STATE OF CONNECTICUT
PUBLIC UTILITIES REGULATORY AUTHORITY

January 7, 2022

2021 Connecticut Public Utilities Annual Cybersecurity Report

I. Introduction

With the release of the 2016 Connecticut Public Utilities Action Plan,[1] the Public Utilities Regulatory Authority (PURA or Authority) established a collaborative process with Connecticut's regulated electric, natural gas and two large, public service water companies to meet individually with each company to discuss the cybersecurity threats faced by them and to review in detail the cybersecurity program of each. The Action Plan identified the need for the Authority to establish a program to ensure that the public utilities are able to meet ever-growing cybersecurity threats. The purpose of the review meetings and subsequent report, then, is to ensure that the public service companies that own and operate critical infrastructure in the state have designed and run a cybersecurity program that is appropriately robust and able to prepare for and respond to cyber threats. This type of program continues to be necessary to ensure the companies meet their obligations for public safety and reliable service.

2021 is the fifth consecutive year of this review process, culminating in the year-end report. The review team included utility, cybersecurity, and emergency response subject matter experts. The specific make-up of the state team is described in a subsequent section.

As in the past, the review meetings and this report are the result of a collaborative effort. The State of Connecticut officials and the Connecticut public utilities participating in the 2021 public utility cybersecurity review concur in this report. Based on the sensitivity of some the information discussed at the meetings, no specific information associated with a participating utility company has been included in this report.

[1] See, Connecticut-Public-Utilities-Cybersecurity-Action-Plan-April-6-2016.pdf

II. Meeting Framework

The Authority, its state agency partners, and participating utility companies followed the framework established by the Cybersecurity Action Plan. The framework calls for separate annual meetings with the following utility companies: The Connecticut Light and Power Company d/b/a Eversource Energy, Avangrid, Connecticut Water Company and Aquarion Water Company. The meetings took place during August, September, and October of this calendar year.

A number of Connecticut officials participated in each of the reviews, including:

- Marissa Gillett; Chairman, PURA;
- Jeff Brown; Chief Information Security Officer, State of Connecticut;
- Brenda Bergeron; Principal Attorney, Division of Emergency Management and Homeland Security in the Department of Emergency Services and Public Protection;
- Stephen Capozzi; Supervisor of Technical Analysis, PURA; and
- David Palmbach; Intelligence Analyst, Connecticut Intelligence Center (CTIC).

The meetings followed the structure and process set up in PURA's Cybersecurity Action Plan dated April 6, 2016, with the lone exception being that meetings were held virtually. The meeting agenda was drafted by PURA and focused on three main topics:

1. Corporate Culture;
2. Threats; and
3. Cybersecurity Capability Maturity Model (C2M2);

First, participants emphasized and discussed corporate culture to ensure that each company's management, including the executive-level leadership, adopts a serious commitment to cybersecurity policy and practices. Next, specific threats faced by the companies during 2021 were discussed. Finally, each meeting incorporated a C2M2 review, which includes a technical review of specific company security controls. The C2M2 is a self-assessment tool, whereby each company reviews the risks and objectives of its cybersecurity program across various technical and managerial domains. The tool enables companies to prioritize objectives based on their cyber risk profile. The C2M2 details a list of practices that would need to be employed to meet the objectives for each technical domain. According to the tool, the more practices that are implemented by the company, the more mature the company's cybersecurity program is with respect to that domain. It is important to keep in mind that not all domains or objectives require significant action; all action is based on the specific cybersecurity risks as evaluated by the company.

For each meeting, the utilities developed their presentations within the established agenda and addressed the specific questions sent by PURA and its state agency partners ahead of the meeting.

Chief Executive Officers or senior managers led the company review session teams. The professional positions represented included cybersecurity leadership, physical and cyber risk management, operations, finance, human resources, network management and infrastructure services, customer service, threat and incident response management, and law, government relations and regulatory affairs management.

III. Threat Environment

Overview.
While the types of Cyber-attacks have remained fairly consistent with last year the quantity has continued to grow. As attacks such as phishing become more automated and easier to conduct, more unsophisticated malicious cyber actors are entering into the cybercriminal eco system. On the other side of the sophistication scale this year saw a record number of zero-day vulnerabilities exploited in the wild. Vulnerabilities such as ProxyLogon and Proxyshell resulted in a significant number of network intrusions and were exploited by a large variety of actors. The ransomware eco system has also continued to thrive as many new groups targeted entities within the United States this year and showed no signs of slowing down.

