October 12, 2017

Connecticut Critical Infrastructure 2017 Annual Review Report

Executive Summary

Connecticut's first annual cybersecurity reviews with the state's electric, natural gas and water utilities achieved its objectives of cooperative, candid, productive and insightful sharing of pertinent information regarding the state of Connecticut's critical infrastructure cybersecurity defense .

The consensus assessment of both state and utility officials is that Connecticut utilities are taking cyber threats seriously, have improved defense capabilities during the past year in personnel/employee awareness and skills, focused programs and targeted capital investment. All four companies are aware of the need to prepare for the possibility of recovery from a cyber attack and to cooperate with state authorities in prevention planning and rehearsal training exercises.

The four State of Connecticut officials and all four public utilities participating in these annual reviews concur in the wording of this report. It is a consensus document. No language, statement or finding is meant to reflect a fact or situation in any particular company.

Framework for Annual Reviews

By mutual agreement, Eversource Energy, Avangrid, Connecticut Water Company and Aquarion Water Company held annual review sessions with four State of Connecticut officials between January and April 2017 to review their respective states of cybersecurity and ongoing progress.

Four Connecticut officials participated in each of the reviews:

- Arthur House, Chief Cybersecurity Risk Officer and former Chairman of the Public Utilities Regulatory Authority;
- Stephen Capozzi, Public Utilities Engineer, 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
- Brett Paradis, Intelligence Analyst, Connecticut Intelligence Center (CTIC).

As agreed, each company brought to the review sessions whomever they chose. Some meetings had six or seven company employees and representatives, and others more. Company teams included senior-level executive, professional cybersecurity officers with direct operational responsibility, and in some cases retained specialists.

All four companies chose to conduct the reviews using the Cybersecurity Capabilities Maturity Model (C2M2).

A starting point for the annual reviews was acknowledgement that Connecticut utilities face ongoing, changing and serious cybersecurity probes and need to maintain constant vigilance with skilled personnel and up-to-date defense systems. Those seeking to penetrate critical infrastructure systems regularly deploy new means and methods to seek access and overcome existing defenses. Ensuring cybersecurity is an ongoing process of vigilance, attention and modern counter-measures to evolving attacks. Effective defense is a process, not a condition or state. In that setting, all four companies have deployed an array of internal company defenses, retained external specialists, trade association insights and assets and use other means to detect and thwart efforts to penetrate and compromise cybersecurity defenses.

The four participating companies have healthy corporate cultures addressing cybersecurity hygiene. All have currently adequate operational defense systems and all are investing in ways to strengthen cybersecurity going forward.

The Connecticut officials concurred that there have been marked, positive improvements in all four companies' cybersecurity cultures since completion of the Critical Infrastructure Cybersecurity Strategy in 2014 and the 2016 PURA Action Plan.

The C2M2 Model

Use of the C2M2 evaluations was productive and conducive to constructive discussion. The model calls for self assessment, and the utilities were often tough and demanding in grading their own performance. The model provided benefits beyond assessment. The companies used the C2M2 model to evaluate risk for various cyber domains, to prioritize current needs and to develop both near-term and long-term plans. As expected, some companies had more mature starting points than others. The model is designed to accommodate company differences and target programs to specific company risks.

Use of the model was often time consuming but beneficial in focusing and simplifying discussions. The model proved flexible enough for effective use for both the large and medium-sized companies. The result was evidence of structured approaches to cybersecurity risk management that satisfactorily meet all the requirements outlined in the 2016 PURA Action Plan.

Challenges and Areas of Progress

Since PURA opened dialogue with Connecticut's utilities through the 2014 Critical Infrastructure Cybersecurity Strategy and throughout development of PURA's 2016 Critical Infrastructure Action Plan, the public utility companies have revised their cyber programs. Fresh approaches generally reflected honest assessments of existing capabilities and vulnerabilities, resulting in more rigorous and structured defense postures. While there have been some increased capital costs and operational expenses, both have been limited. The notable changes, in some cases profound, are more the product of a serious, fresh look at cybersecurity than increased expenditures.

