# States of Cybersecurity: Electricity Distribution System Discussions

*I. Peña, M. Ingram and, M. Martin, NREL. Prepared for Greg Singleton, DOE/EPSA*

# Acknowledgment

This document was prepared for Greg Singleton at the Department of Energy's Office of Energy Policy and Systems Analysis (EPSA). NREL would like to acknowledge EPSA's encouragement and support throughout the process. The authors would like to specially thank Gian Porro at NREL for his thoughtful comments, and to the 22 participating utilities.

# Notice

# List of Acronyms

| | |
|---|---|
| APPA | American Public Power Association |
| CIP | Critical Infrastructure Protection |
| DHS | U.S. Department of Homeland Security |
| DOE | U.S. Department of Energy |
| EEI | Edison Electric Institute |
| EPSA | Office of Energy Policy and Systems Analysis |
| ES-C2M2 | Electric Subsector Cybersecurity Capability Maturity Model |
| FBI | Federal Bureau of Investigation |
| IOU | investor-owned utility |
| ISO | International Organization for Standardization |
| IT | information technology |
| NERC | North American Electric Reliability Corporation |
| NIST | National Institute of Standards and Technology |
| NISTIR | National Institute of Standards and Technology Internal/Interagency Report |
| NRECA | National Rural Electric Cooperative Association |
| NREL | National Renewable Energy Laboratory |
| OT | operational technology |
| RMP | U.S. Department of Energy Risk Management Process |
| TVA | Tennessee Valley Authority |

# Executive Summary

State and local entities that oversee the reliable, affordable provision of electricity are faced with growing and evolving threats from cybersecurity risks to our nation's electricity distribution system. All-hazards system resilience is a shared responsibility among electric utilities and their regulators or policy-setting boards of directors. Cybersecurity presents new challenges and should be a focus for states, local governments, and Native American tribes that are developing energy-assurance plans to protect critical infrastructure. This research sought to investigate the implementation of governance and policy at the distribution utility level that facilitates cybersecurity preparedness to inform the U.S. Department of Energy (DOE), Office of Energy Policy and Systems Analysis; states; local governments; and other stakeholders on the challenges, gaps, and opportunities that may exist for future analysis.

The need is urgent to identify the challenges and inconsistencies in how cybersecurity practices are being applied across the United States to inform the development of best practices, mitigations, and future research and development investments in securing the electricity infrastructure. By examining the current practices and applications of cybersecurity preparedness, this report seeks to identify the challenges and persistent gaps between policy and execution and reflect the underlying motivations of distinct utility structures as they play out at the local level.

This study aims to create an initial baseline of cybersecurity preparedness within the distribution electricity sector. The focus of this study is on distribution utilities not bound by the cybersecurity guidelines of the North American Electric Reliability Corporation (NERC) to examine the range of mechanisms taken by state regulators, city councils that own municipal utilities, and boards of directors of rural cooperatives.

Using evidence from a questionnaire covering 22 utilities, 19 of which are non-federally regulated by NERC, this document outlines the identified minimum actions that these utilities are performing to secure their infrastructure from cyber threats. This questionnaire consists of 33 questions covering 6 categories:

1. Demographics—type of utility, size of utility, and annual budgets for information technology (IT) and cybersecurity
2. Standards and governance—policies, efforts in place, involvement with collaborative initiatives or organizations, and handling of IT and operational technology responsibilities
3. Oversight—state-level efforts, including public utilities commission efforts; county and city governments; and reporting of attempted cybersecurity breaches
4. Planning—security plans, business processes, cybersecurity audits, and prioritization of components and functions for new cybersecurity measures
5. Execution and performance—number and type of cybersecurity attacks faced by the utility, situational awareness, penetration testing, and business and control systems integration

6. Support—cybersecurity criteria applied to vendors, vulnerability assessment for new acquired products, and learning from past cybersecurity incidents and adapting to new models.

**Notable Findings & Discussion**

Typically, public power distribution companies, cooperatives and municipalities, are connected to the local governments within their service territory. These governments usually compose, appoint, or are otherwise members of the public power utility boards of directors. It is incumbent on any board of directors to determine company policies and review threats and risks. Yet the main findings of our research suggest that having an internal cybersecurity policy is not necessarily the first step toward addressing cybersecurity; rather, different efforts such as budgeting projects, piloting programs, and establishing strategies to implement cybersecurity practices can be the first initiatives. In fact, it was surprising that utilities listing more than one cybersecurity effort do not have an established cybersecurity policy.

Cybersecurity expenses are usually provided through a base rate allocation, meaning that expenses are covered from existing rates. Understandably, several respondents reported budgeting for cybersecurity as a primary challenge; in fact, some reported that no formal cybersecurity budget is established. For those that reported specific cybersecurity budgets, the cyber budgets are not consistent with higher IT budgets.

Utilities reported interacting mostly with national associations to improve their cybersecurity postures. In addition to associations such as the National Rural Electric Cooperative Association, American Public Power Association, and Edison Electric Institute as well as InfraGard and fusion centers, utilities reported collaborating with multiple organizations, including the Utilities Telecom Council, Utility Technology Association, Information Sharing and Analysis Center, and regional public power associations and trade associations. Utilities also reported that state, county and city agencies have encouraged them to work individually to improve cybersecurity, and to some extent state-level agencies have monitored security planning, implementation, and performance. However, the data collected suggest that the boards of directors of municipalities and cooperatives are not strongly involved in cybersecurity actions.

Although many utilities do not have a formal cybersecurity policy in place, eight reported conducting risk assessments for their cybersecurity plans and following best practices. They perceive these efforts as actions beyond those required by federal, state, and local regulators. In addition, more than half of the utilities have already conducted cybersecurity assessments or audits on information or control systems. There is broad utilization of guidelines from the National Institute of Standards and Technology and DOE, but the International Organization for Standardization (ISO) 11000, ISO 20071, ISO 27002, and NERC's Critical Infrastructure Protection standards suggest a lack of a cohesive cybersecurity approach. It seems that most utilities choose one or two of the known guidelines, but the reason to select one instead of another is not clear.

Most utilities reported using network segmentation as a cybersecurity strategy. Two other strategies, defense in depth and defense in breadth, are also popular. The data suggest that when

a utility reported a defense in depth or defense in breadth cybersecurity strategy, they also reported having a zero-trust network, network segmentation, or air gapping.

In addition, most utilities reported some type of adaptation and learning from past cybersecurity incidents. Even those that did not report being hit by a cyber attack in the last year reported establishing forensic investigations or upgrading or replacing software and sponsoring staff training.

# Table of Contents

# List of Figures



# List of Tables

# 1 Introduction

Although the bulk power system's providers[1] are bound by the North American Energy Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) guidelines for physical security and cybersecurity, distribution companies in the United States are under various state and local cybersecurity compliance regimes. In fact, it has been estimated that only 10–20% of grid assets are covered by NERC's CIP guidelines (Phelan 2015). The depth and specificity of cybersecurity practices varies tremendously from one state to another. This variation can lead to potential cybersecurity vulnerabilities at the distribution level while remaining compliant with guidance or requirements from the relevant regulatory bodies.

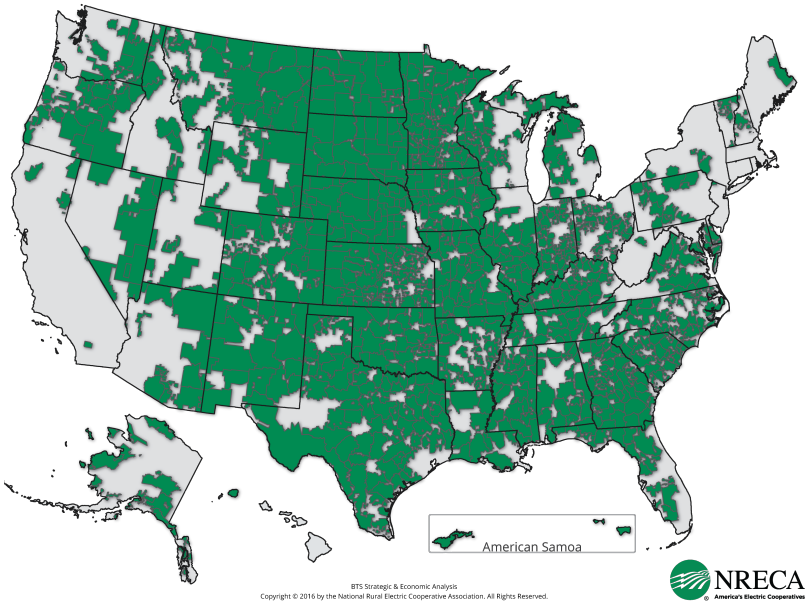


**Figure 1. Footprint of cooperative utilities across the United States.** ***Image from the National Rural Electric Cooperative Association (2016)***

Presidential Policy Directive—Critical Infrastructure Security and Resilience (The White House 2013), Executive Order 13636—Improving Critical Infrastructure Cybersecurity (The White House 2013), and the cybersecurity tenets included in Chapter 4 of the 2015 *Quadrennial Energy Review* (Office of Energy Policy and Systems Analysis 2015) highlight the need to strengthen the electricity sector's cybersecurity. The need is urgent to identify the challenges and inconsistencies in how cybersecurity practices are being applied in the electricity sector throughout the United States. Identifying these challenges will inform the U.S. Department of Energy (DOE), states, local governments and other stakeholders to support the development of best practices, mitigations, and future research and development investments to address cybersecurity in the electricity infrastructure.

[1] Generation companies producing more than 300 MW and regional transmission organizations and independent system operators

This study aims to create an initial baseline of cybersecurity preparedness within the electricity sector and to inform the DOE Office of Energy Policy and Systems Analysis, states, local governments, and other stakeholders on the challenges, gaps, and opportunities that may exist for future analysis. The focus is on distribution utilities not bound by NERC's cybersecurity guidelines to examine the range of policy approaches taken by state regulators, city councils that own municipal utilities, and boards of directors of rural cooperatives and how utilities implement these policies. This document is organized as follows: Section 2 presents notable findings. Section 3 presents the methodology and an overview of the data set, Section 4 presents the implications for the industry and states, and, finally, Section 5 concludes with further research and recommendations. The appendix contains the questionnaire and a detailed description of the answers.

# 2 Notable Findings

The main highlights of the report as suggested by the responses from the participating utilities are summarized as follows.

1. All the participating utilities reported having a cybersecurity team. Four utilities have single-person teams; most others have teams with no more than five people. A higher information technology (IT) budget does not necessarily imply a higher cybersecurity budget.
2. The most prevalent mechanism for recovering cybersecurity expenses is base rate allocation. This means that expenses are covered from existing rates.
    A. Cooperatives are using a base rate, security recovery factor (or similar), and "other" (i.e., folded into operations) as recovery mechanisms. Almost half of the co-ops reported not having a formal recovery mechanism in place, or they reported uncertainty about how these costs are recovered.
    B. Most municipalities that reported a formal mechanism in place selected using a base rate—five out of six, including one NERC-compliant municipality.
    C. The two participating NERC-compliant investor-owned utilities (IOUs) reported using a base rate and "other" (i.e., Federal Energy Regulatory Commission recovery mechanism).
    D. Utilities do not use adjustment clauses and deferral accounts as recovery mechanisms for cybersecurity expenses.
3. More than half of the utilities have already conducted cybersecurity assessments or audits on information or control systems. When asked about establishing priorities, responses suggested a reactive approach.
    A. In particular, 15 utilities reported that systems with known vulnerabilities become a priority for upgrade and replacement.
    B. All utilities except for one responded that a system becomes a priority for upgrade and replacement when it is compromised during a penetration test, and they also agreed that a system becomes a priority for upgrade and replacement if it has known vulnerabilities.
    C. Only one utility (NERC compliant) recognized that risk is an integral part of setting cybersecurity priorities.
4. Regarding established cybersecurity efforts, the data collected suggest that having a cybersecurity policy is not necessarily the first step toward addressing cybersecurity. It is important to highlight that the questionnaire did not specify criteria about what a cybersecurity policy includes, and as such the responses regarding the existence of a cybersecurity policy or governing document can represent different maturity levels. Similarly, the responses may suggest that policies are defined as experience is gained through practice.

A. Budgeting, piloting programs, and establishing strategies to implement cybersecurity practices were the most popular efforts reported, which suggests that these can be the first initiatives toward cybersecurity.

B. Seven utilities (six non-federally regulated) explicitly reported that they have no cybersecurity policy in place, and one reported having an in-process policy. Except for three of these, all reported having cybersecurity efforts in place, including an internally approved cybersecurity policy or governing document.

