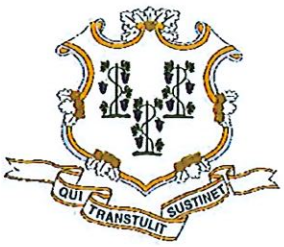

Chief Cybersecurity Risk Officer
55 Farmington Avenue
Hartford, Connecticut 06105
October 10, 2019

Honorable Ned Lamont, Governor, State of Connecticut
Co-Chairs, Vice Chairs and Ranking Members, Committee on Energy and Technology
Acting Connecticut Consumer Counsel Richard E. Sobolewski

Honorable Connecticut Officials:

Four representatives of the State of Connecticut and four Connecticut public utilities have completed the third annual cybersecurity review of Connecticut's electricity, natural gas and water public utilities. This letter conveys their report.

Our review followed the agreed process established in 2016: that the proceedings and information shared are to remain confidential to protect each company's cybersecurity defenses, and that any information made public will be done by explicit consent of each company. The State of Connecticut participants and the four participating utilities approved this report. The State of Connecticut team was:

- Arthur House, Chief Cybersecurity Risk Officer representing the Public Utilities Regulatory Authority (PURA);
- Stephen Capozzi, PURA Public Utilities Engineer, representing the Public Utilities Regulatory Authority (PURA);
- David Geick, Director of Information Technology Security Services, Bureau of Enterprise Systems & Technology, Department of Administrative Services; and
- David Palmbach, Intelligence Analyst, Connecticut Intelligence Center

The four participating utilities were:

- Aquarion;
- Avangrid;
- Connecticut Water; and
- Eversource

The following are some of the key points in the 2019 Annual Review Report:

- Connecticut's critical infrastructure companies took seriously the increased threat levels they faced during the past year and appear to have thwarted the threats they identified. Utilities improved their cybersecurity defenses, invested more in resilience and added to their human resources dedicated to cybersecurity.

- The four Connecticut officials conducting the 2019 annual review concluded that the four utilities they reviewed are taking adequate defense measures to protect themselves against their perceived threats.

- The stark 2018 U.S. Intelligence Community warnings of cybersecurity threats to our national critical infrastructure continued during 2019. Current and former intelligence officials offered troubling public statements regarding the extent and severity of nation state threats against the American energy sector. Among their warnings were that nation states can penetrate any computer and Internet system, and that the more skilled actors can move from compromise of communications systems to digital implantation in operating systems. In September 2019, three former Secretaries of the Department of Homeland Security judged that the country "risks calamity if the United States does not step up its game."

- The past year saw extensive, new work to bolster Connecticut public utility cybersecurity resilience. Phishing, spear phishing, threats to cloud information storage and insider threats were often cited as among the most worrisome threats faced. The companies also reported greater attention to human resources including finding cybersecurity personnel, vetting the hiring of all employees and managing insider threats to security compromise. Supply chain management and vendor vetting received increased scrutiny. The companies sought and received greater cooperation from federal authorities, trade associations and other companies. There remains room for more extensive collaboration with the Connecticut Intelligence Center.

- An unresolved question demanding federal attention is the distance between reported Intelligence Community assessments of the extent and depth of critical infrastructure cyber penetration and the fact that Connecticut utilities report no evidence of breaches despite serious, intense efforts to detect and deflect such penetration. If American public utilities including ours in Connecticut are as compromised as Intelligence Community officials assert, and if those utilities, despite arduous, serious, good-faith efforts to detect and eliminate threats do not find evidence of penetration, they need and deserve U.S. Government timely and detailed information sharing.

All four Connecticut utilities participating in this review explicitly affirm that neither the Department of Homeland Security nor any other federal agency has not notified them of cyber compromise.

The State of Connecticut officials and the Connecticut public utilities participating in the 2019 critical infrastructure 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.

Sincerely,

Arthur H. House

Arthur H. House
Chief Cybersecurity Risk Officer, State of Connecticut

Copies:

Commissioner Katie S. Dykes, Department of Energy and Environmental Protection
Chair Marissa P. Gillett, Public Utilities Regulatory Authority
Commissioner Josh Geballe, Department of Administrative Services
Commissioner James C. Rovella, Department of Emergency Services and Public Protection
Chief Information Officer Mark Raymond

October 10, 2019

Connecticut Critical Infrastructure 2019 Annual Report

Executive Summary

Connecticut's critical infrastructure companies took seriously the increased threat levels they faced during the past year and appear to have thwarted the threats they identified. Utilities improved their cybersecurity defenses, invested more in resilience and added to their human resources dedicated to cybersecurity. The four Connecticut officials conducting the 2019 annual review concluded that the four utilities they reviewed are taking adequate defense measures to protect themselves against their perceived threats.