Phishing attempts continue to be the largest attack vector and pose a significant risk to all of the state's critical infrastructure entities. Phishing attempts are continually evolving as malicious cyber actors try to evade detection and bypass security measures. One common item that emerged from the meetings was that the lack of multi-factor authentication was the source of many successful hacks of utility vendors and business partners. Therefore, the review team cannot stress enough the importance of instituting multi-factor authentication as a security measure for all users that have access to information systems.

Noteworthy items in the 2021 threat environment are outlined below.

Prominent hacks. There were a number of prominent hacks during the year, including some direct attacks on companies in the energy and utilities industry.

Calendar year 2020 ended with the announcement of the widespread Solar Winds Orion software supply chain compromise which potentially impacted the networks of private and public sector entities, including government agencies and critical infrastructure companies.[2] This was discussed at length in the review meetings and has been discussed extensively in the cybersecurity industry for the past year.

In February, software developed by Accellion for providing file sharing software to public and private organizations, including those in the telecommunications and energy sectors, was exploited resulting in the potential leak of confidential information for entities using the software.[3] Similarly, in July a prominent supply-chain ransomware

[2] See, CISA Issues Emergency Directive to Mitigate the Compromise of Solarwinds Orion Network Management Products | CISA and Supply Chain Compromise | CISA.
[3] See, Exploitation of Accellion File Transfer Appliance | CISA.

attack on Kaseya VSA was announced.[4] A vulnerability in software used to provide IT management service was exploited, potentially affecting companies using the service.

In March, Microsoft identified several zero-day vulnerabilities in their Exchange servers that were being actively exploited by Chinese state actors. (can't paste source) They were able to compromise at least 30,000 devices in the United States alone. They triaged the devices they were able to gain access to and conduct further actions on objective for networks that were of the most value to them.

Additionally, the energy and utility sector saw some direct cyber compromises. In February, malicious cyber actors gained access to the supervisory control and data acquisition (SCADA) system at a water treatment plant in an attempt to manipulate the water treatment process.[5] The hackers exploited an outdated and unsupported computer operating system used for the utility's operations. Personnel prevented any control, and operations were not disrupted. Also, ransomware was deployed against the corporate IT systems of Colonial Pipeline.[6] Only the IT systems were affected in this hack, but operation technology systems were disconnected as a precaution, resulting in disrupted service.

The above compromises reveal a number of things. First, malicious cyber actors have continued to target the IT supply chain and third-party vendors as a means of gaining access to their intended targets network. The associated risk will likely increase as these types of services are relied on more and more by critical infrastructure companies. Second, malicious Cyber Actors have been able to gain access into many networks using legitimate credentials that were likely stolen in previous phishing campaigns or easily guessed based on previous data breaches. Therefore requiring multi-factor authentication – along with other security controls such as secure email gateways, DMARC, enforcing your password policy, updating software regularly, etc. – is a necessary practice to mitigate risk. The following mitigations are proven to reduce the risk of a cyber-attack: (1) requiring multi-factor authentication; (2) performing regular patch management; (3) establishment of accessible and protected system back-ups to include offline copies; (4) restrict access to resources to only those personnel with a true need. (5) collect and retain audit logs for a minimum of 90 days. The more frequent and newsworthy compromises of companies in the energy and utility sector demonstrate the need to develop a mature cybersecurity program.

---

[4] CISA-FBI Guidance for MSPs and their Customers Affected by the Kaseya VSA Supply-Chain Ransomware Attack | CISA

[5] Compromise of U.S. Water Treatment Facility | CISA

[6] DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks | CISA

Phishing. Phishing emails continue to be the main vector for successful cyber-attacks. Successful cybersecurity programs that result in low employee "click-rates" take a multi-pronged approach to educating employees. At a minimum, annual training for employees on general good phishing hygiene should occur. A successful program will conduct phishing campaigns with its employees and target things that employees care about, i.e. vacation time, payroll matters, upcoming holidays, COVID information, etc. Companies have documented an increased employee engagement with the training when they offer modules or programs that treat the training as a game where there may be some reward for successfully identifying phishing emails.