5. In terms of guidelines used, utilities with larger IT budgets (more than $500,000 annually) use the frameworks from either the National Institute of Standards and Technology (NIST) or DOE. There is no relationship between the size of the cyber budget and the use of these guidelines.
6. In terms of IT and operational technology (OT) management, all non-federally-regulated utilities that have an annual IT budget less than $1,000,000 manage IT and OT together.
7. The most prevalent reporting mechanism of attempted breaches is through the utilities' boards of directors. Although municipalities and co-ops are owned by cities or influenced by county leadership, respectively, municipal and co-op boards may not be strongly involved in cybersecurity efforts. This finding is concerning because boards of directors are normally responsible for ensuring effective plans to mitigate risk and protect assets.
8. Utilities reported various primary challenges to their cybersecurity efforts. The most cited by non-federally-regulated utilities was legacy systems (i.e., installed equipment basis), followed by budget, skilled workforce, and technology availability and maturity. One cooperative reported not seeing any issues (i.e., challenges) because they have not had any breaches yet. Other responses included "leaders have prioritized other work," "security is hard to prioritize within IT," "[the] way it is structured is difficult; people in charge of IT don't have a security background," "time constraints," and "lack of engagement from board and executives."
9. One-third of the participating utilities reported having a security plan that addresses both physical and cyber aspects, which aligns with NERC's cybersecurity maturity framework. Only one utility reported having a security plan that identifies critical cyber assets.
10. If a utility reported having a cybersecurity strategy (such as defense in depth, defense in breadth, a zero-trust network, network segmentation, or air gapping), it is likely that it has in place a governing cybersecurity document, a strategy to implement such governing document, or a pilot program. On the other hand, having a governing document or policy in place does not necessarily mean that the utility implements any of the cybersecurity strategies.
11. In addition to the cybersecurity strategies outlined and the situational awareness practices, 10 non-federally regulated utilities reported using penetration testing, and one is planning on using it, although it was not sure about the time frame. One cooperative mentioned using two companies to perform the testing.
12. On the surface, the use of numerous cybersecurity guidelines would imply a certain level of maturity, but given the diversity of these guidelines and the lack of a formal cybersecurity policy, the reactive approach to establish cybersecurity strategies might

suggest no cohesive use of these guidelines. As such, there is a need for a wider understanding of the use and applicability of each guideline and the implications for the design of formal cybersecurity policies. For instance, workshops offering training on the use of the guidelines in which state, county, and city organizations participate are key to promote cohesive approaches.

# 3 Methodology

There is an urgent need to identify the challenges and inconsistencies in how cybersecurity practices are being applied throughout the United States to inform the development of best practices, mitigations, and future research and development investments in securing the electric infrastructure in line with the presidential executive order of February 2013 and the cybersecurity tenets included in Chapter 4 of the 2015 *Quadrennial Energy Review*. The first step in that activity is to identify the foundation on which the states and local governments will need to build their cybersecurity policies. Policy recommendations to enhance distribution-level cyber resilience must reflect the current state of cyber-governance maturity.

To address these needs this project pursued a discussion based model with utility personnel to understand their perspectives, current practices, and ongoing challenges in cybersecurity. The interview framework, at a high level, has two parts: demographics and maturity-model-based questions. The demographics questions are included to enable researchers to assess and break down the overall response data. Early designs of the interview questions included significantly more demographic detail, but test trials provided feedback that participants were concerned with privacy and security of their responses in light of the small sample and limited diversity in the distribution sector.

The interview questions were organized around a maturity-model-based accountability framework, often referred to in the energy sector as GOES (governance, oversight, execution, and support) or GOSP (governance, oversight, support, and perform). Aligning questions that are technically based on federal guidance given by DOE (2014) or NIST (2014) and the public sector (Keogh and Cody 2014) into an accountability framework is consistent with state, local, and internal policy structures.

The interview questions were grouped into the following five sections:

- The first section of questions revolves around demographics, i.e., utility characterization.
- The second section, on Standards and Governance, sheds insight on an electric distribution company's governing policies, principals, and standards for cyber-physical security. These questions consider the accountability to establish the programmatic guidelines and performance expectations for cyber-physical security. Governance accountabilities include the ongoing assurance that the programs and processes are best practices and that they are implemented consistently. This section of questions reflects the direction in the Electric Subsector Cybersecurity Capability Maturity Model (ES-C2M2), which guides organizations to "establish and maintain an enterprise cybersecurity program that provides governance, strategic planning, and sponsorship for the organization's cybersecurity activities in a manner that aligns cybersecurity objectives with the organization's strategic objectives and the risk to critical infrastructure" (DOE 2014).
- The third section of questions, on Oversight, typically translates to compliance with state and local cybersecurity regulations. In a high-performing organization, an internally driven oversight function or operational assurance is necessary to critically monitor,

assess, and evaluate the conduct of operations to ensure that programmatic standards and expectations are met. This internal accountability is especially important when external regulations and accountabilities are underdeveloped or simply do not apply[2] and in organizations that have significant personnel limitations. Although NIST 800-53 prescribes a security control called "separation of duties" to address the potential for the abuse of authorized privileges, DOE recognizes that organizations with resource limitations may compensate for the separation of duty security control by strengthening internal audits and accountability (DOE 2014).

- The fourth and fifth sections on Planning and Execution and Performance are often considered together within a traditional accountability model, but they were broken out to reflect the emphasis on establishing and maintaining plans by the ES-C2M2 (e.g., Workforce Management, Threat and Vulnerability Management, Cybersecurity Program Management, etc.) and NIST Cybersecurity Framework. The NIST Cybersecurity Framework rests on five verbs that are the essence of execution and performance management: identify, protect, detect, respond, and recover.

- Because cybersecurity involves more than only technology and it encompass an integrated set of activities, the questionnaire also considers a sixth section on Support. These questions touch on supplier interdependencies as well training, which reflect the ES-C2M2 domain on Supply Chain and External Dependencies Management as well as Workforce Management.

Consider the sample of 22 participating utilities shown in Table 1. These 12 cooperatives, 7 municipalities, and 3 IOUs are headquartered in the following 14 states: Alaska, Alabama, California, Colorado, Florida, Kentucky, Louisiana, Mississippi, Montana, North Carolina, New Hampshire, Oklahoma, South Carolina, and Tennessee. Because of the size of the sample, the findings described are not representative of the states listed; rather, they can serve as starting points of discussions and assessments of cybersecurity approaches in any state.

[2] For example, although all bulk power system owners, operators, and users must comply with NERC-approved reliability standards, most distribution utilities and distribution business units within IOU's are not subject to these standards, including NERC's CIP standards.

**Table 1. Participating Utilities**

| State | No. of Utilities | Type of Utility[a] | Size of Utility (No. of Meters)[b] | NERC Compliant?[c] | TVA Jurisdiction?[c] |
|---|---|---|---|---|---|
| AK | 1 | 1 | Small | No | No |
| AL | 2 | 1,2 | Small, large | No | Yes |
| CA | 2 | 2,3 | Very large | Yes | No |
| CO | 1 | 1 | Small | No | No |
| FL | 1 | 1 | Large | No | No |
| KY | 1 | 2 | Very small | No | Yes |
| LA | 1 | 1 | Small | No | No |
| MS | 1 | 2 | Very small | No | Yes |
| MT | 1 | 1 | Very small | No | No |
| NC | 1 | 1 | Very small | No | No |
| NH | 1 | 3 | Medium | Yes | No |
| OK | 1 | 3 | Small | No | No |
| SC | 1 | 1 | Medium | No | No |
| TN | 7 | 1,2 | Very small, small, large | No | Yes |

[a]Type of utility—1: cooperative; 2: municipal; 3: investor-owned
[b] Size of utility (m)—<25,000: very small; 25,000–50,000: small; 50,000–100,000: medium; 100,000–250,000: large; >250,000: very large
[c] Columns added by the authors. These questions were not part of the questionnaire.

Because of the sample size, the analysis performed is descriptive and not intended to be statistically significant. Also, because of the characteristics of the questions, the level of cybersecurity maturity identified is subject to the respondents' and authors' interpretations. The results presented should be used as *examples* of the status of cybersecurity awareness and preparedness in utilities located in specific states, and the conclusions drawn are *not* necessarily representative of the state where the utilities are located. The appendix includes a description of the responses collected in each of the categories.

# 4 Implications for States

The following are some of the State implications of the findings.

- The data presented in this report suggests that utilities interact the most with National Associations, including the National Rural Electric Cooperative Association (NRECA), the American Public Power Association (APPA), Edison Electric Institute (EEI) and Fusion Centers, and that to some extent state-level agencies have monitored security planning, implementation and performance. Others have reported that role in state-level agencies. For instance, The Bipartisan Policy Center documented: "The New York Public Service Commission's Office of Utility Security monitors utility security planning, implementation, and performance […]. Generally, the commission uses existing NERC CIP standards as benchmarks for adequacy of utility cybersecurity measures"[3] (Bipartisan Policy Center 2014). The tendency of utilities relying more on national level associations versus state-level agencies might encourage states to identify how these national-level interactions originate and are sustained, and replicate some of the practices at state level. The diversity of national-level associations mentioned might also suggest a lack of understanding of the number and scope of cybersecurity support programs at national level, highlighting the need to inform utilities of the role of each agency, and how their cybersecurity agenda complements with each other.

- The responses collected suggest that utilities perceive that actions such as conducting risk assessments for cybersecurity plans and following best practices are efforts that go beyond established regulations. As such, agencies at state or local level can benefit by better understanding how these actions are defined and implemented, and can leverage the experience of "more advanced" utilities to provide guidance broadly across the state or region. In particular, state-level agencies can encourage information sharing across utilities –mainly regarding risk assessments and implementation of best practices. Information can be shared through different channels, such as meetings, briefings or workshops. , The National Regulatory Research Institute has reported that PUC's of some of the states included in this study –mainly, Alaska, Kentucky and South Carolina, have held meetings and briefings with their regulated utilities to address cybersecurity challenges (Phelan 2014). The data collected in this report suggests the need to include not only cybersecurity challenges, but also risk assessment plans and best practices. Due to the nature of the information, PUCs might identify the best ways to encourage and enable sharing across utilities.

- Although most of the participant utilities reported that the cybersecurity expenses were recovered through a base rate mechanism, one of the main challenges listed was a limited budget. State-level agencies might:

    1. Clearly identify how to account the costs and the benefits of cybersecurity expenses. To do so, they might encourage a risk-based cybersecurity framework,

[3] The Bipartisan Policy Center has documented as well that some PUC's have rules on compliance of cybersecurity standards on advanced metering infrastructure, initiation of audits and requirements of establishment of reliability plans.

under which cybersecurity expenses can be accounted as investments that mitigate costly cyber threats and successful cyber attacks.

2. Provide clear guidance on how to recover individual utility investments that benefit other utilities in- and out-of-state.

- Given that the data suggests lack of cohesive use of cybersecurity guidelines, states can promote training to identify and clarify publicly available standards and guidance. As well, state agencies can hold workshops on cybersecurity strategies and the cost and benefits of choosing one over other. Since Defense in Depth and Defense in Breadth were simultaneously chosen by some of the participant utilities, cybersecurity strategies can be highlighted not only individually, but also as a set of measures addressing a broader strategy.

Because the posture of the utilities was reactive, i.e. cybersecurity priorities were established as a reactive measure to specific cybersecurity threats, it might be important for state agencies to highlight the benefits of an alternative risk-based approach. Since pilot programs were popular among the participant utilities, these can be used to include exercises that serve as means of comparing potential consequences if utilities follow a reactive versus a risk-based approach.

# 5 Conclusions

State and local entities that oversee the reliable, affordable provision of electricity are faced with growing and evolving threats from cybersecurity risks to our nation's electric distribution system. All-hazards system resilience is a shared responsibility among the electric utilities and the state and local regulators. Within this responsibility, cybersecurity presents a new challenge for which utilities are implementing resilience measures and seeking cost recovery. Cybersecurity is accordingly a primary focus for states, local governments, and Native American tribes that are developing energy-assurance plans to protect the IT systems of their critical infrastructures.

This study compiled the policy approaches that facilitate cybersecurity preparedness from 22 utilities. It highlights the mechanisms that the participating utilities are using to address cybersecurity threats. Understanding the mechanisms that nonfederally-regulated utilities are implementing to prevent, respond to, and recover from cyber risks is important to draw a baseline of the current cybersecurity maturity level of the distribution power subsector.

The main findings suggest that having a cybersecurity policy is not necessarily the first step toward addressing cybersecurity; instead, utilities that did not report having a cybersecurity plan in place did report having other cybersecurity efforts, such as developing pilot programs and developing strategies to implement cybersecurity practices or budgeting efforts, and thus these efforts can be considered the first steps toward a cybersecurity strategy. Although many utilities do not have a cybersecurity policy in place, many utilities reported conducting risk assessments for their cybersecurity plans or following best practices. They perceive these efforts as actions beyond those required by federal, state, and local regulators. In addition, more than half of the utilities have already conducted cybersecurity assessments or audits on information or control systems.

In terms of guidance, the utilities are using a broad number of documents. On the surface, the use of these numerous guidelines would imply a certain level of maturity, but the diversity of these guidelines, the reported lack of a formal cybersecurity policy, and the reactive approach to establish cybersecurity strategies might suggest no cohesive use of these guidelines. Further, it seems that most utilities choose one or two of the known guidelines, but the reason to select one instead of another is not clear. As such, there is a need for a wider understanding of the use and applicability of each guideline and the implications for the design of formal cybersecurity policies. For instance, workshops offering training on using the guidelines in which organizations at the state, county, and city level participate are key to promote cohesive approaches.

Utilities interact mostly with national associations to improve their cybersecurity posture. The data collected suggest that the boards of municipalities and cooperatives are not strongly involved in cybersecurity actions.

Most utilities use network segmentation as a cybersecurity strategy. In addition, most utilities reported some type of adaptation to and learning from past cybersecurity incidents. Even those that did not report having been hit by a cyber attack during the last year reported establishing forensic investigations or upgrading or replacing software and sponsoring staff training.

# References

Bipartisan Policy Center. 2014. "Cybersecurity Electric Grid and the North American Electric Grid." Bipartisan Policy Center. http://bipartisanpolicy.org/wp-content/uploads/sites/default/files/Cybersecurity%20Electric%20Grid%20BPC.pdf.

California Public Utilities Commission. 2012. Cybersecurity and the Evolving Role of State Regulation: How It Impacts the California Public Utilities Commission. (Technical Report.) San Francisco, CA. Accessed December 2, 2015. http://www.cpuc.ca.gov/uploadedfiles/cpuc_public_website/content/about_us/organization/divisions/policy_and_planning/ppd_work/pre_2013_ppd_work/theevolvingroleofstateregulationincybersecurity9252012final.pdf.

