STATE OF CONNECTICUT
PUBLIC UTILITIES REGULATORY AUTHORITY

March 31, 2023

2022 Connecticut Public Utility Annual Cybersecurity Report

I. Introduction

Cybersecurity threats facing Connecticut's public utilities are ever present and continue to grow in number and sophistication. To address this growing challenge in the utility industry, the Public Utilities Regulatory Authority (Authority or PURA) initiated the annual cybersecurity review process following the 2014 release of the strategic plan, Cybersecurity and Connecticut's Public Utilities, and the Cybersecurity Action Plan (Action Plan) in 2016.[1] A key focus and justification for the development of the Action Plan was the December 2015 cyberattack on Ukrainian power systems that resulted in blackouts. Action Plan, pp. 4-6. With the invasion of Ukraine by Russia in February 2022, and as discussed below, this year's annual review process saw a renewed focus on Ukraine.

In the Action Plan, the Authority established a collaborative process with state agency partners and with Connecticut's electric, natural gas, and two large water public service 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 purpose of the review meetings 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 properly 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. In 2022, the review process included a review with Frontier Communications Corporation (Frontier). The participation by Frontier has enabled the cybersecurity review process to expand into the telecommunications sector.

Calendar year 2022 marks the sixth consecutive year of this review process, culminating in this 2022 report. The review team took advantage of interagency relationships and included utility, cybersecurity, and emergency response subject matter experts. The composition of the state team is described in a subsequent section.

The growth of the number and types of attacks continues, and phishing attempts remain the most prominent source of cyber attacks. Ransomware resulting from

[1] Both available at: Cybersecurity and Connecticut Public Utility Companies

successful phishing attempts and other cyber attacks is growing in number and sophistication. Cyber vulnerabilities in supply chain and third-party vendors remain a persistent threat. The past year saw unique cyber attacks against Ukraine by Russia preceding and coincident with the invasion, as discussed below.

II. Meeting Framework

The Authority and its state agency partners and utility companies followed the framework that was established by the 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, Aquarion Water Company, and Frontier (collectively, Utilities). The meetings took place during November and December 2022.

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

- John W. Betkoski III; Vice-Chairman, PURA;
- Jeff Brown; Chief Information Security Officer, State of Connecticut;
- Brenda Bergeron; Deputy Commissioner, Division of Emergency Management and Homeland Security (DEMHS) in the Department of Emergency Services and Public Protection;
- William Turner; Emergency Management Director, DEMHS; and
- Stephen Capozzi; Supervisor of Technical Analysis, PURA.

The meetings followed the structure and process set up in the Action Plan, except meetings were held virtually. Specifically, the meetings remained structured around an agenda drafted by PURA, which focused on three main topics:

1. Corporate Culture;
2. Current Threats and Vulnerabilities; and
3. Cybersecurity Framework Security Practices and Controls.

The emphasis on corporate culture is included first to ensure that each company's management, including the executive-level leadership, has a serious commitment to cybersecurity policy and practices. Next, specific threats faced by the companies during 2022 were discussed. Each meeting incorporated a review of a company's cybersecurity program management by cyber domain or focus area. The cyber domains include:

1. Asset, Change, and Configuration Management;
2. Threat and Vulnerability Management;
3. Risk Management;
4. Identity and Access Management;
5. Situational Awareness;
6. Event/Incident Response;
7. Third-Party Risk Management;

8. Workforce Management;
9. Cyber Architecture; and
10. Cyber Program Management.

The review for each domain includes a technical review of company objectives, as well as specific practices and security controls to achieve those objectives. Not all domains or objectives require significant action since they are evaluated based on the cybersecurity risks as evaluated by the company.

With regard to running the meetings, the utilities developed their own presentations within the established agenda. PURA and its state agency partners send specific questions to the utilities ahead of the meeting to lead the review.

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

As noted in the introduction, the threat environment changed significantly in 2022 following the Russian invasion of Ukraine. The actions taken against Ukraine by Russia should be considered a microcosm of what a modern-day war looks like. The invasion in February was preceded by various cyber activity against Ukrainian critical infrastructure. The cyber activity continued as Russia began the invasion. Industries including electric, natural gas, telecommunications, and healthcare were all targeted to weaken the Ukrainian economy and the morale of its people. For example, in January 2022, a campaign to deface multiple Ukrainian government websites took place pre-invasion. The hackers posted messages to the citizens of Ukraine to, “Be afraid and expect the worst” and “All your personal data has been sent to a public network.”[2] On February 24, 2022, as Russian forces assaulted Ukrainian cities, there was an attack on Viasat, a satellite communications service provider that disrupted communications services of Ukraine’s military and civilian population.[3]

In advance of the invasion, the U.S. government and the electric and natural gas industries shared significant information to ensure preparedness of potential retaliation for U.S. support of Ukraine. The Department of Homeland Security’s Cybersecurity & Infrastructure Security Agency (CISA) developed the “Shields Up”[4] program to provide critical infrastructure industries recommendations for escalating their cyber posture and

[2] See https://www.csoonline.com/article/3647072/a-timeline-of-russian-linked-cyberattacks-on-ukraine.html
[3] See https://www.cpomagazine.com/cyber-security/ukraine-satellite-internet-service-hit-by-cyber-attack-intelligence-agencies-investigating/#:~:text=A%20%EE%80%80cyber%EE%80%81%20%EE%80%80attack%EE%80%81%20that%20disrupted%20international%20satellite%20internet,The%20service%20interruption%20began%20on%20the%20morning%20
[4] Available at: Shields Up | CISA

security program. While the Utilities stated they were already working at the "Shields Up" level of readiness, they did increase their posture by: (1) implementing new restrictions for certain types of remote access; (2) reviewing and updating cyber response plans; (3) communicating across their organizations the need to be vigilant; and (4) increasing sensitivity for reporting unusual activity to internal cybersecurity teams.