The stark 2018 U.S. Intelligence Community warnings of cybersecurity threats to our national critical infrastructure continued during 2019. Current and former intelligence officials offered troubling public statements regarding the extent and severity of nation state threats against the American energy sector. Among their warnings were that nation states can penetrate any computer and Internet system, and that the more skilled actors can move from compromise of communications systems to digital implantation in operating systems. In September 2019, three former Secretaries of the Department of Homeland Security judged that the country "risks calamity if the United States does not step up its game."

The past year saw extensive, new work to bolster Connecticut public utility cybersecurity resilience. Phishing, spear phishing, threats to cloud information storage and insider threats were often cited as among the most worrisome threats faced. The companies also reported greater attention to human resources including finding cybersecurity personnel, vetting the hiring of all employees and managing insider threats to security compromise. Supply chain management and vendor vetting received increased scrutiny. The companies sought and received greater cooperation from federal authorities, trade associations and other companies. There remains room for more extensive collaboration with the Connecticut Intelligence Center.

An unresolved question demanding federal attention is the distance between reported Intelligence Community assessments of the extent and depth of critical infrastructure cyber penetration and the fact that Connecticut utilities report no evidence of breaches despite serious, intense efforts to detect and deflect such penetration. If American public utilities including ours in Connecticut are as compromised as Intelligence Community officials assert, and if those utilities, despite arduous, serious, good-faith efforts to detect and eliminate threats do not find evidence of penetration, they need and deserve U.S. Government timely and detailed information sharing.

All four Connecticut utilities participating in this review explicitly affirm that neither the Department of Homeland Security nor any other federal agency has not notified them of cyber compromise.

The State of Connecticut officials and the Connecticut public utilities participating in the 2019 critical infrastructure review and 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.

The 2019 Review Process

Avangrid, Eversource Energy, Aquarion Water Company and Connecticut Water Company held review sessions with four State of Connecticut officials during July, August and September 2019 to review their respective states of cybersecurity resilience. The participating Connecticut officials were:

- Arthur House, Chief Cybersecurity Risk Officer;
- Stephen Capozzi, Public Utilities Engineer, Public Utilities Regulatory Authority;
- David Geick, Director of Information Technology Security Services, Bureau of Enterprise Systems & Technology, Department of Administrative Services; and
- David Palmbach, Intelligence Analyst, Connecticut Intelligence Center.

Chief Executive Officers or senior managers led the company review session teams, which normally included ten to fourteen participants. 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.

Threats and Challenges

2018 had seen two major disclosures of threats posed to U.S. critical infrastructure management. The first was the March 2018 Department of Homeland Security (DHS) and Federal Bureau of Investigation (FBI) warning of Russian involvement in cyber attacks on

U.S. infrastructure to target commercial networks and stage malware, spear phishing and remote access into energy sector networks. The second was a July 2018 update stating that that there were hundreds of victims of Russian military intelligence attacks including infiltration of power plant control rooms and control of parts of the electricity grid.

Such disclosures continued in 2019. United States Intelligence Community leaders and former intelligence officials made remarkable public statements regarding the extent and severity of nation state threats against the American energy sector. Two consistent themes of these statements are (1) that nation states with investment of money and time can penetrate any computer and Internet system; and (2) that the more skilled actors can move from compromise of communications systems to digital implantation in operating systems.

The Director of National Intelligence in the January 29, 2019 statement for the record of the Worldwide Threat Assessment of the U.S. Intelligence Community offered stark assessments of adversary nation state cyber capabilities, concluding that "For years, they have conducted cyber espionage to collect intelligence and target our critical infrastructure to hold it at risk."

Specifically, China "has the ability to launch cyber attacks that cause localized, temporary disruptive effects on critical infrastructure – such as disruption of a natural gas pipeline for days to weeks – in the United States." Russia "is now staging cyber attack assets to allow it to disrupt or damage U.S. civilian and military infrastructure during a crisis" and "has the ability to execute cyber attacks in the United States that cause localized, temporary disruptive effects on critical infrastructure – such as disruption an electrical distribution network for at least a few hours…"

The report assesses that Iran is "attempting to deploy cyber attack capabilities that would enable attacks against critical infrastructure in the United States and allied countries." North Korea is a significant threat to financial institutions, but also "retains the ability to conduct disruptive cyber attacks." Non-state and unattributed actors "could increasingly disrupt U.S. critical infrastructure."