DOE. 2014. "Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)." http://energy.gov/oe/cybersecurity-capability-maturity-model-c2m2-program/electricity-subsector-cybersecurity.

Office of Energy Policy and Systems Analysis. 2015. Quadrennial Energy Review: Energy Transmission, Storage, and Distribution Infrastructure. (Technical Report.) Washington, D.C.: U.S. Department of Energy. http://energy.gov/sites/prod/files/2015/07/f24/QER%20Full%20Report_TS%26D%20April%202015_0.pdf.

Keogh, Miles, and Christina Cody. 2014. Cybersecurity for State Regulators 2.0 with Sample Questions for Regulators to Ask Utilities. (Technical Report.) Washington, D.C.: National Association of Regulatory Utility Commissioners. http://energy.gov/sites/prod/files/NARUC%20Cybersecurity%20for%20State%20Regulators%20Primer%20-%20June%202012.pdf.

National Association of Regulatory Utility Commissioners. 2010. Resolution Regarding Cybersecurity. (Technical Report.) http://pubs.naruc.org/pub/5398456D-2354-D714-512A-F90E1B1A3268.

NIST. 2014. Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, National Institute of Standards and Technology. (Technical Report). Gaithersburg, MD. http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

National Rural Electric Cooperative Association. 2016. "The National Rural Electric Cooperative Association (NRECA)." Accessed April 15, 2016. http://www.nreca.coop/.

Phelan, Daniel. 2014. "A Summary of State Regulators' Responsibilities Regarding Cybersecurity Issues." National Regulatory Research Institute. http://www.energycollection.us/Companies/NRRI/Summary-State-Regulators.pdf.

Phelan, Daniel. 2015. "Cybersecurity Challenges for State Utility Regulators." EnergyBiz April. http://www.energybiz.com/magazine/article/404853/cybersecurity-challenges-state-utility-regulators.

The White House. 2013. Executive Order 13636—Improving Critical Infrastructure Cybersecurity. February 12. https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

The White House. 2013. Presidential Policy Directive—Critical Infrastructure Security and Resilience. February 12. https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

# Appendix

## Questionnaire

The utilities were contacted by email or phone. In total, more than 250 utilities were contacted, of which 22 agreed to participate. Initially, the questionnaire consisted of 80 questions. After further refinement, the final questionnaire consisted of the following 33 questions divided into 6 sections.

### *1. Demographics*

1. In which U.S. state is your utility headquartered?
2. What is your utility type?
    A. Municipal
    B. Cooperative
    C. Investor-owned
3. What is your total number of electric meters?
    A. <25,000
    B. 25,000–50,000
    C. 50,000–100,000
    D. 100,000–250,000
    E. >250,000
4. How many employees do you have?
    A. <10
    B. 11–50
    C. 51–100
    D. 100–500
    E. >500
5. How many people are on your cybersecurity team?
    A. 1
    B. 2–5
    C. 6–10
    D. 11–20
    E. >20
6. What is the total annual budget for all IT?
    A. <$50,000
    B. $50,000–100,000

C. $100,001–250,000

D. $250,001–500,000

E. $500,001–1,000,000

F. >$1,000,000

7. What is your annual budget for cybersecurity?

   A. <$10,000

   B. $10,000–25,000

   C. $25,001–100,000

   D. $100,001–250,000

   E. $250,001–500,000

   F. >$500,000

   G. N/A (No formal cybersecurity budget is established.)

### 2. Standards and Governance

1. What cost-recovery mechanism is used to address your cybersecurity spending? (Select all that apply.)

   A. Base rate

   B. Adjustment clauses

   C. Closed proceedings

   D. Deferral accounts

   E. Security recovery factor (or similar)

   F. Other (Please specify.)

2. What is the status of your cybersecurity effort? (Select all that apply.)

   A. We have an internally approved cybersecurity policy or governing document.

   B. We have a strategy for implementing our policy or governing document.

   C. We have an approved budget for cybersecurity efforts.

   D. We are deploying cybersecurity pilot programs.

   E. We have a fully implemented cybersecurity program.

3. Does your utility handle cybersecurity efforts in-house, or do you outsource this work to one or more third parties?

   A. In-house

   B. Outsourced

   C. Combination

   D. N/A

4. Is the cybersecurity policy at your utility audited?
    A. Yes—audited internally
    B. Yes—audited externally by an outside party
    C. Yes—audited by a combination of internal and external resources
    D. No
    E. N/A (We have no cybersecurity policy.)
5. If your cybersecurity policy is audited, how often?
    A. More than once per year
    B. Every 1–2 years
    C. Less frequently than once every two years
    D. N/A (We have no cybersecurity policy.)
6. What collaborative organizations or efforts have your utility interacted with or become involved with to improve its cybersecurity posture? (Select all that apply.)
    A. National association (National Rural Electric Cooperative Association, American Public Power Association, Edison Electric Institute, or other)
    B. Statewide association of distribution utilities
    C. InfraGard
    D. One or more fusion centers
    E. Other organizations or efforts (Please specify.)
7. What are the primary challenges to your cybersecurity efforts? (Select all that apply.)
    A. Lack of support from utility board
    B. Lack of support from utility executives
    C. Budget
    D. Technology availability and maturity
    E. Legacy systems (installed equipment basis)
    F. Lack of standards
    G. Regulatory model—investment recovery issues
    H. Regulatory model—performance standards and requirements
    I. Lack of skilled workforce
    J. Other (Please specify.)
8. What governing principles, protocols, and/or standards does your utility use for cybersecurity guidance? (Select all that apply.)
    A. NISTIR 7628

B. NIST Cybersecurity Framework (v1)

C. DOE's ES-C2M2

D. DOE's RMP

E. N/A (We do not use any of these.)

F. Other (Please specify.)

9. What is the job title of the person at the executive level within your utility who has explicit responsibility for organization-wide cybersecurity efforts (i.e., they oversee all cybersecurity efforts and have responsibility for the success of those efforts)?

    A. Chief Security Officer (CSO)

    B. Chief Information Security Officer (CISO)

    C. Chief Information Officer (CIO)

    D. N/A (No such position exists at our utility.)

    E. Other (Please specifys)

10. Are IT and OT cybersecurity efforts handled by the same people within your organization?

    A. No—IT and OT cybersecurity handled by different people.

    B. Yes

    C. N/A

### *3. Oversight*

1. At the state level, what has your public utilities commission, public service commission, or equivalent agency done in regard to cybersecurity? (Select all that apply.)

    A. Imposed regulation on distribution utilities in the state

    B. Monitored utility security planning, implementation, and performance of technical developments related to cybersecurity

    C. Tested utility cybersecurity plans through cyber-attack exercises

    D. Established a program to provide support during emergencies related to cyber events and encouraged utilities to participate in voluntary standards developments

    E. Established cyber-event reporting requirements for utilities

    F. Mandated self-certified compliance with specific guidelines, standards, or policies

    G. Encouraged distribution utilities in the state to collaborate on developing a statewide voluntary program to improve cybersecurity

    H. Encouraged distribution utilities in the state to work individually to improve cybersecurity or offered training or workshops to improve cybersecurity

    I. Other (Please specify.)

2. At the local level, what has your county and city government done in regard to cybersecurity? (Select all that apply.)
    A. Imposed regulation on distribution utilities in the state
    B. Monitored utility security planning, implementation, and performance of technical developments related to cybersecurity
    C. Tested utility cybersecurity plans through cyber-attack exercises
    D. Established a program to provide support during emergencies related to cyber events and encouraged utilities to participate in voluntary standards developments
    E. Established cyber-event reporting requirements for utilities
    F. Mandated self-certified compliance with specific guidelines, standards, or policies
    G. Encouraged distribution utilities in the state to collaborate on developing a statewide voluntary program to improve cybersecurity
    H. Encouraged distribution utilities in the state to work individually to improve cybersecurity or offered training or workshops to improve cybersecurity
    I. Other (Please specify.)
3. Does your utility's cybersecurity efforts go beyond those required by federal, state, and local regulators?
    A. Yes—we conduct a risk assessment and design our cybersecurity program accordingly.
    B. Yes—we follow industry best practices and guidelines to determine the right program for our utility.
    C. No—we do not go beyond requirements by regulators.
    D. N/A
    E. Other (Please specify.)
4. What reporting occurs in the event of an attempted cybersecurity breach, successful or not? (Select all that apply.)
    A. We report to our board of directors.
    B. We report to our city councils.
    C. We report to our state public utilities commission.
    D. We report to the FBI.
    E. We report to DHS.
    F. Other (Please specify.)

### *4. Planning*

1. How is your security plan structured?
    A. Our cybersecurity plan contains both cybersecurity and physical security components.

B. Our physical security plan identifies critical cyber assets.

C. N/A

D. Other (Please identify.)

2. Has business process (enterprise) cybersecurity been included in the continuity of operations plans for areas such as customer data, billing, etc.?

   A. Yes

   B. No

3. Has your utility conducted a cybersecurity audit or assessment of any of the following? (Select all that apply.)

   A. Information systems

   B. Control systems

   C. Other networked systems (Please specify.)

4. How do you determine which systems, components, and functions get priority in regard to implementing new cybersecurity measures? (Select all that apply.)

   A. A system with known vulnerabilities becomes a priority for upgrade and replacement.

   B. Software packages become a priority for upgrade when a new version is released.

   C. A system that is compromised during a penetration test becomes a priority for upgrade and replacement.

   D. A system that is compromised during a cyber attack becomes a priority for upgrade and replacement.

   E. Other (Please specify.)

### *5. Execution and Performance*

1. During the last year, has your utility been hit by any form of cyber attack?

   A. No

   B. Yes—a denial-of-service attack

   C. Yes—a ransomware attack

   D. Yes—an attack in which data was stolen from our system

   E. Yes—an attack in which hackers took control of physical devices in our system

   F. Yes—other (Please specify.)

2. Does your utility employ any of the following? (Select all that apply.)

   A. Defense in depth approach (layered defenses)

   B. Defense in breadth (complementary blended, overlapping)

   C. Zero-trust network

   D. Network segmentation

E. Air gapping

F. Other?

3. How do you maintain situational awareness of system security? (Select all that apply.)
   A. Internal network monitoring
   B. Incident sharing throughout the organization
   C. Sharing threat information with others in the industry and government
   D. Understanding critical dependencies among systems
   E. Other (Please specify.)
4. Do you utilize outside testing to verify cybersecurity effectiveness and robustness to simulated exploitation (penetration testing)?
   A. Yes
   B. No
5. Are your cybersecurity efforts integrated among business systems and control systems?
   A. Yes
   B. No

### 6. Support

1. How are cybersecurity criteria used for vendor and device selection? (Select all that apply.)
   A. We question vendors during the request-for-proposal stage about how well they follow best practices for secure development.
   B. We depend on third-party evaluations of a vendor's cybersecurity.
   C. We examine reports of security breaches for signs that a vendor's products may not be secure.
   D. We depend on anecdotes from others in the industry.
   E. Other (Please specify.)
2. Does your organization perform vulnerability assessments as part of the acquisition cycle for products in each of the following areas? (Select all that apply.)
   A. Cybersecurity
   B. SCADA
   C. Smart grid
   D. Internet connectivity
   E. Website hosting
   F. Other (Please specify.)
3. How does your utility learn from and adapt to past cybersecurity incidents? (Select all that apply.)

A. We hire an outside firm to conduct a forensic investigation and make changes based on the mode of the attack.

B. We do our own forensic investigation and make changes based on the mode of the attack.

C. We upgrade or replace software systems that have been compromised.

D. We add staff training if the incident involves phishing attacks or social engineering.

E. Other (Please specify.)

## Demographics

The 22 participating utilities are headquartered in the following 14 states: Alaska, Alabama, California, Colorado, Florida, Kentucky, Louisiana, Mississippi, Montana, North Carolina, New Hampshire, Oklahoma, South Carolina, and Tennessee. The state most widely represented is Tennessee, with seven utilities; followed by California, with two utilities. All other states are represented by one utility. The majority of participating utilities are cooperatives (12), followed by municipalities (7). Only three investor-owned utilities participated.

Of the 22 utilities, 11 are under Tennessee Valley Authority (TVA) jurisdiction, all of which are nonfederally regulated. In addition, of the 22 utilities, 3 are partially or completely compliant with the North American Electric Reliability Council (NERC). In particular, one investor-owned utility (IOU) is NERC compliant for a share of its assets, and one IOU and one municipality are fully NERC compliant. All cooperatives are nonfederally regulated.

Because TVA is an agency of the federal government, the Supremacy Clause of the U.S. Constitution preempts traditional state regulation of the cooperative and municipal utilities that purchase their power from TVA.[4] Thus, utilities under TVA jurisdiction are not subject to state-level regulations, and their responses are not necessarily aligned with state-level regulation. Table 2 summarizes the types and sizes of the participating utilities.