During the year, the Utilities stated that cyber activity at times was lower than traditional volumes. They generally attributed this to Russian-supported cyber actors and organizations focusing efforts on Ukraine.

Despite experiencing lower than normal cyber activity at times, the Utilities continued to experience phishing attempts and an increase in vulnerability scanning. The Utilities believe that these attacks were more easily negated because of the elevated security posture taken in advance of, and in response to, the invasion of Ukraine. However, in 2022, non-utility organizations experienced significant data and ransomware breaches. Florida International University and North Carolina Agricultural and Technical State University separately experienced ransomware attacks, which included the exfiltration of over 1.2 terabytes of data including personal information.[5] The managed service provider Rackspace Technology suffered a ransomware attack causing significant outages to it hosting services business and the loss of data for customers.[6]

IV. Workforce Development

The cybersecurity industry continues to face challenges filling open cybersecurity positions with qualified professionals. The Utilities are not exempt from this challenge. In the Utilities' experience, many cybersecurity professionals are seeking positions with remote work. The Utilities have put in place methods to develop new staff, such as partnering with local universities to bring aboard entry-level staff.

Specifically, the Utilities adopted some or all of the following IT-specific recruitment practices to secure qualified candidates from a limited resource pool:

- Developing Hybrid/Remote Work Policies;
- Staffing career fairs with IT specialists in hard-to-fill career positions;
- Utilizing LinkedIn networks to promote positions;
- Working with external talent recruiting firms to find specific technical specialties;
- Offering more internship programs with a focus on rotational responsibilities for learning multiple disciplines; and
- Incorporating development tracks for growth and career development opportunities for current employees.

[5] See https://securityintelligence.com/articles/13-costliest-cyberattacks-2022/

[6] See Rackspace identifies hacking group responsible for early December ransomware attack | TPR

V. Supply Chain/Vendor Risk Management

The Utilities increased their emphasis on the oversight and governance of supply chain and vendor risk management. The Utilities have enacted more rigorous policies and practices to evaluate vendors that host utility data. These policies and practices are intended to ensure that the vendors have sufficient cyber practices in place to protect customer data and sensitive utility data.

The Utilities are expanding the reviews of third-party suppliers to include reviews of the vendors' software development and manufacturing practices. The process and ability of suppliers to meet the new expectations will mature over time. These changes are being put in place in response to recent data hosting and data analysis provider compromises, of which the Solar Winds Orion software compromise is the most widely known example.[7]

In 2022, there were additional notable attacks against managed service providers. In January 2022, Okta, an authentication service provider was hacked through a third-party sub processor, resulting in the compromise of 375 Okta customers. The Utilities stated this attack did not impact their operations or data.[8] The Royal Ransomware hacking group took responsibility for an attack against Intrado, a telecommunications service provider. While the Utilities stated there were no impacts to customers, Intrado provides call center services to 82% of Fortune 500 companies and various 911 services.[9] The Utilities also referenced an attack on engineering services provider and federal government contractor Sargent & Lundy as an example that hackers are targeting the energy grid. Sargent & Lundy helped design over 900 power stations across the country. While not directly impacted, the energy sector remains an area of focus for malicious cyber actors.

Utilities can partner with entities interacting with its IT and physical distribution systems to support its operation to share relevant cybersecurity threat information. As mentioned above, the DHS "Shields Up" strategy is one resource that should be used by all organizations who are working on improving their cyber security posture.

[7] The 2021 Connecticut Public Utilities Annual Cybersecurity Report discussed the Solar Winds Orion hack. The 2021 report is available at: https://portal.ct.gov/-/media/PURA/2021-Connecticut-Public-Utility-Annual-Cybersecurity-Report.pdf

[8] See https://www.immuniweb.com/blog/5-biggest-supply-chain-attacks-in-2022-so-far.html

[9] See https://www.bleepingcomputer.com/news/security/royal-ransomware-claims-attack-on-intrado-telecom-provider/#:~:text=The%20Royal%20Ransomware%20gang%20claimed%20responsibility%20for%20a,and%20the%20initial%20ransom%20demand%20was%20%2460%20million.

VI. Conclusion

Despite the cybersecurity incidents related to the invasion of Ukraine, the threat landscape in 2022 was in many ways not new and, in fact, highlights the impetus for the annual cybersecurity review process in the first place, which were, among other events, the cyberattacks on Ukraine's energy industry in 2015. Moreover, the challenges discussed this year echoed those from prior years. The review team offers its appreciation to the program participants, including both the state agency partners and the Utilities. The level of commitment to cybersecurity is evidenced across all levels of decision-makers and employees. Nevertheless, continued improvement, particularly in the area of cross-sector coordination, is necessary to face challenges that only continue to grow.

Sincerely,

Marissa P Gillett

Marissa P. Gillett
Chairman