By all accounts, the volume, sophistication, creativity and persistence in efforts to penetrate and gain control of U.S. utilities and their services all were greater in 2019 than in the past. Former Deputy Director of the National Security Agency Chris Inglis reported a significant increase in the sheer number of probes and attempted attacks on American critical infrastructure. In May 2019 he stated that Russian hackers "are managing 200,000 implants in U. S. critical infrastructure." In September 2019, three former Secretaries of the Department of Homeland Security concurred that the U.S. Government was not doing enough to defend against cyber attacks and that the country "risks calamity if the United States does not step up its game."

Intelligence officials in informal discussions and public presentations have made the point that those in the energy generation, transmission and distribution businesses cannot

presume that barriers to Russian penetration exist or are working. They assert that the implantations have gone beyond communications, into what they call “administration,” meaning beyond simple internal and external communications and into management systems. Generation and transmission activities are identified as being the most directly penetrated and compromised.

Cybersecurity awareness and threat information sharing also increased substantially, including constructive work from the Multi-State Information Sharing and Analysis Center (MS-ISAC) and the Electricity Information Sharing and Analysis Center (E-ISAC).

During the year, the Department of Homeland Security increased its outreach to Connecticut utilities, established or reinforced contacts and offered resources to assist in detection and control of threat vectors. DHS created the Cybersecurity and Infrastructure Security Agency (CISA) at the end of 2018, “…working with partners to defend against today’s threats and collaborating to build more secure and resilient infrastructure for the future.” Some Connecticut utilities also received limited classified information briefings from the FBI. Utilities also received assistance from U.S. National Laboratories during 2019.

All Connecticut utilities participating in this report have seen more extensive, proactive communication with the federal government to identify and defend against cyber penetration. Yet, national security officials insist that utility executives and many players with high-level security clearances are not aware of the extent of ongoing operations penetration and implantation.

If that is indeed the case, the result is a significant national security vulnerability partially addressed by domestic authorities but not fully communicated beyond the boundaries of the national security intelligence agencies. While local distribution companies such as those in Connecticut make serious, strenuous efforts to find and root out foreign implantations, their work will necessarily be incomplete until intelligence sharing reflects partnership at levels not currently in place.

All four Connecticut utilities participating in this review explicitly affirm that neither the Department of Homeland Security nor any other federal agency has not notified them of cyber compromise.

Connecticut utilities manage their cybersecurity defense programs fully aware of serious attempts to compromise their operations. Some use the most modern, effective defense systems available. All receive at least some degree of federal government support, and all work with trade associations and other companies to protect themselves. Yet this work proceeds while top national intelligence personnel warn that not all information is being shared, that nation states and other actors can compromise American utilities, and that, in fact, their administrative systems currently bear foreign presence.

In recent years, Connecticut utility officials have increased communications with federal authorities, especially the Department of Energy, and expressed appreciation for the

enhanced cooperation. The Connecticut officials conducting this annual assessment and some of the Connecticut utility executives share the understanding that there is scope for more extensive federal partnerships, underscored by statements from current and previous federal leaders who have warned of and lamented foreign penetration. National Security Agency General Counsel Glenn S. Gerstell gave voice to this frustration in September 2019 in stating: "The simple fact of the matter is that no nation has yet devised an effective solution to the conundrum of how to respond in a definitive and dispositive way to another nation state's malicious cyber activity."

Connecticut utilities displayed seasoned, mature responses to the question as whether they were more or less resilient to the prospect of a cyber attack than they were last year. Among the areas cited as deserving increased attention, utilities pointed to the need for more security cloud computing and protection against compromise from internet-connected devices. In addition to having more names to call in federal agencies for help with specific problems, Connecticut utilities continue to bring on board more personnel with higher-level security clearances than in the past – or are able to secure such clearances for existing personnel. Utilities find more briefings available with some redundancy in those briefings, a situation inevitable in the general effort to structure more extensive and productive classified information sharing.