**Table 2. Basic Description of Utilities**

| State | No. of Utilities | Type of Utility[a] | Size of Utility (No. of Meters)[b] | NERC Compliant?[c] | TVA Jurisdiction?[c] |
|---|---|---|---|---|---|
| AK | 1 | 1 | Small | No | No |
| AL | 2 | 1,2 | Small, large | No | Yes |
| CA | 2 | 2,3 | Very large | Yes | No |
| CO | 1 | 1 | Small | No | No |
| FL | 1 | 1 | Large | No | No |
| KY | 1 | 2 | Very small | No | Yes |
| LA | 1 | 1 | Small | No | No |
| MS | 1 | 2 | Very small | No | Yes |
| MT | 1 | 1 | Very small | No | No |
| NC | 1 | 1 | Very small | No | No |
| NH | 1 | 3 | Medium | Yes | No |
| OK | 1 | 3 | Small | No | No |
| SC | 1 | 1 | Medium | No | No |
| TN | 7 | 1,2 | Very small, small, large | No | Yes |

[a] Type of utility—1: cooperative; 2: municipal; 3: investor owned

[4] The Tennessee Valley Authority Act of 1933 established that TVA Board is authorized to provide for rules and regulations. See https://www.tva.gov/file_source/TVA/Site%20Content/About%20TVA/TVA_Act.pdf.

[b] Size of utility (m)—<25,000: very small; 25,000–50,000: small; 50,000–100,000: medium; 100,000–250,000: large; >250,000: very large
[c] Columns added by the authors. These questions were not part of the questionnaire.

All utilities have a cybersecurity team, four of which consist of only one person. The majority of the cybersecurity teams include at most five people. Only one utility (an IOU, NERC compliant) has a cybersecurity team of more than 20 people. Table 3. shows the relationship between the cybersecurity team and the utility's total number of employees. In some cases, the ratio of the size of the cybersecurity team compared to the size of the utility is larger for smaller utilities. For instance, utilities that have less than 50 employees have at most cybersecurity teams of 5 people, representing at most 10% of the company. On the other hand, large utilities that have more than 500 employees have cybersecurity teams of at most 20 people, representing less than 5% of the company. Nevertheless, there are other cases in which large utilities have a higher ratio than smaller utilities. For example, one utility with 101–500 employees reported having 11–20 employees on its cybersecurity team, meaning that 2%– 20% of the workforce is devoted to cybersecurity. Another utility of 51–100 employees reported a cybersecurity team of 6–10 employees, representing 6%–20% of the workforce.

**Table 3. Number of Employees on Cybersecurity Team by Utility Size**

| | No. of Employees on Cybersecurity Team | | | | |
|---|---|---|---|---|---|
| **Total No. of Employees** | **1** | **2–5** | **6–10** | **11–20** | **>20** |
| <10 | 0 | 0 | 0 | 0 | 0 |
| 11–50 | 1 | 5 | 0 | 0 | 0 |
| 51–100 | 1 | 2 | 1 | 0 | 0 |
| 101–500 | 2 | 5 | 1 | 1 | 0 |
| >500 | 0 | 1 | 0 | 1 | 1 |

In terms of budget, four cooperatives reported having no formal cybersecurity budget established. The other cooperatives reported an annual cybersecurity budget of less than $100,000.[5] Municipalities (nonfederally regulated) had a slightly higher budget than cooperatives: one up to $250,000 and one of more than $500,000.

Interestingly, having a higher information technology (IT) budget does not necessarily imply a higher cybersecurity budget. For example, two utilities (nonfederally regulated) with annual IT budgets of more than $1,000,000 reported cybersecurity budgets of less than $100,000 and less than $25,000. On the other hand, a higher cybersecurity budget was consistent with a higher IT budget. The cooperatives that have higher cybersecurity budgets (up to $100,000) have IT budgets between $250,000 and more than $1,000,000, and the cooperative that has the lowest cybersecurity budget (less than $10,000) did not report its IT budget.

[5] One cooperative reported not knowing the information (labeled "Not sure" in Figure 2).

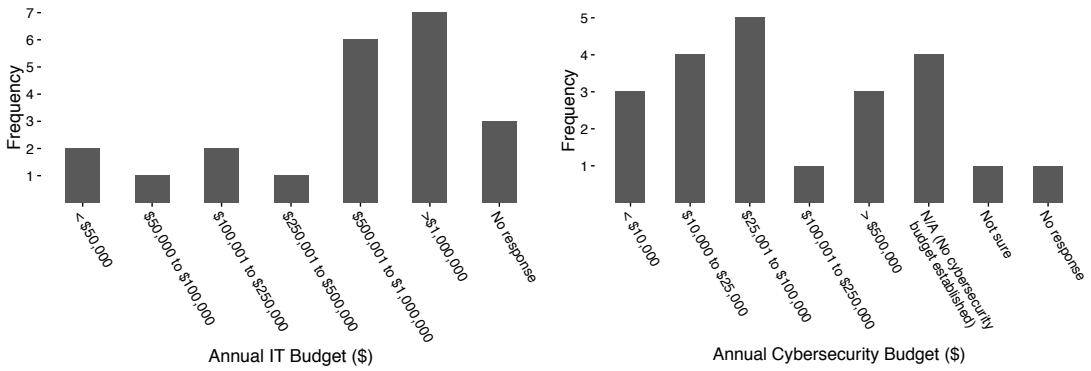


**Figure 2. Annual IT and annual cybersecurity budgets in participating utilities**

## Standards and Governance

State regulators are in charge of regulating the cybersecurity of electric distribution systems. In 2010, the National Association of Regulatory Utility Commissions (NARUC) published its resolution regarding cybersecurity in which it encouraged "commissions to make efforts to give the highest priority to ensure that cybersecurity will be consistently monitored and evaluated to remain effective to meet ongoing threats to the utility systems" and to "revisit their own cybersecurity policies and procedures to ensure they are in compliance with applicable standards and best practices" (NARUC 2010). Later on, in 2013 and 2014, NARUC published its guidelines on cybersecurity for state regulators (Keogh and Cody 2014). All states can use these guidelines to have an open dialogue with their regulated utilities. Some states have been particularly proactive in defining cybersecurity measures, such as California (California Public Utilities Commission 2015), and different approaches have been implemented across the country.

This section highlights the different approaches taken by utilities to fund and implement cybersecurity efforts as well as the challenges they have faced. It also points to the organizations with which utilities interact to improve their cybersecurity posture, including federal and state agencies.

### *Cost-Recovery Mechanisms*

Three cooperatives reported no formal cost-recovery mechanism for cybersecurity, but one highlighted using a base rate as the recovery mechanism for all IT. Figure 3 shows the different recovery mechanisms reported.

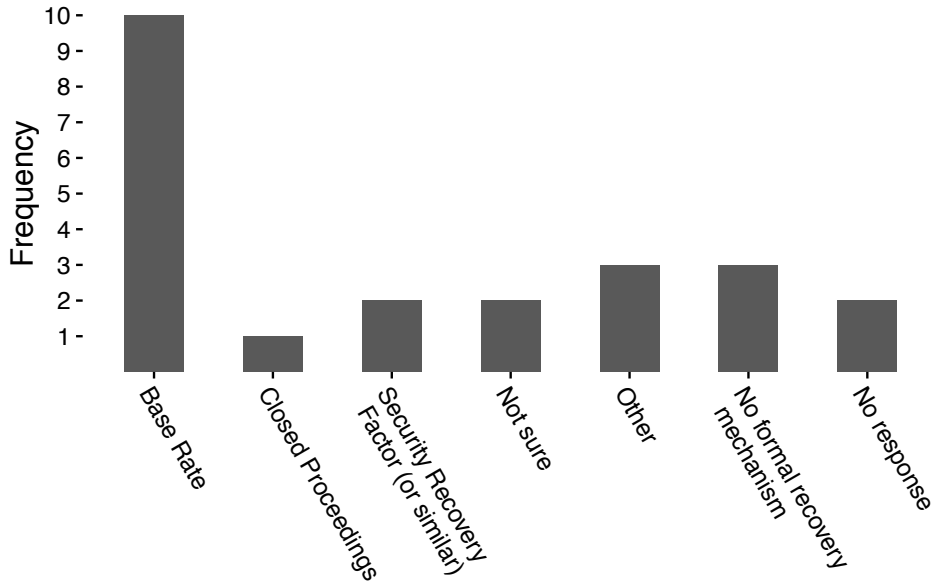


**Figure 3. Cost-recovery mechanisms for cybersecurity spending**

"Base rate" is the most popular mechanism for recovering cybersecurity expenses: it was selected by 10 of the 22 utilities, and 8 of the 19 non-NERC utilities. "Adjustment clauses" and "deferral accounts" were not chosen, and "closed proceedings" and "security recovery factor" were chosen only by one and two non federally-regulated utilities, respectively. Non federally-regulated utilities that chose "other" indicated that they were "folded into operations." NERC-compliant utilities reported "Base rate" or "other" as their recovery mechanism, including in "other" the following: "general rate case" and "Federal Energy Regulatory Commission recovery mechanism plus operating budget plus state recovery."

### *Status of Cybersecurity Efforts*

This question addressed non mutually exclusive cybersecurity efforts. The list of options was presented in ascending order, suggesting that later options represented higher levels of cybersecurity maturity. For utilities that have established efforts, the status is diverse, but the majority of utilities reported having at least two efforts in place. In particular, of the five efforts included in the questionnaire, "internally approved cybersecurity policy or governing document"[6] and "implementation strategy" were the most popular, which can represent first steps toward cybersecurity preparedness. In addition, having a "fully implemented cybersecurity program" was the least popular effort, selected by one cooperative and two municipalities, which suggests that the majority of the respondents are in the earlier stages of cybersecurity preparedness. Table 4 shows how these responses can be mapped to a qualitative scale, and it summarizes the number of efforts selected by non-NERC and NERC-compliant utilities. One nonfederally-regulated cooperative reported having the five efforts in place, including a "fully implemented cybersecurity program."

[6] Note that the questionnaire did not specify criteria to determine what a cybersecurity policy considers; thus, choosing this alternative was left to the respondent's interpretation.

**Table 4. Status of Cybersecurity Efforts**

| Maturity Level (Qualitative Mapping)[a] | Effort | No. of Nonfederally-Regulated Utilities (% of Group) | No. of NERC-Compliant Utilities (% of Group) |
|---|---|---|---|
| 0 | No effort in place | 1 (5%) | 0 |
| 1 | 1. Internally approved cybersecurity policy | 9 (47%) | 3 (100%) |
| 1 | 2. Implementation strategy | 10 (52%) | 1 (33%) |
| 2 | 3. Approved budget for cybersecurity efforts | 7 (37%) | 3 (100%) |
| 3 | 4. Cybersecurity pilot programs | 6 (32%) | 2 (67%) |
| 4 | 5. Fully implemented[b] cybersecurity program | 3 (16%) | 1 (33%) |
| - | Other effort | 1 (5%)[c] | 1 (5%) |
| - | No response | 4 (20%) | 0 |

[a] The number 0 represents the least mature, and the number 4 represents the most mature.
[b] None of the terms, e.g., *fully implemented*, were explicitly defined in the report.
[c] This was selected by a cooperative; it reported the following: "Some policies in place but mostly supported through a consultant company." This utility also reported outsourcing its cybersecurity efforts.

### Efforts In-House or Outsourced

The most common alternative was a combination of in-house and outsourced cybersecurity resources. Understanding if the cybersecurity efforts are performed using in-house or outsourced resources highlights the cybergovernance policy and architecture. Either approach, or a combination, is ***strategy***. Do the corporate policies and accountability framework ensure implementation of the strategy (e.g. , supply chain and external dependency management)? Outsourcing cybersecurity efforts was not popular: only one municipality and one cooperative reported this option. Of the four utilities that did not respond to the previous question on the status of cybersecurity efforts, only one did not respond regarding whether the efforts are outsourced or managed in-house. Interestingly, the other three utilities that did not respond regarding which efforts were in place reported having in-house and outsourced efforts, which suggests a lack of information availability on specific efforts but available information on the overall types—in-house or outsourced.

### Cybersecurity Policy Audit

Half of the cooperatives reported having a cybersecurity policy in place. Of the other 50%, one cooperative reported a cybersecurity policy "in progress." Interestingly, of the five cooperatives that reported not having a cybersecurity policy, three reported having at least one effort in place, one of which responded to having "an internally approved cybersecurity policy or governing document." This might mean that although there is no cybersecurity policy in place, there is a governing document that addresses cybersecurity. The other two cooperatives that have no cybersecurity policy but do have cybersecurity efforts in place reported having an "established

cybersecurity budget" and a "cybersecurity pilot"; and a "strategy to implement the policy," an "established budget," and a "cybersecurity pilot." The cooperative that reported having a cybersecurity policy in progress (but no cybersecurity policy in place) also reported having four of the five listed efforts in place.

These responses suggest that having a cybersecurity policy is not necessarily the first step toward addressing cybersecurity; rather, different efforts, such as budgeting, piloting programs, and setting strategies to implement cybersecurity practices can be the first initiatives toward cybersecurity. Similarly, it can suggest that policies are defined as experience is gained through practice. In addition, the fact that cybersecurity efforts are in place in utilities that have no formal cybersecurity policy might indicate that a cybersecurity framework has not been identified across business processes or that the efforts are disaggregated, not standardized or volatile. Table 5 summarizes these findings for nonfederally-regulated utilities by type of utility.

**Table 5. Cybersecurity Policy and Audit of Participating Non-NERC Utilities**

| Type of Utility | Status |
|---|---|
| Cooperatives | • One has a cybersecurity policy but no cybersecurity audit. Two efforts are in place.<br>• Five cooperatives have both a cybersecurity policy (one with a policy in progress) and an audit. At least one effort is in place.<br>• Six cooperatives do not have a cybersecurity policy. One did not report any effort, and one reported "other: working toward a cybersecurity program." Four have at least one effort in place. |
| Municipalities | • Four municipalities have both a cybersecurity policy and an audit, one of which did not report any effort in place.<br>• One municipality does not have a cybersecurity policy. No efforts were reported.<br>• One municipality did not respond. No efforts were reported. |
| IOUs | • One IOU has both a cybersecurity policy and an audit. Three efforts are in place. |

Most utilities that perform an audit on their cybersecurity policy do so every 1–2 years. Only two utilities perform an audit more often, more than once per year. Of the 10 non federally-regulated utilities that responded to having a cybersecurity policy audit in place, two perform an audit more than once per year and six perform an audit every 1–2 years. Only one cooperative reported performing an audit with a frequency of less than 2 years. In addition, from the 10 non-NERC utilities that audit their cybersecurity policies, only 3 perform an internal audit; the other 7 have their cybersecurity audits provided by an outside party or by a combination of internal and external resources.

