September 17, 2018

Connecticut Critical Infrastructure 2018 Annual Report

Executive Summary

Connecticut's electric, natural gas and major water utilities faced a larger number and greater sophistication of penetration attempts during the past year but met them with adequate defense capabilities. While vulnerable to compromise, the companies have enhanced their cybersecurity assets, personnel and training to prevent future attacks.

In early 2018, the U.S. Department of Homeland Security warned of Russian reconnaissance of U.S. critical infrastructure. In late July, DHS expanded its report to state that Russian military intelligence had conducted a hacking campaign targeting hundreds of critical infrastructure companies including electric power utilities during the past two years. The Head of the DHS Hunt and Incident Response Team stated that "quite a few" of the hit organizations were compromised. None of the Connecticut utilities have identified related activity based on DHS-provided information, nor have they been informed that they were among those penetrated.

This year's review found that Connecticut's utilities are spending more time, devoting more resources, educating their workforces and transforming their cultures more thoroughly to meet the increased level of threats.

The four State of Connecticut officials and all four public utilities participating in the 2018 cybersecurity review concur in this report. It is a consensus document. No language, information, statement or finding is intended to reflect a specific fact or situation pertaining to any particular company.

Main Points

1. Connecticut utilities are subject to a persistent, changing array of increasingly sophisticated and dangerous efforts to penetrate their communications and operating systems. In some cases, more than a million distinct probes are received and deflected in a single day from both nation states and private actors. Attacks take varied forms including both attempted systems compromise and phishing directed at employees.

2. During the past year, both federal authorities and Connecticut's utilities have become more aware of threats posed to the management of critical infrastructure and the distribution of vital services.

    - On March 15, 2018, the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) warned that Russia had been involved in cyber attacks on U.S. infrastructure since at least 2016. Their warning stated that: "DHS and FBI characterize this activity as a multi-stage intrusion campaign by Russian government cyber actors who targeted small commercial facilities' networks where they staged malware, conducted spear phishing, and gained remote access into energy sector networks." DHS and FBI warned that Russian probes were paired with efforts to "override control for those systems."

    - The July 2018 update to that sharing of information stated that there were "hundreds of victims" of the Russian military intelligence attacks, and that the Russians had infiltrated power plan control rooms in utilities across the United States, enabling remote control of parts of the electricity grid. Referring to the Russian actions, on July 23, 2018, Jonathan Homer, chief of the industrial control systems group at DHS's Hunt and Incident Response team stated: "They got to the point that they could turn the switches, but they didn't." There was no stated intelligence indicating that hackers had tried to assume control of plant operations as happened in Ukraine in 2015 and 2016.

    - American intelligence officials have indicated informally that the July 2018 information "had understated the scope of the threat." There has been suggestion that other foreign actors in addition to Russia have probed entry into U.S. utilities.

    - Connecticut utilities recognize that powerful nation-state actors are probing them, but none reported that they were among the group of U.S. utility companies notified by the DHS or FBI that they had been penetrated by Russia or other nation states. While there have been a large number of cyber incidents (attempts to penetrate communications or operations), none reached the level of an actual breach (penetration).

- In late July 2018, Federal Energy Regulatory Commission (FERC) Chairman Kevin McIntyre urged U.S. utilities to divulge more information regarding cybersecurity incidents, noting that present reporting requirements do not portray the risks presented by hackers. McIntyre stated that cyber threats to the bulk power system, and consequently to the delivery of electricity, are "ever changing" and demand "constant vigilance."

- Connecticut utilities also reported both increased volume and changing forms of cyber probes on their operating systems during the past year.

3. In 2016, when Connecticut established its voluntary program of annual cybersecurity reviews, the perspectives of state public utility regulators and utilities differed. The Public Utilities Regulatory Authority (PURA) was concerned by reports of growing cybersecurity threats to critical infrastructure and questioned the adequacy of utilities' defense. Some utilities were unconvinced that annual reviews were necessary, concurred in the existence of cyber threats, but were generally confident of their ability to defend against the threats.

   In 2018 there is a notable convergence of perspectives. Both state officials and utilities recognize that cyber threats are serious and acknowledge the real possibility of compromise. Both understand that no company or organization can assume security. In 2018 the Connecticut review process found both sides on the same page and agreeing that cyber threats are real and potentially damaging and that Connecticut companies are literally attacked all the time. Both share commitment to see that Connecticut's defenses are and will continue to be adequate to prevent breaching of critical infrastructure operations.