Specific Threats Reported by Connecticut Utilities

Aggression against Connecticut utilities grew during the past year, with an increased number of threat actors, larger volume of attempted penetrations and introduction of new, more sophisticated attack weaponry. Nation states remain active, with most threats coming from the same four nations previously reported: Russia, China, Iran and North Korea. One utility recorded threat attempts from more than 1,000 distinct actors (which may include sources using multiple identities). As in the past, threat management is constant work, placing considerable pressure on utility security management teams.

As in past years, during 2019, phishing and spear phishing attempts to gain entry into communications systems remained among the top threats. The companies all reported increased attention to insider threats – the potential for security compromise caused by employees or trusted vendors and contractors.

A new factor in 2019 has been the growth of machine-to-machine threats, met by concurrent machine-to-machine defenses. A rough parallel is the scenario the Navy faces with the former pattern of one aircraft seeking to bomb a ship replaced by the modern scenario of a large number of computer-managed attack missiles met by computer-managed defense counter measures.

Utilities reported that increased use of cloud storage has brought new forms of cybersecurity problems threatening information compromise or diversion of vital information to unauthorized places.

Main Points and Findings

Managing cybersecurity threats became more difficult during the past year. One reason was that some companies have augmented their searches for nation state, signature-based, specific attack technology with greater reliance on artificial intelligence to detect behavior suggesting or indicating compromise. In recent years, companies have moved from closely holding and protecting information regarding cyber attacks and defenses to settings of better situational awareness, more extensive information sharing and comparison of effective detection techniques. Companies share both information regarding threats and effective counter measures through more timely and specific briefings with federal resources, trade associations and specialized consultants.

Despite such advances, utilities still face the security challenge of protecting substations spread across an operating area, monitored by surveillance systems and requiring periodic human inspections. Monitoring obviously seeks to pay greatest security attention to the most critical facilities. Ensuring both cyber and physical substation security is demanding; every company must decide what level of time and effort is appropriate, realizing that complete coverage is not possible. The utilities continue to seek additional ways to strengthen the dual problem of physical and cyber security including advances in verification software, social engineering advances and the use of drones.

There is room for improved collaboration between Connecticut utilities and the Connecticut Intelligence Center. Connecticut utilities understandably protect information regarding external penetration attempts and their ability to thwart them. At the same time, CTIC's efforts to understand and share information regarding cyber aggressions against Connecticut companies would be improved by more extensive information exchange.

Corporate Culture

Corporate culture is a reflection in employee behavior of company leaders' priorities and values. That which is taken seriously inevitably starts with honest, heartfelt CEO exhortation. In all Connecticut utilities, boards of directors state their interest in cybersecurity, and executive management conveys that concern to employees. Some companies are more adamant and systemic in emphasizing cybersecurity, but in varying degrees cybersecurity awareness is part of every Connecticut utility's culture. One utility continues to start every employee meeting – on any topic – with a cybersecurity tip.

The Edison Electric Institute (EEI) has published a self-assessment product on the culture of security, which one utility uses to measure awareness and craft supplementary actions. Corporate culture vehicles include messages from management and discussions with

supervisors, security webinars, training sessions, sharing of intranet articles posters, emails and videos.

One executive described the unfinished effort to instill a healthy cybersecurity culture by saying, “We’re getting there.” Another reported the use of sanctions and disciplinary actions for employees insufficiently cognizant of the need for healthy cybersecurity habits. Efforts to create and sustain high levels of cybersecurity practices appear to be making progress but are still incomplete. The need to detect and counter insider threats was an enhanced area of security concern during 2019, related to corporate culture.

One interesting change has been the growing redundancy in alert communications. Utilities find that multiple alert paths result in similar, often overlapping warnings for the same event or vulnerability, from their internal detection, an Information Sharing and Analysis Center (ISAC), the Connecticut Intelligence Center (CTIC) or from consultants, government and private resources. Utilities report satisfaction in receiving concurrent threat communications. In the future, these redundancies may be combined or refined, but in the initial stages of detection they welcome information sharing and in turn convey messages to vendors and customers.

Human Resources

Insider threat was an area of particular attention during 2019, perhaps related to the success of other perimeter defenses and by the creativity of attackers trying to exploit new vulnerabilities. External probing of utility employees places a new burden on utilities to vet new employees more carefully and to verify the integrity of the existing workforce. Connecticut’s defense industry has long experience in reviewing the security of employees working in sensitive areas; their practices are becoming more commonplace in utilities, with some reporting significantly enhanced background checks prior to employment.