### *Collaborative Organizations or Efforts*

Of the 19 nonfederally regulated utilities, 14 have interacted with at least one collaborative organization or effort to improve their cybersecurity posture. In particular, nine utilities have collaborate with national associations (including the National Rural Electric Cooperative

Association, American Public Power Association, Edison Electric Institute, or other), and six collaborate with state associations of distribution utilities. In addition, five nonfederally-regulated utilities have interacted with InfraGard. Besides interacting with the listed national and statewide associations, InfraGard, and fusion centers, non-NERC utilities reported collaborating with multiple organizations, including the Utilities Telecom Council, National Information Solutions Cooperative, Utility Technology Association, Information Sharing and Analysis Centers (ISAC), regional public power associations, Critical Infrastructure Communications Coalition, and regional trade associations. NERC-compliant utilities mentioned having interacted with collaborative efforts from NERC, the Federal Energy Regulatory Commission, Electric Power Research Institute, Center for Internet Security, Electricity Information Sharing and Analysis Center, Critical Infrastructure Communications Coalition, National Institute of Standards and Technology (NIST), and the Large Public Power Council. One utility mentioned its intention to join the Center for Research in Implementation Science and Prevention.

### *Primary Challenges*

Utilities reported various primary challenges to their cybersecurity efforts. The most cited by non federally-regulated utilities was legacy systems (installed equipment basis) (cited by six utilities), followed by budget (five utilities), skilled force (five utilities), and technology availability and maturity (four utilities). One cooperative reported not "seeing any issues [i.e., challenges] as there has not [been] any breaches yet."

Other challenges mentioned were "leaders have prioritized other work," "security is hard to prioritize within IT," [the] way it is structured is difficult; people in charge of IT do not have security background," "time constraints," and "lack of engagement from board and executives."

In general, co-ops reported the most diverse set of challenges. IOUs and municipalities reported a less diverse set. For example, IOUs and municipalities did not select a lack of support from utility boards or a lack of support from utility executives.

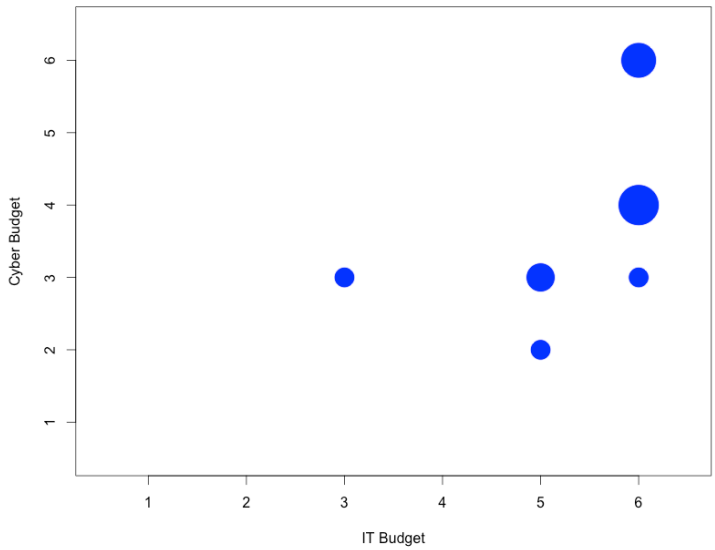


**Figure 4. Number of cybersecurity challenges reported by range of cyber budget and IT budget. Scale from 1–6 corresponds to the levels of the questionnaire. Utilities that have relative higher IT or cyber budgets identified more cybersecurity challenges.**

Note that Figure 4 includes only the eight utilities that responded to the three questions on cyber budget, IT budget, and cybersecurity challenges. This graph shows the relationship between the number of cybersecurity challenges faced and the IT and cyber budgets. It shows that the utilities that have relatively higher IT or cybersecurity budgets identify more cybersecurity challenges, which may suggest a more sophisticated perspective on their cybersecurity.

### *Governing Principles*

Utilities reported using various principles, protocols, and standards for cybersecurity guidance. The three NERC-compliant utilities mentioned NIST's Cybersecurity Framework as a common guiding document. In addition, two of the three mentioned using DOE's ES-C2M2 and the NIST Internal/Interagency Report (NISTIR) 7628. Of the nonfederally-regulated utilities, four utilities reported not using any of these guidelines. Five utilities (three cooperatives and two municipalities) use NIST's Cybersecurity Framework (v1), two use NISTIR 7628, one uses DOE's ES-C2M2, and one uses DOE's Risk Management Process (RMP) guideline. These are not exclusive. For example, one nonfederally-regulated municipality uses NISTIR 7628, NIST's Cybersecurity Framework (v1), and DOE's RMP guideline. Utilities reported using other guidance as well: non-NERC utilities mentioned the International Organization for Standardization (ISO) 20071, ISO 27002, and NERC's CIP; and NERC-compliant utilities mentioned ISO 11000, the PCI Security Standards Council, state privacy laws, and ISO 20071. The sole nonfederally-regulated utility that mentioned using NERC's CIP as a guideline reported that even though the utility is not subject to NERC's CIP, it "mirrors it just in case that changes."

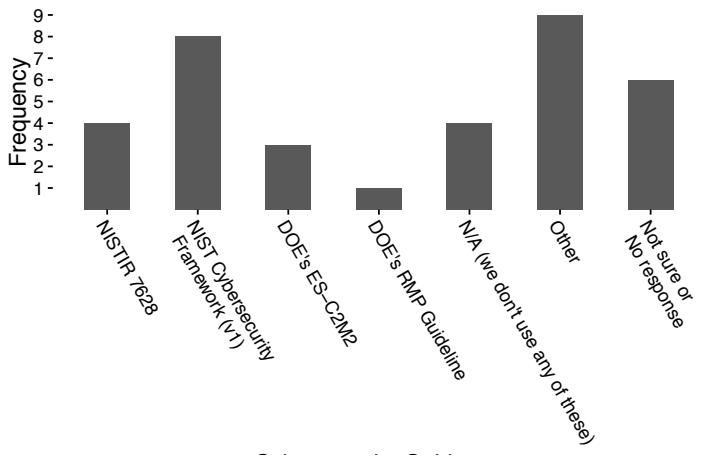


**Figure 5. Cybersecurity guiding principles**

Table 6 shows that nonfederally-regulated utilities that reported ranges of annual IT budgets more than $500,000–$1,000,000 use NIST or DOE cybersecurity guidelines.

**Table 6. Relationship between IT Budget and NIST and DOE Guiding Principles in Non-NERC Participating Utilities**

| IT Budget | NISTIR 7628 | NIST Frame-work | DOE ES-C2M2 | DOE Cyber-security RMP | Any | Other | Not Sure or No Response |
|---|---|---|---|---|---|---|---|
| <$50,000 | - | - | - | - | - | - | 2 |
| $50,000–$100,000 | - | - | - | - | - | - | 1 |
| $100,001–$250,000 | - | - | - | - | 1 | - | 1 |
| $250,001–$500,000 | - | - | - | - | - | 1 | - |
| $500,001–$1,000,000 | 1 | 2 | 1 | - | 3 | 2 | - |
| >$1,000,000 | 1 | 2 | - | 1 | - | 2 | 2 |
| No response | - | 1 | - | - | - | 2 | - |
| **Total** | 2 | 5 | 1 | 1 | 4 | 7 | 6 |

**Table 7. Relationship between Cybersecurity Budget and NIST and DOE Guiding Principles in Non-NERC Participating Utilities**

| Cybersecurity Budget | NISTIR 7628 | NIST Frame-work | DOE ES-C2M2 | DOE Cyber-security RMP | Any | Other | Not Sure or No Response |
|---|---|---|---|---|---|---|---|
| <$10,000 | - | 1 | - | - | - | 1 | 1 |
| $10,000–$25,000 | - | - | - | - | 1 | 1 | 3 |
| $25,001–$100,000 | 1 | 1 | 1 | - | 1 | 3 | 1 |
| $100,001–$250,000 | 1 | 1 | - | 1 | - | | - |
| >$500,000 | | 1 | | | | 1 | |
| No formal budget established | | 1 | | | 2 | 1 | |
| Not sure or response | - | | - | - | - | | 1 |
| **Total** | 2 | 5 | 1 | 1 | 4 | 7 | 6 |

Utilities that have larger IT budgets (more than $500,000) use the reports. This does not translate directly to the same conclusion when looking at cybersecurity budgets because of a lack of direct correlation between both.

### *Job Title*

The utilities reported a variety of job titles of the person at the executive level who has explicit responsibility for organization-wide cybersecurity efforts. The job titles reported are Chief Information Officer, Chief Information Security Officer, Chief Security Officer (CSO), Chief Financial Officer, Information Technology Manager, Telecommunications Manager, Vice President of IT, Assistant General Manager, Director of IT, Manager of IT, and Vice President of Engineering and Technical Services. Six of the nonfederally-regulated utilities reported not having this type of position at the utility, and other four did not respond to this question.

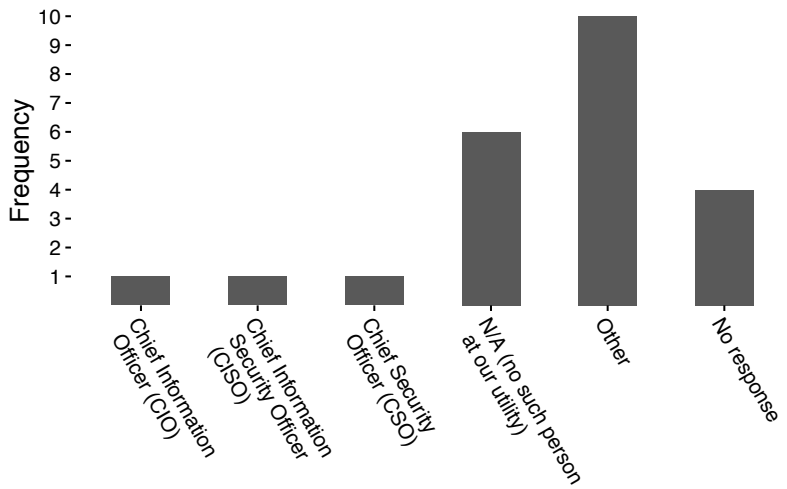


**Figure 6. Job titles of executives who lead cybersecurity efforts**

### *IT and OT Handled by the Same People*

Of the 19 nonfederally-regulated utilities, 8 cooperatives and 3 municipalities reported that IT and OT are managed by the same people, and 2 cooperatives and 1 municipality responded that the same people do not handle IT and OT. The two NERC-compliant IOU's reported having separate management for IT and OT. Four utilities did not respond to the question, or the question did not apply to them (N/A). Table 8 shows that all of the nonfederally-regulated utilities that have an annual IT budget less than $1,000,000 manage IT and OT together and that utilities that have higher IT annual budgets are split between a separate and a unified IT/OT management structure.

**Table 8. Relationship between IT Budget and IT and OT Handling in Non-NERC Participating Utilities**

| IT Budget | IT and OT Managed Together? Yes | IT and OT Managed Separately? No | N/A or No Response |
|---|---|---|---|
| <$50,000 | - | - | 2 |
| $50,000–$100,000 | - | - | 1 |
| $100,001–$250,000 | 1 | - | 1 |
| $250,001–$500,000 | 1 | - | - |
| $500,001–$1,000,000 | 6 | - | - |
| >$1,000,000 | 2 | 2 | 1 |
| No response | 1 | 1 | - |
| **Total** | 11 | 3 | 5 |

## Oversight

States and local regulators have oversight responsibility on cybersecurity. This section outlines their role in cybersecurity regulation of the participating utilities.

### *State and Local Cybersecurity Actions*

Of the 19 non-federally-regulated utilities, 8 did not respond regarding what their state public utilities commission, public service commission, or equivalent state-level agency had done for cybersecurity. The other 11 reported the following: the commission has encouraged distribution utilities to work individually to improve cybersecurity (4), the state-level agency has encouraged utilities to participate in voluntary standards development (2), it has encouraged distribution utilities to collaborate on developing a statewide voluntary program to improve cybersecurity (1), it has offered training or workshops to improve cybersecurity (1), that the state-level agency has done nothing regarding cybersecurity (2), and that they did not know (1).

The three NERC-compliant utilities identified the following commission actions: imposed regulation; monitored security planning, implementation, and performance; established cyber event-reporting requirements; encouraged distribution utilities to collaborate on developing a statewide voluntary program to improve cybersecurity; and encouraged distribution utilities to work individually to improve cybersecurity.

The following alternatives where not chosen by any utility: "monitored technical developments related to cybersecurity," "tested utility cybersecurity plans through cyber-attack exercises," and "established a program to provide support during emergencies related to cyber events."

Louisiana is the state with the most actions identified by a single respondent (three). Tennessee is represented by seven nonfederally-regulated utilities—three of which in sum identified three actions taken by the state-level (or equivalent) agency.[7] Interestingly, one cooperative in Tennessee responded that the state-level agency has done nothing. And one municipality in Tennessee did not respond to the question.