All four companies demonstrated clear evidence of strong executive support for cybersecurity programs, including CEO involvement and of board of director engagement.

Each company made efforts to strengthen cybersecurity practices and create cultures of cyber awareness and vigilance, including cyber threat awareness briefings, the use of posters, flyers, email messages, "red team" phishing campaigns and cybersecurity training, some with annual training programs and some more frequent. Staff education at one company included required reference to a cybersecurity point at the start of every meeting regardless of the subject of the meeting and frequent testing including "PHISH" drills and penetration warnings.

For all companies, two main areas require ongoing vigilance and continued improvement to counter constantly evolving threat environments. In both, change is frequent and quality control is requires dedicated, focused attention.

The first is keeping up with the ways and means of penetrating a company's security perimeter through new spear phishing methodologies forms of malware and techniques of insinuating damaging intrusions into systems. Trade associations and specialized vendors who track threat scenarios and provide revised defenses are critical to sustained security.

The second is managing third-party services. The U.S. experiences of companies other than utilities in suffering damaging breaches through third-party vendors are reminders of the need to establish and maintain effective control of vendors, the supply chain and everything that comes from outside of the company**.** Connecticut utilities are aware of this threat and recognize that contractors and suppliers who integrate external systems into a company's operating environment can cause security gaps and present a host of vulnerabilities. This

second challenge, like the first, is an ongoing matter of inspection, challenge, verification and review. Our meetings concurred on the need to establish standardized cybersecurity protocols for supply chain vendors.

The rapid expansion of "The Internet of Things" (IoT) connected to electricity distribution increases the array of penetration points to the distribution system and thereby enhances the possibility and danger of a cyber attack. The public utilities do not control installation and maintenance of such devices, which individual consumers and broadband/cable companies put in place. Effective cybersecurity requires attention to the dangerous proliferation of IoT devices. The utilities pledged to work with the broadband and cable companies should the latter agree to address this problem.

Both utilities and state officials noted that participation by Connecticut's cable and broadband/cable companies would enhance value of these annual reviews. Their participation in preparation and defense is key to Connecticut having effective defense and recovery systems. The utilities and the state officials agreed to communicate their request to the cable and broadband companies that good corporate citizenship requires their participation in and contribution to this civic effort.

Although PURA does not have oversight of the municipal utilities and cooperatives in Connecticut, nor the regional and municipal water companies, all are part of Connecticut's public utility cybersecurity system. In the future, we should consider how to include them in this effort to strengthen cybersecurity defense.

Emergency Management and Intelligence

A positive benefit of including a DEMHS officer and a representative of CTIC in the reviews was increased utility understanding of local and state resources, especially intelligence, law enforcement and emergency management, to support cybersecurity. Participants agreed on the value of expanded contacts and on the prospect of benefit from cooperation in defense and recovery exercises. Existing forums and vehicles for improved communication include:

- The State Cybersecurity Working Group, a subcommittee of the DEMHS Advisory Council;
- The Connecticut Intelligence Center;
- The public/private, FBI-supported group Infragard;
- The DEMHS Regional Emergency Planning Teams in each of the five DEMHS regions; and
- The state and regional Emergency Support Function Working Groups supported by DEMHS, particularly ESF 7 (Resource Support/Private Sector) and ESF 12 (Energy and Utilities).

Connecticut needs to establish an agreed process regarding when and how the utilities will share news of a cyber intrusion with the CTIC, both to facilitate trend identification and to enable more prompt and extensive sharing of warnings with other parties facing similar threats. State authorities also need to know of possible threats to public safety and the need for public resources to restore security. As the volume and complexity of cyber threats increases and more federal, state and local law enforcement and intelligence agencies become active in the field, the greater the need for agreed roles and processes and clearly understood reporting pathways. One recommendation is to have the CTIC and the state ESF 12 Working Group convene a meeting with utilities to explore a coordinated approach to information sharing.

