwords, it is important to remove access to existing or old passwords for users who should no longer have access. Often, employees and service providers will save passwords for future access. These passwords can be compromised, depending on how they are stored, and they can also be used by the bearer for unauthorized access. Maintenance of passwords is largely a manual process, but it can be aided by some automated methods such as password timeouts, shared directory functions, and locking out infrequent users.
- **Updating malware and software protection.** All parties must accept that they have a responsibility to ensure software patches and malware protection are kept up-to-date on all devices, regardless of regulatory mandate. Requirements such as these could be integrated into UL 1741 listing requirements.
- **Encrypting messages.** Encryption solutions with minimal resource requirement and high protection should be chosen. When utilizing encryption, the latest NIST standards should be followed. Endpoint devices should not share secret and/or private keys.
- **Firmware protective measures.** At the device level, firmware should be signed by the device manufacturer and it should not be possible for unsigned firmware to be loaded into the device.
- **Isolation.** As more IT/OT integration is seen, as well as new products are developed that require information and connection to critical infrastructure systems, it is becoming more difficult to keep these environments truly isolated from the internet. Best practices include network segmentation with distinct security enclaves and enabling groups of devices to interact via a NIST-recommended method for securely sharing a certificate, such that the DER resource can communicate to other devices on the premise (e.g., when enabled by an application that manages the interaction of the DERs with consumer devices at the premise as well as the utility's load-side meter).
- **External interface protection limitations.** Interfaces should be disabled at the operating system level and not available for use unless specifically activated. Applications or operating systems (OS) that run on the device should have the ability to be securely updated or patched as needed.
- **Penetration testing.** Comprehensive penetration testing should also be done prior to release and periodically thereafter to validate that no vulnerabilities have been introduced.

CONSIDERATIONS FOR GRID OPERATORS

The adoption of DERMS by utilities and other grid operators may create an additional opportunity to further harden the cybersecurity of intelligent grids. DERMS providers with an understanding of cybersecurity can address these concerns as new systems are rolled out, and should include these considerations:

- **Customer data protection.** DERMS platforms should ensure secure storage and maintenance of customer data and device integrity. DERMS platforms should incorporate strict requirements to address issues ranging from secure transfer and storage of customer information to authentication protocols when interacting with devices and utility systems. Only essential information should be collected by DERMS platforms (i.e., name, email, address, time zone, Wi-Fi name (SSID), device IP address). Personally Identifiable Information and device-related information should be stored on a hardened and encrypted server with multiple layers of security control.
- **Hardware vendor engagement.** DERMS providers should work with DER hardware vendors to assure the security and integrity of the DER devices themselves and to promote end-to-end system security, regardless of the communication medium (e.g., Wi-Fi, cellular, ZigBee, and Z-Wave), each of which have different approaches to network security.
- **Third-party cloud security.** Many DERMS rely on cloud-to-cloud-based integrations for connected devices and rely on third-party cloud services, such as Amazon Web Services, for management and control of devices under a utility's purview. Cloud vendors utilized by DERMS platform providers should be fully compliant with applicable security standards and undergo periodic Statement on Standards for Attestation Engagements (SSAE) auditing. Incorporating such communication protocols and end-to-end encryption for server storage and data access prevents the device or the network itself from being exploited by packet sniffing, IP spoofing, and Man-in-the-Middle attacks.
- **Security assessments and monitoring.** DERMS platforms should undergo periodic penetration and security assessments, as recommended by the Department of Energy's Office of Electricity Delivery and Energy Reliability and NIST. Third-party services to monitor performance and alert system administrators of downtime should also be employed.
- **Reliable operations.** DERMS platforms should employ network redundancy methods for data storage, distributed across multiple servers, to ensure 24/7 availability of data. All data changes should be logged into an audit trail, by capturing the user, date and time of the change, and the application that was used (e.g., web or mobile). Databases used must be backed up using a method that was designed for high availability.[23]
- **User security measures.** DERMS platforms must utilize role-based access controls in accessing application functions and data access within the software platform, log all events for reporting purposes, and require multi-factor authentication for all users.
- **Training.** In addition to software and hardware considerations, it is also critical that organizations across the value chain educate their staff on the risks of cyberattack and train them in mitigation strategies.

Summary of Recommendations

To encourage adoption of these best practices, AEE Institute recommends several concepts for consideration by industry and policymakers:

- Development of a short list of mandatory and standardized requirements that are no-cost or low-cost to implement. This could include, for example, drawing on existing industry standards that encourage end-to-end protection of both DER devices and the management systems that control them.
- Creation of guidelines for implementing reliable and secure DER systems, with illustrative use cases.
- Cybersecurity embedded as part of standard security practices that affect manufacturers (e.g., UL Listing or ISASecure[24]) and/or end-use adopters (e.g., factory default password reset requirements).
- Coordination and unification of DER cybersecurity efforts. There are numerous ongoing policy and standards developments that would benefit from closer coordination and support.
- Due consideration for international standards bodies, such as BEIS SMETs2,[25] with a vision for platform integration and interoperability.
- Support for ongoing innovation in the face of emerging threats. New endpoint protection technology needs to be developed for critical infrastructure devices. Critical infrastructure devices will also need the ability to run, store, and safeguard themselves. Device health awareness and non-conformity (network access control) blocking are just two areas that will need to be embedded in critical infrastructure systems.