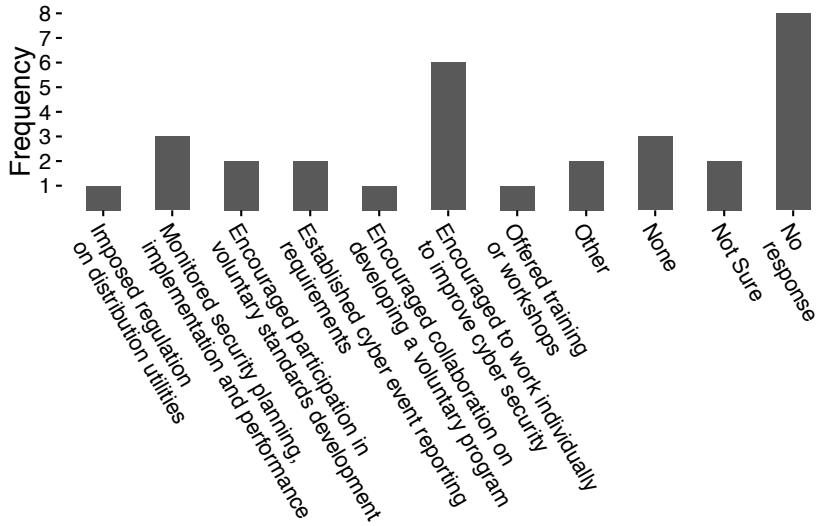


**Figure 7. State agency actions on cybersecurity according to participating utilities**

[7] In this case, these might be actions taken by TVA.

### *County and City Government Cybersecurity Actions*

Two of the three actions that were not identified at the state level were identified at the county and city level: "tested utility cybersecurity plans through cyber-attack exercises" and "established a program to provide support during emergencies related to cyber events." Actions not identified at the county or city level and identified at the state level include imposed regulation and established cyber-event reporting requirements. Thus, between state, county, or city regulations, all the actions were identified.

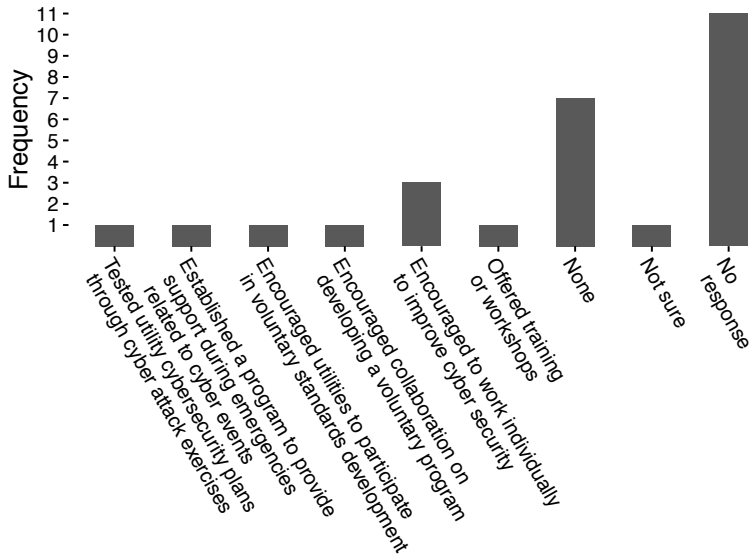


**Figure 8. County and city actions on cybersecurity according to participating utilities**

Given that both municipalities and cooperatives are owned by cities or influenced by county leadership, respectively, this graph suggests that municipalities' and cooperatives' boards are not strongly involved in cybersecurity actions.

### *Efforts beyond Requirements by Regulators*

Six nonfederally-regulated utilities did not respond to this question. Of those that responded, two utilities reported conducting a risk assessment and following industry best practices. Interestingly, one of these utilities did not report an IT or cybersecurity budget, and the other utility reported moderate budgets: an IT budget of $250,000–$500,000 and a cybersecurity budget of $25,000–$100,000. In total, six nonfederally-regulated utilities reported performing a risk assessment, and five reported following industry best practices. Only one utility, a cooperative, reported explicitly not going beyond regulator requirements.

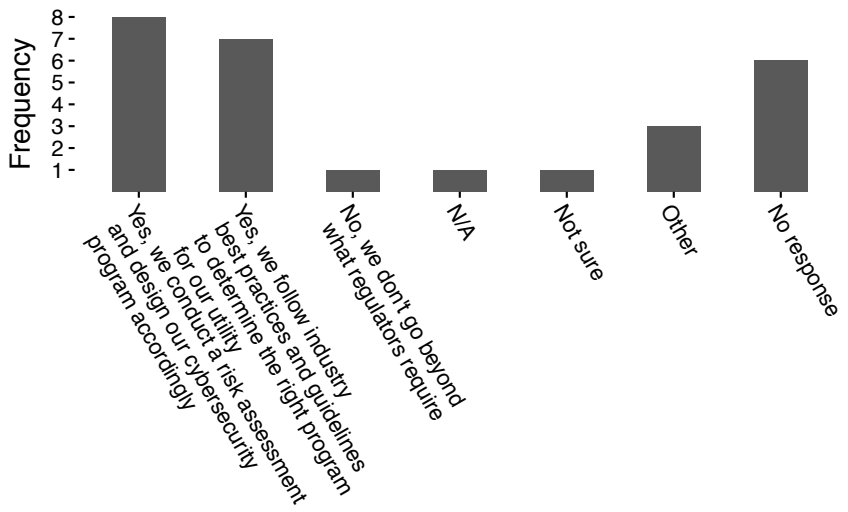


**Figure 9. Utility efforts beyond requirements by regulators**

### *Reporting Occurs in the Event of a Cybersecurity Breach*

The most common reporting mechanism is through the board of directors. Some utilities responded that they reported to the public utilities commission or the Federal Bureau of Investigation (FBI) but not to a board of directors. For boards of directors to review threats/risks and determine mitigating policies, it is incumbent on management to inform them of performance. This gap with some utilities seems to reflect a lack of engagement by some boards of directors in cybersecurity governance, and it supports other indications found in this research that raises this same concern.

Six utilities did not respond to this question. No utility answered, "We report to our city councils." Most utilities (nine of the nonfederally-regulated utilities) responded that they report only to the board of directors. Of these, a municipality with the largest IT budget also reports to the FBI and U.S. Department of Homeland Security (DHS), two cooperatives (one with the largest IT budget and another with no information on its budget) also report to DHS, and one cooperative also reports to the FBI. In total, four nonfederally regulated utilities report to the FBI, and three report to DHS. Of the three utilities that report to the public utilities commission, only one is nonfederally regulated—from Tennessee. Two nonfederally regulated utilities mentioned not having any breaches yet, and one mentioned "nothing," suggesting that no event has happened yet.

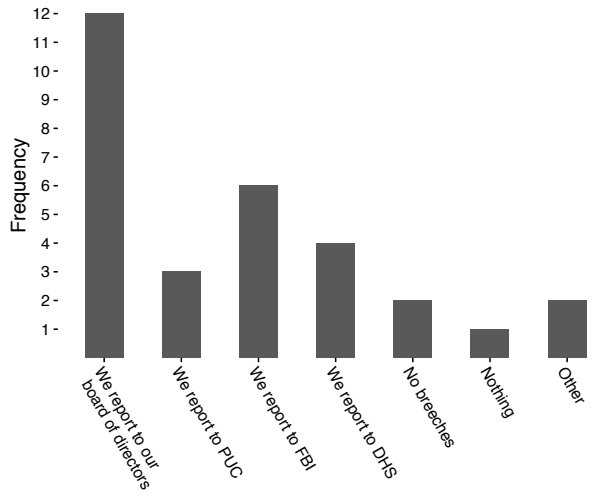


**Figure 10. Reporting attempted breaches according to participating utilities**

# Planning

## *Security Plan Structure*

NERC-compliant utilities reported N/A and "other" as the alternatives to the question on how their security plan is structured. Six nonfederally-regulated utilities did not respond. Eight reported having a security plan that contains both physical and cyber aspects, which is aligned with NERC's cybersecurity maturity framework. Only one utility reported having a security plan that identifies only critical cybersecurity assets.

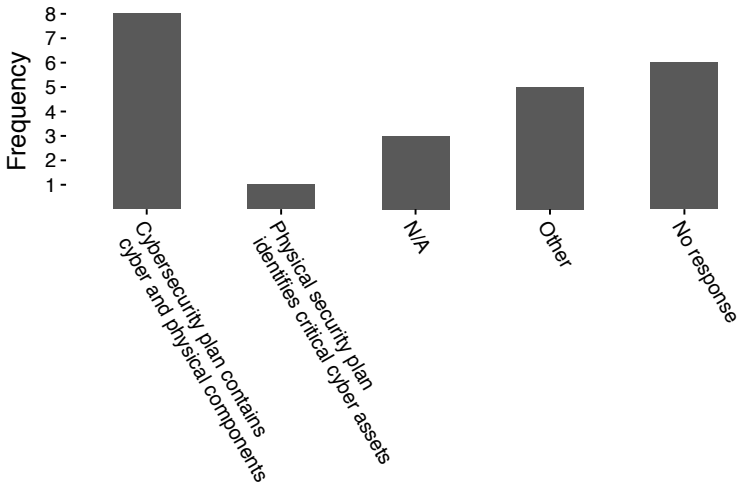


**Figure 11. Cybersecurity plan structure**

Of the 19 nonfederally-regulated utilities, 6 did not responded to the question about whether cybersecurity has been included in their continuity of operations plans for areas such as customer data and billing. Of the other 13, 12 responded "yes," and two responded "no." Of these 12, less than half (5 utilities) have an established cybersecurity policy in place, and one additional has a cybersecurity policy "in progress," suggesting that the inclusion of cybersecurity in operation plans does not depend on having a formal cybersecurity policy. The utilities that have both a

cybersecurity policy in hand or under development and have integrated cybersecurity into their business continuity plans are likely moving toward a formal strategy for cybersecurity that is applied consistently across their entire enterprise. Although addressing cybersecurity is clearly an IT/OT risk and issue, it is not *only* an IT/OT issue—from a resilience-management perspective, it is dependent on other core business processes. Incorporating these risks is evidence of cybersecurity maturity.

Most utilities (14 in total) have conducted a cybersecurity audit or assessment on information systems, and 11 have conducted an audit or assessment on control systems. Other assessments reported include physical security, wireless, and voice-over Internet protocol. Two utilities have scheduled first assessments for 2016.

When asked about the establishment of priorities, responses suggested a reactive approach. Cooperatives lead the number of reactive answers shown in Figure 12. In particular, 15 utilities reported that systems with known vulnerabilities become a priority for upgrade and replacement. Three cooperatives selected all the options presented. All utilities except one responded that a system becomes a priority for upgrade and replacement when it is compromised during a penetration test, and they also agreed that a system becomes a priority for upgrade and replacement if it has known vulnerabilities. Only one utility (NERC compliant) recognized that risk was an integral part of setting priorities: they responded, "upgrade by risk. Hardened against perceived risk." From a maturity perspective, "other" might be preferred. While other options could infer proactive vulnerability assessment and remediation, such as "known vulnerabilities" could suggest active scanning; "systems compromised during a penetration test" could suggest programmatic penetration testing, more research is needed to verify underlying controls.

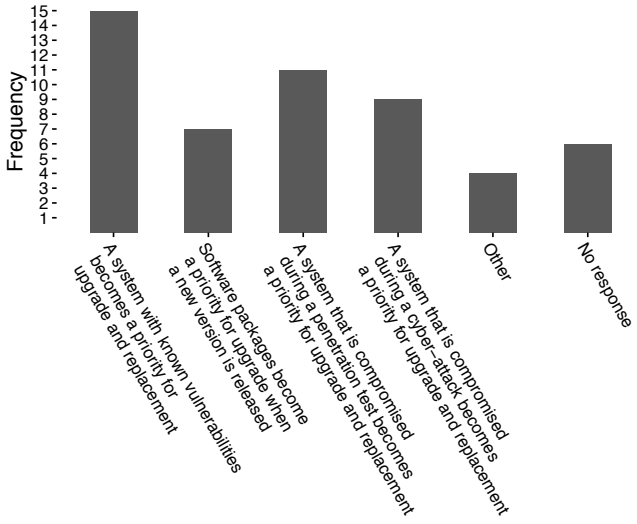


**Figure 12. Establishment of priorities**

Other includes include "methods still being determined" and "replacement of firewall due to limited functionality."

## Execution and Performance

### *Attacks*

Half of the utilities (11) reported not having been hit by any form of cyber attack in the last year, including a denial-of-service attack, a ransomware attack, an attack in which data was stolen from the system, and an attack in which hackers took control of physical devices of the system. Only five utilities (including two NERC-compliant) reported explicitly having been hit by an attack or having received multiple attempts. One nonfederally-regulated municipality commented that attack attempts happen on a near-daily basis, but they did not report an attack, and a nonfederally-regulated cooperative mentioned, "attempts happen all the time, but [we] haven't been breached." A nonfederally-regulated municipality mentioned that such information is not available. Other reported attacks by two NERC-compliant utilities include the following: "one machine […] bounced data back out" (presumably attack detected but repelled) and "some infections via disk images from vendors." In summary, the utilities reported attempts, but the responses suggest very few successes.