Hiring, training and retaining cybersecurity personnel has moved from a relatively small focus of human resource departments in past years to a high priority effort today. Utilities have rightly emphasized the need to hire and retain cybersecurity professionals to manage system architecture and network security across information technology (IT) and operational technology (OT) environments.

Hiring cybersecurity professionals has become more difficult challenge for smaller utilities. Nevertheless, the past year saw a marked increase in internships and in efforts to recruit needed talent through relationships with Connecticut and other New England colleges. Still, utilities noted successful recruitment and retention of cybersecurity personnel as an ongoing concern.

There has been a net increase in the number of utility officers with security clearances, at both the top secret and secret levels.

Some Connecticut utilities increasingly look to consultants to manage their cybersecurity activities. The ability to draw on the resources of a consultancy and to benefit from its work in other sectors sometimes outweighs the disadvantage of in-depth company-specific experience.

Phishing and Spear Phishing

Phishing and spear phishing remain prevalent and dangerous, the single most common means to attempt entry into a company's IT and OT systems, and defenses to prevent such entry continue to receive considerable attention. Sustained, custom-tailored spear phishing attacks are difficult to thwart. 2019 saw increasingly clever spear phishing, some of which succeeded in compromising their targets before being contained. One company used an example of a genuine spear phishing penetration against a senior executive as a teaching example.

One utility reported detection of ongoing phishing attempts to extract money from employees: frauds appearing to originate from senior officers asking that funds be sent to a given account or asking for personal financial information and account numbers. Such activity is called "Business Email Compromise" and is a significant threat facing the business community.

All utilities have phishing training programs, some expanded to include awareness of suspicious attachments and dangerous data entry threats. Some companies do post-training tests to evaluate the training. Even with such efforts, in some cases more than ten percent of employees have continued to click on false messages.

Most companies now have "report phishing" buttons on their email applications, enabling employees to forward suspicious emails for review. This simple feature enables employees to help in detection of and response to phishing attempts. Some companies offer "shark awards" to the first employees to detect "phishing." Another innovation is establishment of more clear identification of external sources of emails and internet traffic, so recipients can more reliably see from whom email is coming.

Utilities are experimenting with solutions for employees who do not learn the required discipline to decline phishing attempts. Remedies include having supervisors talk to employees who fail phishing tests. Another is to identify employees who require advanced, remedial training. The problem of recidivism remains, and utilities will eventually need to decide whether lack of phishing awareness is grounds for suspension or dismissal.

Consulting Services

Utilities increasingly use national information sharing and analysis centers for assistance in becoming aware of new threats, in addition to their roles as information resources. Private consultants are more important to security than ever, as cybersecurity is increasingly a

private security domain. Aside from national security considerations, the invention of new cyber programs and malware and the defenses against new dangers largely take place in private companies. The scope and technical demands of detecting and managing cyber threats present challenges beyond the in-house capabilities of Connecticut utilities. In past years, consultants were used especially to bolster firewalls and detect vulnerabilities. 2019 saw increased consultant use for a broad range of cybersecurity needs, especially to recommend future cybersecurity investments.

C2M2 Results and Discussion

Connecticut's annual cybersecurity process allows utilities to select their own standard of progress measurement. To date all have elected to use the Cybersecurity Capabilities Maturity Model, or "C2M2."[1] During the first two years of using C2M2, all utilities saw growth toward greater maturity, albeit at different rates and in different areas, in the ten C2M2 cybersecurity domains. Some used external consultants to assist in C2M2 evaluation.

All utilities continued on their prior growth paths. One utility conducts semi-annual C2M2 assessments and uses the results to identify areas of future improvement and set future goals. Some, however, reported that their self-evaluation scores for the C2M2 domains have tended to stabilize at the upper levels as they approach the highest maturity C2M2 levels.

Both the challenge difficulty and the ability to meet the challenge continued to evolve in a pattern suggesting constant adjustment. Some utilities question whether C2M2 should continue to be their standard to progress measurement in future years. They acknowledge that should they decide to change standards, they would bear the burden of selecting and managing a replacement standard. Some have looked toward the National Institutes of Standards and Technology Cybersecurity Framework standards as possible future measurement standards, replacing C2M2.

For the present, all utilities still found value in performing the C2M2 self-assessment to identify and prioritize cybersecurity program needs.