Recovery

There was consensus that emergencies potentially involving cyber attacks on critical infrastructure would present scenarios and demands Connecticut has not experienced. There is a lot of work to do to ensure that state and local government agencies and the private sector plan, collaborate and seek to understand the new challenges and required preparation activities. The strain on civil order, the need for unprecedented forms and messages in communications and the demands for collaborative work will require planning and cooperation beyond existing norms.

Participants agreed that while addition of distributed generation to the electric distribution system might have the net effect of greater reliability in case of large-scale outages, the addition also brought vulnerabilities. As more distributed generation and IoT devices connect to the grid, the grid becomes more open to intrusion. Operation of many distributed generation and IoT devices is outside of public utilities' control. If the adoption rates of these technologies continues to grow, it is possible to imagine a much larger problem of new intrusion avenues and grid vulnerabilities. New technologies adopted for "smart" use can bring added security costs. It is not clear who will be responsible for security and protection of the new generators and devices. Nevertheless, it is clear that this area requires public policy attention.

A specific recovery point agreed upon was the need to exercise manual operations. Should a cyber attack disable computer control of vital utility functions, manual management is the other option. It must remain a practiced, exercised option.

The number of cybersecurity exercises offered both in the New England region and nationally is increasing, and often their focus and audiences overlap. Both public utilities and state officials need to set priorities and participate effectively in a few such exercises, taking advantage of exercising together when possible.

Specific Actions to Strengthen Deterrence and Recovery

The following actions support conclusion that Connecticut's utilities are actively working to strengthen deterrence and to prepare for post-incident recovery:

- All utilities reported or demonstrated top executive-level and board of director support and involvement to improve cybersecurity resilience; increased budget allocations for cybersecurity work; and retention of specialist cybersecurity expertise to supplement company defense efforts.

- All utilities either established or planned cybersecurity threat-related working groups and participated in cybersecurity exercises to test incident response, business continuity and disaster-recovery plans.

- All utilities have to some extent sought and created both formal and informal information-sharing groups with peer companies to exchange information regarding industry-specific threats, maintain situational awareness and compile best practices.

- Several utilities manage recurring reviews of their plans and systemically re-evaluate areas of concern through vulnerability scanning, "red-team phishing" and penetration testing using internal, external and third-party resources.

- Intelligence and information sharing is an area of increasing focus. The utilities are becoming aware of the federal, state and local resources available to them and either have or are establishing working contacts with these resources and the Information Sharing and Analysis Centers (ISACs). The utilities are at varying stages of active engagement with these resources, but all are learning about available resources and are establishing working ties.

- There is room for growth and improvement in the relationships between utilities and the nascent effort to create a center of law enforcement and investigation at the state level. A common theme was greater propensity to call state and local law enforcement in the event of a physical incident and less likelihood to report cyber-related information. As Connecticut develops its intelligence and investigation capabilities, a central repository could alleviate duplicated reporting burdens.

- Security of equipment supply chain is a shared concern. The utilities all recognize the possibility of supply chain tampering and the possible presence of malicious software and hardware. The utilities are paying increased attention to supply chain security and are looking for ways to ensure the security and reliability of procured equipment.

Looking Forward

The Connecticut state reviewers were pleased that the utilities prepared carefully for these reviews and took seriously the challenge of making this experiment in voluntary collaboration an initial success. The utilities and the reviewers agreed that top-level attention to cybersecurity, dedicated efforts to create a corporate culture or awareness and responsibility, targeted investments and constructive work with other companies, trade associations and supporting partners are all important future priorities. All these activities need to continue. At the same time, as the threats facing cybersecurity continue to evolve, so, too, must creative and energetic efforts to stay ahead of the threats.

Regarding response and recovery, everyone agreed that while it is difficult to foresee and prepare for harmful activity yet experienced, serious efforts to anticipate and plan are essential. The utilities all offered to participate in state emergency activities designed to manage and alleviate the consequences of a cyber incident.