These recommendations must be balanced against the high cost of cybersecurity attacks. Cybersecurity practices for advanced and intelligent distribution grids should be developed and deployed in a manner that enables, rather than constrains, innovation and advancement in energy technology.

CONCLUSION

Currently, distribution-focused security measures are only loosely regulated. Some may suggest that a "regulatory imperative" would drive stronger security and force greater budgetary commitment. For the foreseeable future, however, and foregoing any unforeseen event, it is unlikely that the blurred boundary between the "compliance" jurisdictions at the federal level and the public utility commissions at state levels will resolve into a single policy for security of our electric grid all the way to the grid edge. Therefore, the security of the distribution system, and especially the grid edge of DER, must come from the industry itself – utilities and their service and solution providers.

Given current circumstances, it seems appropriate to ask what is a reasonable objective for cybersecurity threat management in a distributed energy future?

For systems that have exposure to IoT, utilities and their service providers should operate under a program of security controls and governance measures at all points of the solution lifecycle. From design to ongoing operations of the latest applications, such as DERMS, and the deployments of endpoint sources such as batteries and solar arrays, security should not be an afterthought.

It is also reasonable to expect these capabilities to be able to not only predict, prevent, detect, or respond, but also recover efficiently and effectively from a cybersecurity breach.

This paper is a step toward demonstrating that the outlook on grid edge security should be positive. There are technologies, processes and operational strategies currently available that will reduce exposure to cyberattack. With appropriate application of these protective measures, the risk of a major service outage resulting from a breach at the grid edge can be minimized.

END NOTES

[1] It is important to note that cybersecurity involves not only the connected products, but also the physical perimeter security and access to critical infrastructure, especially for unmanned assets.
[2] Navigant Research, "Advanced Energy Now 2017 Market Report: Global and U.S. Market Revenue 2011-2016 and Key Trends in Advanced Energy Growth" (Washington, DC: Advanced Energy Economy, 2017).
[3] CNA Military Advisory Board, "Advanced Energy and U.S. National Security," June 2017.
[4] Forrest Small, "Why and What to Plan for? Meeting PUC Objectives with the Technology and Functionality of a Modern Grid" (Advanced Energy Economy Institute Midwest Public Utility Commission Staff Forum, Chicago, IL, March 28, 2017); M.J. Bradley and Associates, "Powering into the Future: Renewable Energy & Grid Reliability" (Concord, MA, February 2017).
[5] National Academies of Sciences, Engineering, and Medicine, "Enhancing the Resilience of the Nation's Electricity System" (Washington, DC: The National Academies Press, 2017).
[6] Cybercrime costs quadrupled from 2013 to 2015 to $400 billion and are projected to quadruple again between 2015 and 2019 to reach $2 trillion https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#2636f79f3a91.
[7] https://www.wired.com/2016/12/botnet-broke-internet-isnt-going-away/
[8] https://www.wired.com/2016/10/internet-outage-ddos-dns-dyn
[9] https://internetofbusiness.com/brickerbot-iot-devices-destroyed/
[10] Ransomware is malware that "locks your keyboard or computer to prevent you from accessing your data unless you pay a ransom." *See* https://www.wired.com/2017/05/hacker-lexicon-guide-ransomware-scary-hack-thats-rise/
[11] https://www.csis.org/programs/technology-policy-program/cybersecurity-and-warfare/other-projects-cybersecurity-0.
[12] The electricity industry industrial control systems are known as SCADA, or Supervisory Control and Data Acquisition, and are used to remotely control the operations of the grid.
[13] https://fas.org/sgp/crs/misc/R43989.pdf
[14] https://dragos.com/blog/crashoverride/CrashOverride-01.pdf
[15] https://ics-cert.us-cert.gov/Information-Products
[16] https://csrc.nist.gov/publications/detail/nistir/7628/rev-1/final
[17] http://www.sgip.org/wp-content/uploads/NISTIR-7628-Users-Guide-FINAL-2014-02-27c.pdf
[18] https://www.nist.gov/cyberframework/draft-version-11
[19] *Connecticut Public Utilities Cybersecurity Action Plan*, Connecticut Public Utilities Regulatory Authority, Docket No. 14-05- 12, PURA Cybersecurity Compliance Standards and Oversight Procedures, April 6, 2016.
[20] In the matter on the Commission's own motion, to review issues concerning cybersecurity and the effective protection of utility infrastructure. Case No. U-18203, November 22, 2016.
[21] https://en.wikipedia.org/wiki/Cyber-physical_system
[22] These include limited bandwidth, lack of protocol stack management and protection, and limited logging and monitoring.
[23] HA Systems should be used to run the DRMS application platforms that use backup systems which encrypt the data in transit and at rest. Within DRMS environments IDS/IPS controls should be in place to detect potential threats. Configuration control management systems should also be in place to detect if any unauthorized changes have been made. These systems provide an alarm and an audit trail of capturing the user, date and time of the change, and the application that was used (e.g., web or mobile).
[24] http://www.isasecure.org/en-US/Certification/IEC-62443-EDSA-Certification
[25] British Department for Business, Energy, & Industrial Strategy Smart Metering Equipment Technical Specifications: Second Version