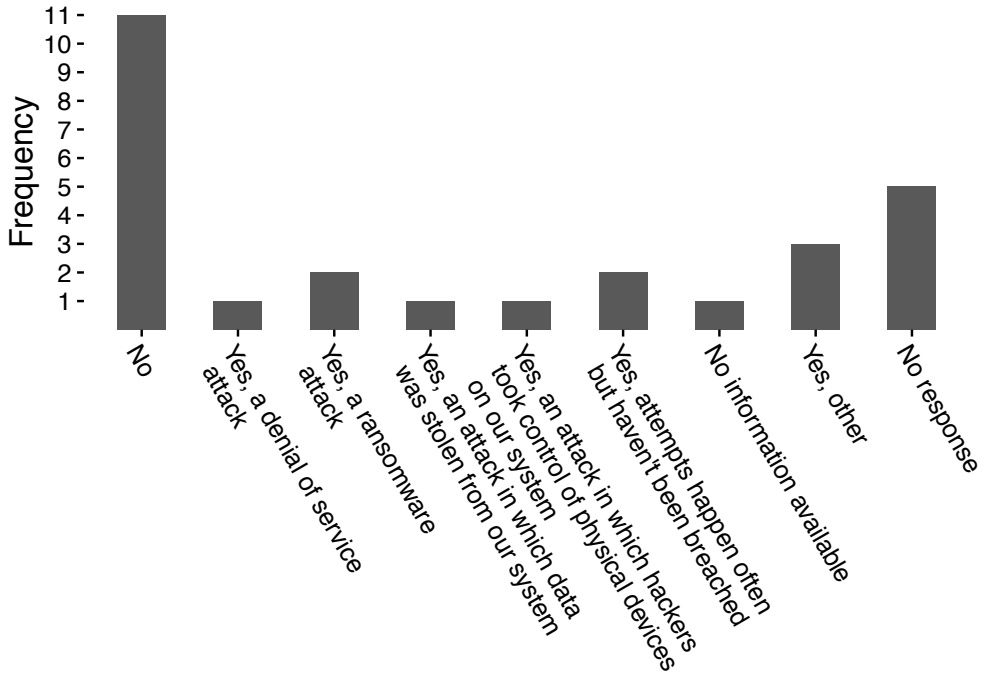


**Figure 13. Cybersecurity attacks reported by participating utilities**

### *Cybersecurity Strategies*

Only one utility reported not using any of the cybersecurity strategies listed, and seven did not respond to the question. The most popular cybersecurity strategy was network segmentation: 10 nonfederally-regulated utilities and 2 NERC-compliant utilities use this approach. Defense in depth and defense in breadth were selected by eight and five utilities, respectively, and in general, having one of these two indicated having another alternative simultaneously (with the exception of one NERC-compliant IOU that reported implementing only defense in depth).

In addition, four nonfederally-regulated utilities that reported at least two cybersecurity efforts did not respond to this question. Of the 10 nonfederally-regulated utilities that reported having at least one of the strategies presented, only 3 did not report their cybersecurity efforts.

These results suggest that if a strategy is in place (i.e., defense in depth, defense in breadth, a zero-trust network, network segmentation, or air gapping), it is likely that at least one cybersecurity effort is in place, such as a governing document, a strategy to implement such a governing document, or a pilot program. On the other hand, having a governing document or policy in place does not necessarily translate into having implemented any of these cybersecurity strategies.

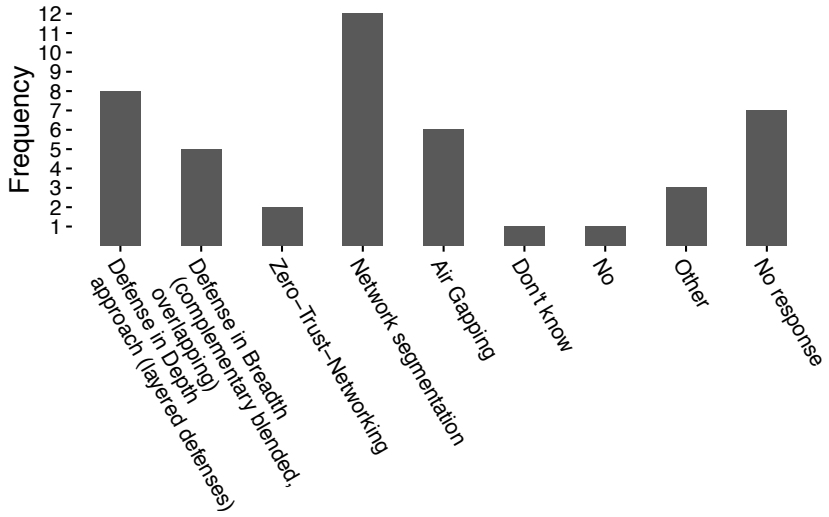


**Figure 14. Cybersecurity strategies**

### *Situational Awareness*

Utilities reported that they maintain situational awareness of system security primarily through incident sharing across the organization. Nine non federally regulated utilities reported having three or more methods in place. From the responding utilities, only one (non federally regulated) reported using only one method, which they defined as "network monitoring by outside IT agency." The other methods specified were the use of SecureWorks and receiving email alerts from Industrial Control Systems Cyber Emergency Response Team.

### *Use of Penetration Testing*

In addition to the cybersecurity strategies outlined and the situational awareness practices, 10 non-NERC utilities reported using penetration testing, and one additional utility is planning on using it, although it was not sure about the time frame. One cooperative mentioned using two companies to perform the testing.

### *Integrated Cybersecurity Efforts across Business Systems and Control Systems*

The majority of utilities responded that they have integrated cybersecurity efforts across business systems and control systems: 14 in total, one of which is NERC compliant. Only one NERC-compliant IOU responded "no," and the other NERC-compliant utility reported having a partial integration. Six non federally regulated utilities did not respond to the question.

Table 9 compiles the responses related to integrating networks (IT and OT) and systems (business and control) according to the non-federally regulated participating utilities. Of these 19 utilities, less than half reported integration in both areas, and three utilities reported integration at the systems level but not at the network level. Any utility reported integration at the network level and not at the systems level, suggesting that integration at the systems level might be implemented earlier than integration at the network level.

**Table 9. Relationship between Responses About Integration Across Networks (IT and OT) and Systems (Business and Control)**

| | IT and OT Managed by Same People | Integration of Cybersecurity Efforts Across Business and Control Systems | No. of Nonfederally-Regulated Utilities |
|---|---|---|---|
| 1 | Yes | No response | 5 |
| 2 | Yes | Yes | 6 |
| 3 | No response or N/A | Yes | 4 |
| 4 | No | Yes | 3 |
| 5 | No response | No response | 1 |

## Support

### *Cybersecurity Criteria for Vendors*

All NERC-compliant utilities apply cybersecurity criteria to vendors. Six non federally-regulated utilities did not respond to the question, but only two of those that responded reported using only one criteria; the rest reported using two or more criteria. The data collected suggests that the request-for-proposal stage considers questions on secure development. No utility depends only on a third-party evaluation of a vendor's cybersecurity.

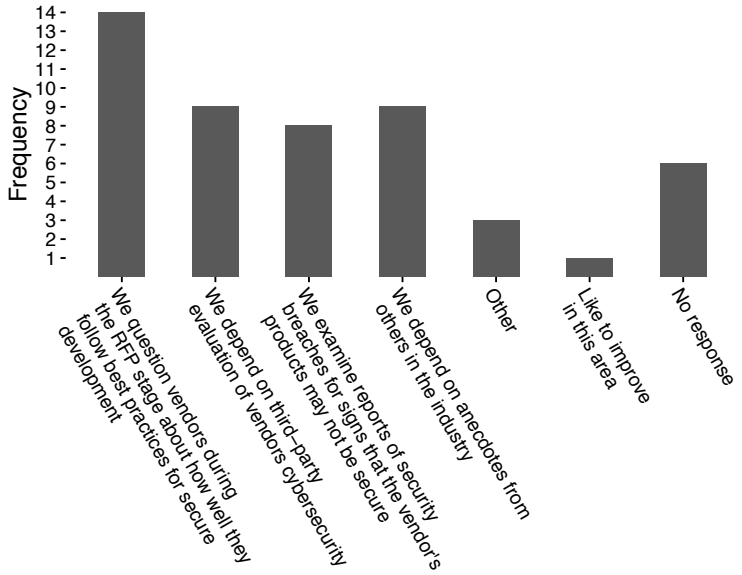


**Figure 15. Cybersecurity criteria used for vendor and device selection**

### *Areas in Which Vulnerability Assessments Are Performed*

Two utilities reported not performing vulnerability assessments in any of these areas, and seven did not respond. The most common area where vulnerability assessments are performed is in cybersecurity, followed by supervisory control and data acquisition systems, smart grids, and Internet connectivity. Seven non federally-regulated utilities reported performing vulnerability assessments in four or more areas. Other areas mentioned included video and access control.

### *Learning and Adaptation from Past Events*

Most utilities reported some type of adaptation to and learning from past cybersecurity incidents. Even those that did not report having been hit by a cyber attack in the last year reported establishing forensic investigations, upgrading or replacing software, and training staff. In particular, four utilities reported not having any cybersecurity problems so far. In particular, one utility reported: "to date we have no known breaches, but we would most likely hire an outside firm to conduct an investigation and make changes." Five utilities reported other mechanisms for learning and adaptation, mainly "internal phishing program," "phishing once a month or sometimes more often," "switching to [security company]," and "we look at what has happened and adjust business processes accordingly."

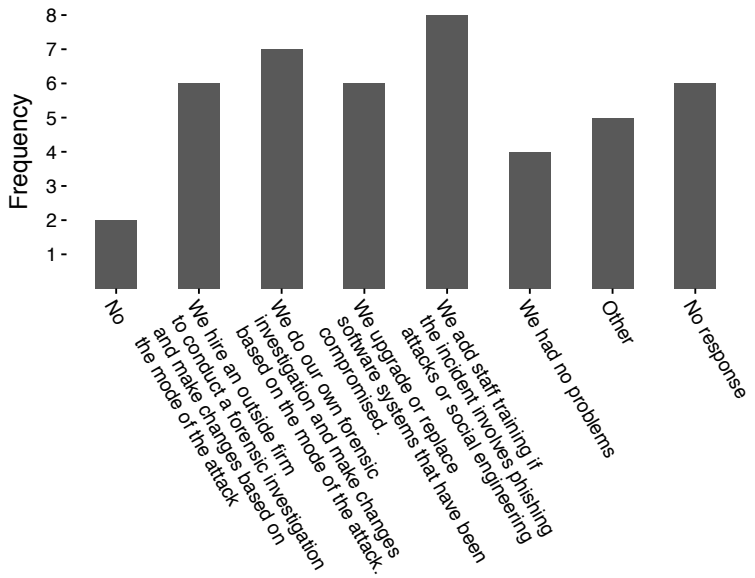


**Figure 16. Learning and adaptation from past events**

## Frequency tables of responses

**Q1.**.

| | State | Frequency |
|---|---|---|
| 1 | AK | 1 |
| 2 | AL | 2 |
| 3 | CA | 2 |
| 4 | CO | 1 |
| 5 | FL | 1 |
| 6 | KY | 1 |
| 7 | LA | 1 |
| 8 | MS | 1 |
| 9 | MT | 1 |
| 10 | NC | 1 |
| 11 | NH | 1 |
| 12 | OK | 1 |
| 13 | SC | 1 |
| 14 | TN | 7 |
| 15 | Total | 22 |

**Q2.**

| | Utility Type | Frequency |
|---|---|---|
| 1 | Cooperative | 12 |
| 2 | Investor-Owned | 3 |
| 3 | Municipal | 7 |
| 4 | Total | 22 |

**Q3.**

| | Number of meters | Frequency |
|---|---|---|
| 1 | < 25,000 | 7 |
| 2 | > 250,000 | 2 |
| 3 | 100,000 to 250,000 | 5 |
| 4 | 25,000 to 50,000 | 6 |
| 5 | 50,000 to 100,000 | 2 |
| 6 | Total | 22 |

**Q4.**

| | Number of employees | Frequency |
|---|---|---|

| | | |
|---|---|---|
| 1 | 11 to 50 | 6 |
| 2 | 51 to 100 | 4 |
| 3 | 101 to 500 | 9 |
| 4 | >500 | 3 |
| 5 | Total responses | 22 |

**Q5.**

| | People in Cybersecurity Team | Frequency |
|---|---|---|
| 1 | 1 | 4 |
| 2 | 2 to 5 | 13 |
| 3 | 6 to 10 | 2 |
| 4 | 11 to 20 | 2 |
| 5 | >20 | 1 |
| 6 | Total responses | 22 |

**Q6.**

| | IT Budget | Frequency |
|---|---|---|
| 1 | < $50,000 | 2 |
| 2 | $50,000 to $100,000 | 1 |
| 3 | $100,001 to $250,000 | 2 |
| 4 | $250,001 to $500,000 | 1 |
| 5 | $500,001 to $1,000,000 | 6 |
| 6 | >$1,000,000 | 7 |
| 7 | No response | 3 |
| 8 | Total utilities that responded to at least one alternative | 19 |
| 9 | Total responses | 19 |

**Q7.**

| | Cybersecurity Budget | Frequency |
|---|---|---|
| 1 | < $10,000 | 3 |
| 2 | $10,000 to $25,000 | 4 |
| 3 | $25,001 to $100,000 | 5 |
| 4 | $100,001 to $250,000 | 1 |
| 5 | > $500,000 | 3 |
| 6 | N/A (No cybersecurity budget established) | 4 |
| 7 | Not sure | 1 |
| 8 | No response | 1 |
| 9 | Total utilities that responded to at least one alternative | 21 |
| 10 | Total | 21 |