C2M2 reviews cover a wide range and support ongoing management adjustments. One specific example of a lesson learned was the need to restrict access to certain accounts to management personnel with elevated security privileges.

Investments

[1] The ten domains covered by the C2M2 self-assessment are: Cybersecurity Program Management, Risk Management, Asset Management, Identity and Access Management, Threat and Vulnerability Management, Situational Awareness, Information Sharing and Communications, Event and Incident Response, Supply Chain and External Dependencies Management and Workforce Management.

Discussion of cybersecurity investments involves both company priorities and the ability to have money spent on those priorities receive regulatory authority approval. In the United States, both utilities and regulators face the difficult challenge of keeping up to speed with technical improvements in cybersecurity detection and management. The normal process is for the utility to decide that a particular investment is wise and would enhance security, to make the investment and then through a rate case to seek approval from the regulator to include that expenditure in the rate base. Regulators face the increasingly demanding challenge of understanding new technology and determining appropriateness for rate base inclusion.

Increased attention to more complex cybersecurity challenges may become expensive. The need for both company and regulator to stay up to speed regarding investment opportunities adds new dimension to a classic regulatory tension. Along with the decision to make such investments, utilities need to keep educating the regulators as to their necessity and usefulness. Connecticut's annual cybersecurity review process investigates and assesses some utility cybersecurity investments but does not replace the core process of regulatory review.

Investment opportunities proliferate in the American tradition of private sector innovators finding new solutions. Connecticut utilities usually reported several categories of cybersecurity investment. Prominent among them in 2019 were design, engineering and implementation of new or improved detection and management systems. There was special attention to security control systems to assess and fill detection gaps, risk assessment, focus on insider threat challenges, user behavior, end-point customer protection, incident response and firewall management. Utilities also noted adding security architecture to their cyber programs, greater investment in people, time allocated to security work, systems development and vulnerability management.

Supply Chains

As utilities seek to solve new cyber problems, the need to rely on third-party vendors in the electricity and natural gas areas is growing markedly. Utilities have to determine how a new piece of equipment, software product or process would affect operations and networks. One utility identifies more than 200 suppliers receiving special scrutiny and has added personnel to manage the process. With such growth comes the need to strengthen supply chain management and tighten up procurement to examine purchases and assess the vulnerabilities that accompany others' products and services.

Utilities are finding interesting solutions to growing supply chain management security concerns. Among them are developing legal and technical processes for testing devices and using federal assistance to test devices that a manufacturer or intellectual property owner would not otherwise allow. Another is performing investigations into supply companies to

evaluate specific product or service risks and also to determine who owns the company offering the sale. Corporate ownership was an area of increased focus during 2019.

Third-party vetting is changing procurement practices and has become a major cybersecurity activity with more systemic monitoring of external suppliers, including international comparisons and use of code verifications. Vendor reaction to enhanced vetting requirements ranges from surprise and need for education to sophisticated incorporation of cybersecurity assurances in requests for business. Vetting is both done on a case-by-case basis and is more automated, reaching beyond third-party to fourth-party components.

Services are available to offer supplier scorecards with grades and assessments of procurement control and risk factors. Active use of external rating services to vet and shape the customer relationship with suppliers has led to terminating vendors and adding new ones based on cybersecurity concerns. One utility reports a net decrease in the number of vendors used because some have not been able to ensure adequate cybersecurity protections.

Of all the areas addressed during 2019, Connecticut utility consensus was that supply chain management was the area of greatest progress. Nevertheless, all companies recognized that supply chain vetting continues to grow in complexity.

Penetration Testing

Terms of reference for penetration testing and use of the results have evolved in recent years. A few years ago, when awareness of cyber threats was in its initial stages, companies would set defenses and retain penetrators to see if they could enter information technology or operating systems (or both). It has become apparent that any company can be penetrated if the force seeking entry devotes enough time and resources to doing so. A good penetration team today looks at all the possible ways to break into IT and operation systems, executes entry, reports on how it was done and identifies changes needed to remedy insufficient protections.

Not all utilities are satisfied with the penetrators hired to do this work. Some saw the task as one of general defense assessment rather than simulation of attack. Others include utility staff in their work, thereby enabling the utility to see how vulnerabilities are discovered. All utilities used penetration testing to identify vulnerabilities and pathways to breaches, but not all utilities focused on testing of operations technology and consequent remediation. The utilities did respond to penetration test findings, which included recommendations regarding security architecture, patches, attention to substations and enhanced security for gas pipeline facilities.