4. All four companies take cybersecurity seriously. During the past year, the leadership of all companies increased attention to cybersecurity management and the culture of awareness and cyber hygiene, enhanced spending on cybersecurity programs and increased the number and levels of personnel with cybersecurity expertise.

5. Connecticut utilities understand that they face clear and present danger; there were no signs of complacency or assumption of safety. They know that cybersecurity is earned every day and that companies need to be aggressive in building new defenses, keeping up with changes and new developments and seeking support from trade associations, consultants and vendors and government agencies.

6. The state officials and the utilities agreed that the potential ramifications of loss of utility service to Connecticut are not well understood, and both need to continue to increase their attention to response and recovery planning for a major cybersecurity compromise of critical infrastructure. Recognizing that loss of electricity, natural gas or water, especially on a regional scale, for more than two weeks would present

unprecedented upheaval and possible suffering, appropriate and realistic scenarios need to be developed and rehearsed.

7. The forms and frequency of cyber probes on Connecticut utilities continue to evolve and present new challenges, requiring both investment in new and revised defense systems and ongoing personnel training to ensure leadership and management capable of sustaining adequate defense. Connecticut's utilities during the past year have continued to meet the new threats with adequate defense capabilities and are making reasonable provisions to prevent future attacks.

The Review Process

Avangrid, Eversource Energy, Aquarion Water Company and Connecticut Water Company held review sessions with four State of Connecticut officials during May and June 2018 to review their respective states of cybersecurity, new kinds of probes and defenses and ongoing progress in their efforts to prevent cyber breaches. The Connecticut officials participating in these reviews were:

- Arthur House, Chief Cybersecurity Risk Officer;
- Stephen Capozzi, Public Utilities Engineer, Public Utilities Regulatory Authority or Quat Nguyen, Supervisor of Technical Analysis, Public Utilities Regulatory Authority;
- Brenda Bergeron, Principal Attorney, Division of Emergency Management and Homeland Security in the Department of Emergency Services and Public Protection; and
- David Geick, Director of Information Technology Security Services, Bureau of Enterprise Systems & Technology, Department of Administrative Services.

Each company determined the size and composition of its review session team; the sessions ranged from eight to sixteen people. All included senior-level management executives including in some cases the Chief Executive Officer, and company officials with responsibilities in operations, security, risk management, cybersecurity, information technology, information and intelligence, finance, law, human resources, threat and incident response, regulatory and tariff affairs and government relations and regulatory affairs.

All four companies selected the Cybersecurity Capabilities Maturity Model (C2M2) as the principal standard to evaluate their performance.

The Cybersecurity Capabilities Maturity Model (C2M2)

The C2M2 model is like an extensive take-home exam that enables a company or organization to assess its performance in a range of cybersecurity defense activities. The organization reviews ten "domains," among them risk management; threat and vulnerability management, situational awareness; information sharing and communications; and workforce management. Each domain is assessed as falling into one of three categories:

1. The level of development and completeness of an activity;
2. The extent to which a practice or activity is ingrained in operations; and
3. The extent to which five activities are institutionalized and the level to which they are being managed.

Some companies used third-party vendors to help grade themselves. Utilities generally were more comfortable assigning higher grades to areas under their direct control and indicated desire to pay greater attention to areas they did not directly control.

In some cases, areas needing attention tended to be asset configuration, supervisory control and data acquisition (SCADA) and risks with vendors.

Two points regarding use of the C2M2 model were apparent. One is that some of the companies would like to spread use of C2M2 assessments to their respective supply chains but need to establish a clearer set of instructions and more definite procedures to do that effectively. The second is that however the companies graded themselves, they all professed an effort to be honest and candid. Some of the companies noted that appropriate responses to the challenges discovered were not always feasible or elegant or easy to describe – but the gaps were recognized and addressed.

Threats and Challenges

Connecticut's utilities have a better understanding in 2018 of the extent and sophistication of the threats they face and the reality of individual and nation-state cyber aggression against them. They fully appreciate the potential damage at risk. In light of successful penetrations of U.S. intelligence and military facilities and of major corporations with advanced cyber defenses, public utility executives accept the reality that they, like every agency, organization and company, are vulnerable.