**Q8.**

| | Recovery mechanism | Frequency |
|---|---|---|
| 1 | Base Rate | 10 |
| 2 | Closed Proceedings | 1 |
| 3 | Adjustment Clauses | 0 |
| 4 | Deferral Accounts | 0 |
| 5 | Security Recovery Factor (or similar) | 2 |
| 6 | Not sure | 2 |
| 7 | Other | 3 |
| 8 | No formal recovery mechanism | 3 |
| 9 | No response | 2 |
| 10 | Total utilities that responded to at least one alternative | 20 |
| 11 | Total responses | 21 |

**Q9.**

| | Cybersecurity Efforts | Frequency |
|---|---|---|
| 1 | Internally approved cybersecurity policy | 12 |
| 2 | Implementation strategy | 11 |
| 3 | Approved budget for cybersecurity efforts | 10 |
| 4 | Cybersecurity pilot programs | 8 |
| 5 | Fully implemented cybersecurity program | 4 |
| 6 | No effort in place | 1 |
| 7 | Other | 2 |
| 8 | No response | 4 |
| 9 | Total utilities that responded to at least one alternative | 18 |
| 10 | Total responses | 48 |

**Q10.**

| | Efforts in house or outsourced | Frequency |
|---|---|---|
| 1 | Combination | 13 |
| 2 | In-house | 6 |
| 3 | Outsourced | 2 |
| 4 | No response | 1 |
| 5 | Total utilities that responded to at least one alternative | 21 |
| 6 | Total responses | 21 |

**Q11.**

| | Cybersecurity policy audited | Frequency |
|---|---|---|
| 1 | No | 2 |
| 2 | Yes, audited by a combination of internal and external resources | 3 |
| 3 | Yes, audited by an outside party | 5 |
| 4 | Yes, audited internally | 3 |
| 5 | N/A (Policy in process) | 1 |
| 6 | N/A (We have no cybersecurity policy) | 7 |
| 7 | No response | 1 |
| 8 | Total utilities that responded to at least one alternative | 21 |
| 9 | Total responses | 21 |

**Q12.**

| | Frequency of audits | Frequency |
|---|---|---|
| 1 | More than once per year | 2 |
| 2 | Every 1-2 years | 7 |
| 3 | Less frequently than once every 2 years | 2 |
| 4 | N/A We have no cybersecurity policy | 7 |
| 5 | N/A Policy in progress | 1 |
| 6 | Not sure | 1 |
| 7 | No response | 2 |
| 8 | Total utilities that responded to at least one alternative | 20 |
| 8 | Total responses | 20 |

**Q13.**

| | Efforts to improve cybersecurity posture | Frequency |
|---|---|---|
| 1 | National Association (NRECA, APPA, EEI, or other) | 11 |
| 2 | Statewide association of distribution utilities | 7 |
| 3 | Infragard | 6 |
| 4 | One or more fusion centers | 2 |
| 5 | Other | 9 |
| 6 | Not sure | 1 |
| 7 | No response | 5 |

| | | |
|---|---|---|
| 8 | Total utilities that responded to at least one alternative | 17 |
| 9 | Total responses | 36 |

**Q14.**

| | Primary challenges to cybersecurity efforts | Frequency |
|---|---|---|
| 1 | Lack of support from utility board | 1 |
| 2 | Lack of support from utility executives | 3 |
| 3 | Budget | 6 |
| 4 | Technology availability and maturity | 7 |
| 5 | Legacy systems (installed equipment basis) | 8 |
| 6 | Lack of standards | 2 |
| 7 | Lack of skilled workforce | 7 |
| 8 | Other | 5 |
| 9 | No response | 5 |
| 10 | Total utilities that responded to at least one alternative | 17 |
| 11 | Total responses | 39 |

**Q15.**

| | Cybersecurity Guidance | Frequency |
|---|---|---|
| 1 | NISTIR 7628 | 4 |
| 2 | NIST Cybersecurity Framework (v1) | 8 |
| 3 | DOE's ES-C2M2 | 3 |
| 4 | DOE's RMP Guideline | 1 |
| 5 | N/A (we don't use any of these) | 4 |
| 6 | Other | 9 |
| 7 | Not sure | 1 |
| 8 | No response | 5 |
| 9 | Total utilities that responded to at least one alternative | 17 |
| 10 | Total responses | 30 |

**Q16.**

| | Job title of lead in cybersecurity | Frequency |
|---|---|---|
| 1 | Chief Information Officer (CIO) | 1 |
| 2 | Chief Information Security Officer (CISO) | 1 |
| 3 | Chief Security | 1 |

| | | |
|---|---|---|
| | Officer (CSO) | |
| 4 | N/A (no such person at our utility) | 6 |
| 5 | Other | 10 |
| 6 | No response | 4 |
| 7 | Total utilities that responded to at least one alternative | 18 |
| 8 | Total responses | 19 |

**Q17.**

| | **Are IT and OT handled by the same people?** | **Frequency** |
|---|---|---|
| 1 | Yes,IT and OT are handled by the same people | 11 |
| 2 | Yes, to some extent, for policy. Compliance done separately | 1 |
| 3 | No, IT and OT are handled by different people | 5 |
| 4 | N/A | 1 |
| 5 | No response | 4 |
| 6 | Total utilities that responded to at least one alternative | 18 |
| 7 | Total responses | 18 |

**Q18.**

| | **What national agencies have done** | **Frequency** |
|---|---|---|
| 1 | Imposed regulation on distribution utilities | 1 |
| 2 | Monitored security planning, implementation and performance | 3 |
| 3 | Encouraged participation in voluntary standards development | 2 |
| 4 | Established cyber event reporting requirements | 2 |
| 5 | Encouraged collaboration on developing a voluntary program | 1 |
| 6 | Encouraged to work individually to improve cyber security | 6 |
| 7 | Offered training or workshops | 1 |
| 8 | Other | 2 |
| 9 | None | 3 |
| 10 | Not Sure | 2 |
| 11 | No response | 8 |
| 12 | Total utilities that responded to at least one alternative | 14 |
| 13 | Total responses | 23 |

**Q19.**

| | What county and city governments have done | Frequency |
|---|---|---|
| 1 | Tested utility cybersecurity plans through cyber attack exercises | 1 |
| 2 | Established a program to provide support during emergencies related to cyber events | 1 |
| 3 | Encouraged utilities to participate in voluntary standards development | 1 |
| 4 | Encouraged collaboration on developing a voluntary program | 1 |
| 5 | Encouraged to work individually to improve cyber security | 3 |
| 6 | Offered training or workshops | 1 |
| 7 | None | 7 |
| 8 | Not sure | 1 |
| 9 | No response | 11 |
| 10 | Total utilities that responded to at least one alternative | 11 |
| 11 | Total responses | 16 |

**Q20.**

| | Efforts beyond of what is required | Frequency |
|---|---|---|
| 1 | Yes, we conduct a risk assessment and design our cybersecurity program accordingly | 8 |
| 2 | Yes, we follow industry best practices and guidelines to determine the right program for our utility | 7 |
| 3 | No, we don't go beyond what regulators require | 1 |
| 4 | N/A | 1 |
| 5 | Not sure | 1 |
| 6 | Other | 3 |
| 7 | No response | 6 |
| 8 | Total utilities that responded to at least one alternative | 16 |
| 9 | Total responses | 21 |

**Q21.**

| | Reporting attempted breach | Frequency |
|---|---|---|
| 1 | We report to our board of directors | 12 |
| 2 | We report to PUC | 3 |
| 3 | We report to FBI | 6 |

| | | |
|---|---|---|
| 4 | We report to DHS | 4 |
| 5 | No breaches | 2 |
| 6 | Nothing | 1 |
| 7 | Other | 2 |
| 8 | No response | 5 |
| 9 | Total utilities that responded to at least one alternative | 17 |
| 10 | Total responses | 30 |

**Q22.**

| | Cybersecurity plan structure | Frequency |
|---|---|---|
| 1 | Cybersecurity plan contains cyber and physical components | 8 |
| 2 | Physical security plan identifies critical cyber assets | 1 |
| 3 | N/A | 3 |
| 4 | Other | 5 |
| 5 | No response | 6 |
| 6 | Total utilities that responded to at least one alternative | 16 |
| 7 | Total responses | 17 |

**Q23.**

| | Cybersecurity in Business Continuity | Frequency |
|---|---|---|
| 1 | Yes | 14 |
| 2 | No | 2 |
| 3 | No response | 6 |
| 4 | Total utilities that responded to at least one alternative | 16 |
| 5 | Total responses | 16 |

**Q24.**

| | Cybersecurity audit or assessment on the following | Frequency |
|---|---|---|
| 1 | Information systems | 14 |
| 2 | Control systems | 11 |
| 3 | Other | 4 |
| 4 | No response | 6 |
| 5 | Total utilities that responded to at least one alternative | 16 |
| 6 | Total responses | 29 |

**Q25.**

| | Establishment of priorities | Frequency |
|---|---|---|
| 1 | A system with known vulnerabilities becomes a priority for upgrade and replacement | 15 |

| | | |
|---|---|---|
| 2 | Software packages become a priority for upgrade when a new version is released | 7 |
| 3 | A system that is compromised during a penetration test becomes a priority for upgrade and replacement | 11 |
| 4 | A system that is compromised during a cyber-attack becomes a priority for upgrade and replacement | 9 |
| 5 | Other | 4 |
| 6 | No response | 6 |
| 7 | Total utilities that responded to at least one alternative | 16 |
| 8 | Total responses | 46 |

**Q26.**

| | Cybersecurity Attacks | Frequency |
|---|---|---|
| 1 | No | 11 |
| 2 | Yes, a denial of service attack | 1 |
| 3 | Yes, a ransomware attack | 2 |
| 4 | Yes, an attack in which data was stolen from our system | 1 |
| 5 | Yes, an attack in which hackers took control of physical devices on our system | 1 |
| 6 | Yes, attempts happen often but haven't been breached | 2 |
| 7 | No information available | 1 |
| 8 | Yes, other | 3 |
| 9 | No response | 5 |
| 10 | Total utilities that responded to at least one alternative | 17 |
| 11 | Total responses | 22 |

**Q27.**

| | Utility employs | Frequency |
|---|---|---|
| 1 | Defense in Depth approach (layered defenses) | 8 |
| 2 | Defense in Breadth (complementary blended, overlapping) | 5 |
| 3 | Zero-Trust-Networking | 2 |
| 4 | Network segmentation | 12 |
| 5 | Air Gapping | 6 |
| 6 | Don't know | 1 |

| | | |
|---|---|---|
| 7 | No | 1 |
| 8 | Other | 3 |
| 9 | No response | 7 |
| 10 | Total utilities that responded to at least one alternative | 15 |
| 11 | Total | 38 |

**Q28.**

| | Situational Awareness | Frequency |
|---|---|---|
| 1 | Internal network monitoring | 13 |
| 2 | Incident sharing across the organization | 14 |
| 3 | Sharing threat information with others in industry and government | 10 |
| 4 | Understanding critical dependencies across systems | 11 |
| 5 | Other | 6 |
| 6 | No response | 6 |
| 7 | Total utilities that responded to at least one alternative | 16 |
| 8 | Total | 54 |

**Q29.**

| | Penetration testing | Frequency |
|---|---|---|
| 1 | No | 4 |
| 2 | Yes | 12 |
| 3 | No response | 12 |
| 4 | Total utilities that responded to at least one alternative | 10 |
| 5 | Total responses | 16 |

**Q30.**

| | Integrated cybersecurity efforts | Frequency |
|---|---|---|
| 1 | No | 1 |
| 2 | Partially | 1 |
| 3 | Yes | 14 |
| 4 | No response | 6 |
| 5 | Total utilities that responded to at least one alternative | 16 |
| 6 | Total responses | 16 |

**Q31.**

| | Cybersecurity criteria for vendors | Frequency |
|---|---|---|
| 1 | We question vendors during the RFP stage about how well they | 14 |

| | | |
|---|---|---|
| | follow best practices for secure development | |
| 2 | We depend on third-party evaluation of vendors cybersecurity | 9 |
| 3 | We examine reports of security breaches for signs that the vendor's products may not be secure | 8 |
| 4 | We depend on anecdotes from others in the industry | 9 |
| 5 | Other | 3 |
| 6 | Like to improve in this area | 1 |
| 7 | No response | 6 |
| 8 | Total utilities that responded to at least one alternative | 16 |
| 9 | Total responses | 44 |

**Q32.**

| | **Vulnerability assessments** | **Frequency** |
|---|---|---|
| 1 | Cybersecurity | 10 |
| 2 | SCADA | 9 |
| 3 | Smart grid | 9 |
| 4 | Internet connectivity | 9 |
| 5 | Website hosting | 7 |
| 6 | Not sure | 1 |
| 7 | Other | 2 |
| 8 | No | 2 |
| 9 | No response | 7 |
| 10 | Total utilities that responded to at least one alternative | 15 |
| 11 | Total responses | 49 |

**Q33.**

| | **Learning and adaptation from past events** | **Frequency** |
|---|---|---|
| 1 | No | 2 |
| 2 | We hire an outside firm to conduct a forensic investigation and make changes based on the mode of the attack | 6 |
| 3 | We do our own forensic investigation and make changes based on the mode of the attack. | 7 |
| 4 | We upgrade or replace software systems that have been compromised. | 6 |
| 5 | We add staff training if | 8 |

| | | |
|---|---|---|
| | the incident involves phishing attacks or social engineering | |
| 6 | We had no problems | 4 |
| 7 | Other | 5 |
| 8 | No response | 6 |
| 9 | Total utilities that responded to at least one alternative | 16 |
| 10 | Total | 38 |