Manual Start-Ups

Most utility operations are computer managed. The 2015 attack on Ukraine's electric distribution system demonstrated that when systems are taken off-line, sometimes the only way to restore power is the old-fashioned way, by sending personnel to facilities and substations and using manual, non-computer managed processes to restart operations. Connecticut utilities all practiced manual restarts during 2019. One company identified 17 distinct exercises requiring non-computer, personnel-generated restarts.

During the past several years, as utilities have transitioned to computer management of operations and manual operations have atrophied, there are fewer employees with manual operations experience. While training in manual operations does continue, there are simply not enough employees able to run all facilities manually. In the event of a cyber compromise shutting down facilities, utilities will need to identify priorities for human attention and startup, recognizing that it will not be possible to restart them all.

Cyber Exercises

In recent years, both public and utility perception of critical infrastructure cybersecurity has advanced from being somewhat esoteric problem shared by utilities and some government agencies to much wider issue of community and national concern. The security of our public utility services is now seen as a legitimate matter of focus by the utilities and federal, state and local governments, security officials, trade associations and first responders. Indeed, in certain circumstances a cyber threat is a matter of national security requiring federal and regional recovery assistance.

The most valuable exercises tend to be those that begin with existing strategies and action plans and move to address threats not identified ahead of time. Companies are compelled to adjust to new scenarios. Rehearsal of the anticipated and reaction to the new with subsequent assessment and candid critique enable lessons learned to form a base for future improvement.

All Connecticut utilities participated in cyber-related exercises during the past year. Among the specific challenges posited were the ability to sustain service delivery, business continuity, response to malware introduction and use of ransomware and manual operations restart. Lessons learned included the need to know the exact location of all servers and how they are controlled.

As threat scenarios evolve, the need to practice response with adequate sophistication also increases. In future years exercises will need increasingly to address the full range of potential community disruption, going well beyond emergency exercises practiced to date.

Post-Compromise Recovery Plans

All utilities maintain emergency response plans. Section 16-32e of the General Statutes of Connecticut requires the four utilities reviewed here (among other public service

companies) to file with the Public Utilities Regulatory Authority every two years an updated plan for restoring utility service interrupted as a result of an emergency. PURA last received and reviewed emergency plans in 2018. See Decision dated August 29, 2018 in Docket No. 18-03-29 2018 PURA Review of Connecticut Public Service Company Plans for Restoration of Service that Is Interrupted as Result of an Emergency. PURA, DESPP and the Department of Public Health (DPH) will next review undated plans in by 2020. Each company should expect to update its respective plans to include any new and relevant cybersecurity information.

Electric distribution companies must have post-compromise of critical infrastructure recovery plans that meet "NERC CIP" – the North American Electricity Reliability Corporation (NERC) critical infrastructure protection (CIP) requirements. The requirements are "designed to secure the assets required for operating North America's bulk electric system." A key part of the NERC CIP is maintenance of updated plans and updated lists of people with assigned responsibilities that move to action plans and exercises.

Connecticut utilities conduct national and trade association exercises and work with Connecticut's Department of Emergency Services and Public Protection (DESPP) in a range of exercises and actual emergencies, often including hurricanes and ice storms. The utilities emphasized their interest in participating in future exercises postulating a cyber attack as the core exercise premise.

Some of the utilities underscored the need to know what state emergency officials and the Governor would want from them in the event of a cyber incident compromising delivery of essential utility services. Knowing that the demands will be different from normal emergency management, the utilities expressed the need to have a better sense of what the Governor will want them to do. Specific concerns are that communications must begin immediately, before all facts are known. Rumor control and command of information would be critical.

In a normal storm, one of the principal requests from Governors is prediction of recovery time, which will not necessarily be possible in a cyber attack. A cyber event may involve new malware requiring assessment, or malware implanted in unanticipated places, requiring discovery, containment and control. A cyber attack is likely to involve more than one state, more than one utility and result in prolonged service disruption. Rehearsed, previously cleared communication templates will also be necessary to address both disinformation and misinformation. The utilities expressed readiness to participate in emergency exercise scenarios in order to comply with the expectations of DESPP and the Governor in the event of a critical infrastructure cyber attack.