IV. Notable Activities

Public Act 21-119. Public Act 21-119, An Act incentivizing the Adoption of Cybersecurity Standards for Businesses (Act) became effective on October 1, 2021.[7] The Act establishes protections for businesses if one of a number of industry-recognized cybersecurity frameworks is implemented. The Act identifies the following frameworks:

1. Framework for Improving Critical Infrastructure Cybersecurity by the National Institute of Standards and Technology (NIST);
2. NIST publication 800-171;
3. NIST publications 800-53 and 800-53a;
4. Federal Risk and Management Program Security Assessment Framework;
5. Center for Internet Security's "Center for Internet Security Critical Security Controls for Effective Cyber Defense"; and
6. International Organization for Standardization/International Electrotechnical Commission 27000-series security standards.

This addition to state policy necessitates a reevaluation of our review framework. First, the C2M2 framework is not included in the above list. Therefore, if a company were to continue to use the C2M2 to comply with our annual critical infrastructure review process, then it may be implementing redundant frameworks. Past reports found that the C2M2 may be nearing the end its useful life in these reviews, as it has been most helpful for the less mature cybersecurity programs. As cybersecurity programs matured within the utility companies, the benefit provided by the C2M2 review has waned. The key limitation in the C2M2 is that while it identifies a set of practices that should be in place to meet cyber objectives, it does naturally allow for a self-assessment of how well those practices are being implemented. The companies whose cyber programs are advancing began implementing portions of the NIST 800 series framework, which offers much more granularity with security controls than does the C2M2.

Due to the recent implementation of the Act, the companies had not had a chance to decide on a path forward. Accordingly, the review team will follow-up with the companies in early 2022 to consider whether and how any of the frameworks listed in

[7] AN ACT INCENTIVIZING THE ADOPTION OF CYBERSECURITY STANDARDS FOR BUSINESSES.

the Act will be used for the technical review portion of the meetings, rather than the C2M2, in 2022 and beyond.

Opportunities for cybersecurity collaboration in the water wastewater industry.
In October 2021, CISA, along with other federal agencies, issued an advisory that highlighted "ongoing malicious cyber activity" targeting IT and OT systems in the water and wastewater sector.[8] The advisory was careful to note that this industry was not necessarily under threat of greater targeting than other sectors. Nevertheless, there are persistent cybersecurity threats sufficient to warrant a unique advisory from CISA.

Due partly to current events, and partly to its own findings, the review team identified an opportunity to both enhance the cooperation among the water organizations and to draft cybersecurity emergency response protocols specific to the water sector. The Authority itself regulates a handful of water investor-owned utilities and the Department of Public Health regulates many small community water systems. So while there are a large number of water organizations, the critical infrastructure review done annually includes only two of the investor-owned utilities: Aquarion Water Company and Connecticut Water Company. Room exists to engage the larger water community.

The state's Emergency Support Function #12-All Hazards Energy and Utilities Annex (ESF-12) specifies the utility-specific emergency response framework within the larger State Response Framework.[9] ESF-12 is intended to enhance statewide coordination during emergency events to facilitate restoration and maintenance of the state's energy, utility, electric, gas, telecommunications, water, and wastewater public services. ESF-12 includes a Water Task Force that has a mission to plan and prepare the water sector for all hazards emergency incidents. That is a valuable tool that can be used to enhance cooperation among entities in the sector. Therefore, the review team will seek to establish a preparedness working group to develop water sector-specific cybersecurity plans and procedures for dealing with cyber disruptions.

Cultivating cybersecurity expertise in the state. Finding qualified personnel to implement a company's cybersecurity program is a continuing challenge due to the high demand for such qualified workers and the limited pool from which to draw; it is also the most important cybersecurity investment a company can make. The challenge is not limited to initial hiring process, but also in the retention of qualified personnel. Special attention needs to be made to ensure the state has qualified personnel in this area. One such effort currently underway that the review team wants to highlight is the partnership between the State of Connecticut and Eversource. Eversource's Chief Information Security Officer is an adjunct professor at Central Connecticut State University's Cybersecurity Program. This partnership helps provide Eversource with qualified individuals for internships during education and employment after completion. Other companies and public entities ought to connect with Eversource to assist in this project and network with qualified individuals coming out of the state universities.