There were new, more powerful viruses and attack vectors unleashed during the past year, such as VPNFilter and NotPetya, capable of infecting critical infrastructure. Their introduction did not radically change the basic truth that in cybersecurity, offense is easier than defense and that the task of ensuring security has become more difficult and demanding.

In tallying the ledger of threats and challenges during the past year, Connecticut's utilities noted the following:

- While the world of cybersecurity consultants and systems remains robust in the United States and for public utilities, the market for cybersecurity professionals (or "cyber warriors") is constrained. Human resources departments face challenges in recruiting, evaluating and retaining cybersecurity subject matter experts. It is difficult to attract technically qualified young people to utilities when such professionals are sought by other companies with higher salaries and by government agencies with more extensive resources.

- Trend analysis is a challenge. Most companies start internally and work out, looking for trends such as determining which vendors may have been hacked and what credentials might be vulnerable.

- The volume of probes is rising, and the list of countries of origin is expanding. A company's attempted penetration contacts may vary from a few thousand to over 10 million per week, coming from every continent.

- An ongoing challenge is the effort to create and improve corporate cybersecurity cultures, the concept that cybersecurity needs to be a team sport, and that the compromise of any individual employee can adversely affect the entire company.

- Phishing and spear phishing (customized phishing efforts tailored to draw in one or a group of employees) is also an ongoing challenge. It is virtually impossible to prevent some success by high-quality spear phishing. Efforts to prevent and to cause immediate reporting of compromise continue.

- The Internet of Things (IOT) proliferates the number of ways companies can be hacked and penetrated and offers more platforms to attack. IOT devices often fall outside of established, traditional vulnerability scanning and security patching procedures for computers and network devices.

- Vendors of materials and services are potential sources of compromise. All companies are dependent on a "supply chain" that may not be as stringent in ensuring cybersecurity safety as the utility.

- The ability to "go manual" to operate a facility, substation or function becomes more challenging each year as the former manual managers are replaced by computer-managed systems. Although utilities run drills to practice return to manual operation, the drills are becoming more of a learning experience and less of a reminder each year.

- All four utilities noted their dependence on cable and broadband companies and the need to work cooperatively with them. The utilities reiterated their request that cable and broadband companies participate in the same annual review process as electricity, natural gas and water.

- The utilities expressed their desire to receive increased assistance and cooperation from federal intelligence agencies. Some utilities noted that after Russian probes of utilities during the past year, some non-Connecticut utilities shared with their Connecticut colleagues their dissatisfaction with the extent of federal intelligence sharing. There are very few utility officers with top secret, special compartmentalized intelligence clearances able to work with the Intelligence Community. The industry as a whole does not enjoy the well-established systems and methods of collaboration with the Intelligence Community that other industries, such as defense contractors, have.

- Utilities would like to have easier access to local secure communication resource sites for classified telephone calls and briefings. Specifically, the very limited number of Sensitive Compartmented Information Facilities (SCIFs) available in Connecticut was identified as a challenge. Access to non-SCIF facilities that support classified communications at the CONFIDENTIAL and SECRET levels would also allow better information flow between federal authorities and utilities.

- Connecticut utilities need to continue to improve their crisis management capabilities. The utilities realize that there is no template or playbook for the broad and unpredictable effects of a cyber attack – among utilities, state governments or federal authorities. Exercises postulating a range of scenarios including breakdown in public order and population migration to seek water and other basic necessities need to be planned and executed. Specific areas of concern are the need to combine physical and cyber drills, to participate more extensively with Connecticut incident response exercises, to improve crisis communications including local secure communications and to include water utilities in statewide emergency exercises.

- Utilities enjoy several trade association and professional ties to share cybersecurity information, but some indicate the need for more direct, structured peer-to-peer information sharing.

Areas of Progress

While the list of threats and challenges is extensive and demands attention, the list of defenses, improvements and areas of progress is also lengthy. The utilities are advancing in several areas. Among them are the following:

- Utility human resource officers are paying greater attention to attraction and retention of cybersecurity professionals. Some are rewriting job descriptions using National Institute of Technology (NIST) guidelines.

- Some utilities experienced management turnover but sustained their structured approaches and followed through on planned improvements, such as formalized cyber risk management guidelines.