The common priority of Connecticut utilities' response plans is to seek resumption of operations. There has not been extensive planning to endure outage greater than 10 days or two weeks. Should utilities not be able to resume delivering electricity, natural gas or water after normal and reserve fuel supplies are depleted, they would look to state

emergency managers and the National Guard to help manage the consequences of critical infrastructure shut down.

Relationship Between IT and OT Systems

A continuing, basic challenge in sustaining sound utility cyber hygiene is shielding operational technology from any form of communication other than the company's disciplined, operational command and control. Connecticut utilities manage separation of IT and OT communications both by use of firewalls to prevent unwanted intrusion, sharing or overlap and by human attention and inspection.

IT and OT communications sometimes need to operate in the same domain in field operations. Connecticut utilities pay special attention to managing their distinct separation in field assets and other field work. This is an area of growing concern as more operational devices and functions use and depend on IT-based systems.

Program Assessment

This being the third year of annual critical infrastructure cybersecurity reviews conducted within the negotiated purview of the 2016 Public Utilities Regulatory Authority Cybersecurity Action Plan, each utility was asked to assess the program's value and to offer suggestions or changes that might improve the process and resulting annual reports. The core tenets of that agreed procedure are that reviews will be annual and confidential, with Connecticut State participation restricted to four representatives and unlimited company attendance. Participating companies are free to choose their own evaluation standards. Although confidential, there will be an ensuing report to the Governor, General Assembly and Office of Consumer Counsel, with the utilities having the right to read and strike any language prior to report release.

Regarding benefits, utilities cited the fact that state authorities, both the executive and legislative branches, learn and consequently gain a degree of comfort about utility cybersecurity resiliency work. Both that knowledge and reduced anxiety resulting from collaboration are valuable in promoting understanding as to the seriousness of cyber threats and the extensive work underway to contain them. The reviews also lay a foundation of current understanding that can be amended if a utility were to identify a new problem or find something that required updating.

There is general comfort with the specific points negotiated in 2016 regarding management of the reviews:

- Annual reviews are the preferred frequency;
- Regarding participation, utilities continue to prefer to bring as few or as many people to the meetings as they deem appropriate. Having four state participants is

roughly the right number, but the utilities are open to a slightly larger number if additional participants would bring new perspectives or fill gaps;
- The meetings should continue to be confidential so that conversations can be candid and constructive;
- The utilities like being able to select their own review standard. There was questioning as to whether C2M2 would continue to be the best vehicle in the future or whether it should be replaced or complemented;
- A final report should be submitted to the Governor, General Assembly and Office of Consumer Counsel; and
- Each participating company needs to have the right to read the report in draft and edit or take out language it finds unacceptable before the report is final.

Conclusions

The array and sophistication of cybersecurity threats facing Connecticut's public utilities is greater than it has been and continues to become more dangerous. The utilities are well aware of the increasing dangers, take them seriously and demonstrate top-level commitment to construct and manage defense. They are increasing cybersecurity culture generally, strengthening their in-house expertise and complementing what they have by retaining the services of external personnel and services. They know of no compromises to Connecticut's critical infrastructure operating systems and deserve credit for concerted efforts to see that none occur.

Connecticut's critical infrastructure cybersecurity work addresses the threats the utilities are aware of, with increasing assistance from other companies, trade associations and proactive assistance from the Department of Homeland Security, Department of Energy and Federal Bureau of Investigation. Connecticut utilities recognize that reports and public comments by senior U.S. Intelligence Community officials state that nation states and perhaps other actors have executed implants into the administrative areas of U.S. energy generators, transmitters and distributors.

The gap between the implantation that the Intelligence Community says is taking place and the ability of utilities to take counter measures must receive priority attention. The discrepancy demands federal attention. If American public utilities are as compromised as Intelligence Community officials assert, and if those utilities, despite arduous, serious, good-faith efforts to detect and eliminate threats do not find evidence of penetration, they need and deserve U.S. Government timely and detailed information sharing. The answers may include more extensive, high-level security clearances, more complete information sharing and increased candor regarding what the threats are and where they are coming from.

Given this setting of increasing threats and constantly threatened defense, utilities must prepare for the consequences of a breach. With potentially unprecedented and damaging consequences of prolonged absence of critical services, the utilities need to participate in

statewide and regional exercises postulated on such absence. They, along with federal, state and local authorities, would face the need for executive decisions, communications demands and crisis alleviation never before encountered. The utilities recognize their obligation to participate in such exercises and rehearsals before an actual compromise occurs.