---

[8] See, Ongoing Cyber Threats to U.S. Water and Wastewater Systems | CISA
[9] https://portal.ct.gov/-/media/DEMHS/_docs/Plans-and-Publications/EHSP0061-SRF-ESF12--EnergyandUtilitiesAnnex.pdf

GridEx VI. Every two years the North American Electric Reliability Corporation's (NERC) Electricity Information Sharing and Analysis Center (E-ISAC) runs a grid security exercise, known as GridEX, a national exercise that seeks to simulate cyber and physical attacks on the nation's electrical grid. NERC's objectives and goals for the 2021 exercise, GridEx VI, included:

1. Activate incident, operating, and crisis management response plans
2. Enhance coordination with government to facilitate restoration
3. Identify interdependence concerns with natural gas and telecommunications sectors
4. Exercise response to a supply chain-based compromise to critical components
5. Identify common mode and cyber operation concerns across interconnections

The State of Connecticut, local governments, and private businesses jointly participated in the exercise. The Division of Emergency Management and Homeland Security led a group of state and local entities in the exercise. The group identified a number of exercise goals. These goals were developed in part based on findings from previous annual cybersecurity critical infrastructure reports:

1. Test and update the state's Cyber Disruption Response Plan.
2. Test communications protocols for the electric distribution companies.
3. Further the public utility annual cybersecurity reviews to address gaps in evaluating emergency response.

The main focus of GridEx VI was to present region-wide disruptions to fuel oil and natural gas supply in New England. The exercise itself presented a number of specific scenarios that saw regional disruptions to the fuel supply, electric grid and communications grid. During the exercise, officials identified a number of lessons-learned and areas of improvement in the current cyber response plans and procedures.

The review group stresses the importance of utilities' participation in cyber disruption exercises. Since many utility emergency response plans and procedures are designed first around extreme weather events, it is necessary to exercise the plans in response to different types of events, including cyber-specific ones. Current procedures may not be directly applicable to cyber disruptions, which have their own particular needs that may be entirely unrelated to weather. Also, cyber exercises help identify areas of interdependence between public and private sector entities that can be disrupted during a large-scale cyber incident. For example, a utility's reliance on IT and communications systems can be severely hampered during a cyber incident, presenting communications challenges with customers and necessitating coordination with telecommunications providers. The disruptions to the fuel supply demonstrated the reliance on fuel oil for electricity generation and heating which reaches all facets of business and personal life. So while GridEx itself is targeted to electrical grid disruptions, the interdependent nature of critical infrastructure sectors must be understood. Exercises like GridEx VI present scenarios that expose vulnerabilities for all energy and utility companies (including

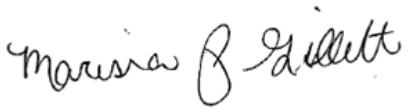
water, telecommunications, and fuel supply). The review team urges all utilities to participate in future GridEx events.

Participation in Connecticut Cybersecurity Committee. Last year's report noted the robust participation by the utility companies in the Connecticut Cybersecurity Committee. The committee is run by the state and comprises state agencies, local governments, federal partners, and private companies. The committee meets monthly and includes a briefing on current threats and cyber trends, information about training and exercise activities, and sharing of information and lessons-learned among members. This active participation has led to two very important outcomes. First, companies receive timely cybersecurity threat and best-practice information from other members, which helps companies cultivate their own cybersecurity expertise and may even fill the gap where personnel can be hard to come by. Second, the committee brings people together such as state and local officials who provide assistance during any potential cyber incidents. The review group continues to emphasize the importance of utility company participation in the committee.

V. Conclusion

The array and sophistication of cybersecurity threats facing Connecticut's public utilities seems to grow every year. In the face of these challenges, the utilities have demonstrated their awareness of the increasing cyber threats and they continue to develop their cybersecurity programs as a result. The review team offers its appreciation for its participants, including state agency partners and the utility companies and their management staff. The level of commitment to cybersecurity is evidenced across all levels of decision-makers and employees. Nevertheless, continued improvement is necessary to face challenges that only continue to grow as the threat landscape evolves.

Sincerely,



Marissa P. Gillett
Chairman