- The companies differ in their processes for auditing cybersecurity risk management, but all companies have some kind of internal review process. All report regular conducting of cyber audits.

- Despite millions of probe attempts, there were no known cyber breaches during the past year. Equally important, the utilities recognize the likelihood that there will be breaches in the future and plan for action to counter them.

- Board of Director involvement was sustained at appropriate levels in some companies and increased to greater levels of inquiry and discussion in others. All boards receive structured updates at varying intervals and review threat landscapes, risk management and plans for response and recovery.

- Cybersecurity has been incorporated into internal audit procedures in all of the companies. While there is no uniformity of standards, cyber generally has become part of risk and threat management.

- Employee training programs focused on cyber challenges are more extensive and of higher quality. All companies have some kind of annual mandatory on-line training covering basic cyber hygiene, awareness and defensive habits. In some cases training rises to the top level such as courses from the SANS Institute and customized executive instruction.

- Connecticut utilities are paying increased attention to the cybersecurity dimensions of corporate culture, including training and other activities designed to establish values and reward positive behavior. Activities include periodic phishing drills (some conducted annually and some continuously); inclusion of cyber themes in safety drills; kudos and rewards to employees who identify cyber threats; and posters, emails and other promotions. One company starts every meeting – no matter the purpose of the meeting – with a cybersecurity reminder, observation or advice.

- While the IOT complicates management, the danger of IOT receives serious attention. Among the actions taken are segregation of recognized IOT devices, efforts to limit IOT connections, installation and upgrading of IOT filters and establishment of sub-security systems to accommodate IOT exposures.

- Penetration or “PEN” testing has become a standard part of cybersecurity defense. The four utilities all recognize that an attacker with sufficient resources, skills and time could breach their security, and all hire an outside firm to conduct probes. Some of the

companies allow the PEN testers to break through and then assess how it was done and how defense should be improved. Others do not proceed to breakthrough but receive immediate reports of weaknesses and areas requiring upgrade. Spearphishing and dark web are both normal components of a PEN test. Some utilities noted their preference for innovative third-party attackers rather than those who tend to run predictable tests.

- Supply chain vetting is an ongoing challenge. The utilities recognize that the art of supply chain assessment is evolving, and there is concurrent agreement that increasing external dependencies have increased attention to supply chain security. Following FBI and DHS alerts to issues related to cloud vendors, that area has received more scrutiny. Some utilities are conducting new reviews of all vendors, including those that have been in place for years, using attestation sheets and requiring demonstration of security measures.

- All utilities report that they run drills of reversion to manual control for their facilities and substations at differing test intervals. They recognize the necessity of doing so for security reasons despite their business models having evolved to computer management.

- The utilities actively engage security consultants and services to enhance in-house capabilities. Among the services most helpful are forensic assessments, review and validation or critique of operations and identification of gaps or ways to enhance security.

- Public utilities work with a number of trade associations and other organizations to improve cybersecurity. Among those mentioned as most useful are the Edison Electric Institute (EEI), the Department of Energy under the Section 9 program of providing cybersecurity advice to utilities, and the New England Utility Cybersecurity Integration Center (NEUCIC).

- Utilities are trying to increase their ability to gather and analyze security data and access to relevant intelligence so that they can better identify adversaries and their attack tools. One helpful organization is the Electricity Information Sharing and Analysis Center (E-ISAC). Another is Infragard, a public-private partnership between businesses and the FBI. A third resource is the Department of Emergency Services and Public Protection (DESPP). DESPP includes the state's fusion center (the Connecticut Intelligence Center), the State Police Cyber Crimes Investigation Unit, and the state's Cybersecurity Committee. The latter brings together representatives from state agencies, municipalities, the federal government and private business to exchange cyber-related information.

- Some utilities have hired individuals with TOP SECRET, sensitive compartmented information clearance, thereby enabling the utilities access to relevant intelligence. A

universal concern among the utilities is inadequate access to intelligence that could help them identify and prevent possible breaches. The utilities would also like to be able to leverage relevant security clearances held by employees currently serving in the National Guard or in military reserves.

- Although the Connecticut utilities have not participated in coordinated emergency response and recovery exercises focused exclusively on a cyber attack, they have begun the preparation process, and some participate in Connecticut or federal government drills.