NARUC
National Association of Regulatory Utility Commissioners

Cybersecurity Strategy Development Guide

Cadmus Group LLC

October 30, 2018

Acknowledgments and Disclaimers

This report was developed under the project "State and Local Innovation and Analysis in Support of Long-Term Energy Planning and Policy," of the National Association of Regulatory Utility Commissioners (NARUC) Center for Partnerships & Innovation. This material is based on work supported by the U.S. Department of Energy under Award Number DE-OE0000818.

The genesis for this report draws from work funded U.S. Agency for International Development's Bureau for Europe & Eurasia under its Cooperative Agreement # AID-OAA-A-16-00049 with NARUC. Discussions held during technical workshops in 2016-2017 led to the preparation of the Black Sea Cybersecurity Strategy Development Guide. NARUC, in coordination with U.S. government agencies, is pleased to support the two-way transfer of knowledge and information between U.S. and international regulators on the critical topic.

This report was authored by the Cadmus Group LLC. Throughout the preparation process, NARUC staff and members provided the authors with editorial comments and suggestions. However, the views and opinions expressed herein may not necessarily agree with positions of NARUC or those of the U.S. Department of Energy.

Special thanks to:
Brian Marko, Sandra Jenkins, and Dan LaGraffe, U.S. Department of Energy
Dan Searfoorce, Pennsylvania Public Utility Commission
David Batz and Ivy Lyn, Edison Electric Institute
Dominic Saebeler and Wei Chen Lin, Illinois Commerce Commission
Hon. Ann Rendahl and Jason Ball, Washington Utilities Commission
Jeff Pillon, National Association of State Energy Officials
Lynn P. Costantini, Matthew Acho, and Danielle Sass Byrnett, NARUC
Stephen Cappozzi, Connecticut Public Utilities Regulatory Authority

Please direct questions regarding this report to Lynn Costantini, Deputy Director, NARUC Center for Partnerships and Innovation, at lcostantini@naruc.org or (609) 915-1685.

NARUC
National Association of Regulatory Utility Commissioners

Table of Contents

Cybersecurity Strategy Development Guide

Introduction

The National Association of Regulatory Utility Commissioners (NARUC) developed this *Cybersecurity Strategy Development Guide* to support state public utility commission (PUC) regulators in developing cybersecurity strategies tailored for their own commissions. This document aims to guide commissions' interactions with their utilities on issues related to cybersecurity, drawing from the experiences of federal, state, and private-sector stakeholders, including state PUCs themselves. Further, it provides guidance and practices for regulators to consider as they develop and implement their strategies. Commissions that have already developed a strategy can use this guide to review and enhance their current strategy.

Background

The increasingly interconnected dynamics of industrial control systems (ICS), recent national and global events, and growing numbers of grid-connected devices have brought cybersecurity to the forefront of priorities for utility operators as well as regulators.

Although no US utility has publicly reported a successful cyberattack with physical impacts on its systems or networks, such attacks have occurred in other countries. In 2010, the Stuxnet virus targeted the ICS of a uranium enrichment facility in Iran, disabling the centrifuges. This attack was the first known to specifically target ICS. In 2015, a multi-pronged cyberattack on three Ukrainian electricity distribution companies compromised supervisory control and data acquisition (SCADA) systems, causing outages that impacted approximately 225,000 customers across the country.[1]

Reported attacks on power utilities globally increased six-fold from 2014 to 2015.[2] Despite no damaging attacks, the US government is aware of several cybersecurity breaches into utilities. The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) responded to 59 energy sector cyber incidents in 2016, a 28 percent increase over 2015.[3] The increase is driven in part by the continued integration of information technology (IT) and operational technology (OT), which is expanding the potential threat landscape.

Possible consequences of cyberattacks include exfiltration of personally identifiable information (PII), ransomware demands, and more significantly, physical impacts such as those experienced in the Ukraine. Experience with natural disasters suggest that a successful cyberattack on the electric grid has the potential to cause power outages that last days, weeks, or longer. The 2003 Northeast Blackout left 50 million people without power for four days and resulted in economic losses estimated between $4 billion and $10 billion.[4] In 2017, Hurricane Maria caused significant damage to Puerto Rico's power grid, recovery from which is still ongoing.[5] These examples emphasize the importance of regulators' engagement with utilities before, during, and after a cybersecurity incident. Developing and implementing a robust strategy to ensure effective engagement is an important first step.

---

1 North American Electricity Reliability Corporation Electricity Information Sharing and Analysis Center. Analysis of the Cyber Attack on the Ukrainian Power Grid, 2016, https://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf.

2 Idaho National Laboratory. Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector,2016, https://www.energy.gov/sites/prod/files/2017/01/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Sector.pdf.

3 Department of Homeland Security National Cybersecurity & Communications Integration Center. ICS-CERT Year in Review,2016, https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2016_Final_S508C.pdf.

4 U.S.-Canada Power System Outage Task Force. Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations, 2004, https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf.

5 Department of Energy Infrastructure Security & Energy Restoration. Hurricanes Maria & Irma: April 4 Event Summary (Report #98 – FINAL), 2018, https://www.energy.gov/sites/prod/files/2018/04/f50/Hurricanes%20Maria%20%20Irma%20Event%20Summary%20April%204%2C%202018.pdf.

Purpose

Because of the increasing frequency and potential severity of attempted cyberattacks on critical infrastructure sectors, state PUCs are increasingly recognizing the need for a robust strategy to address the challenges posed by cybersecurity threats as they pertain to utilities they regulate. In turn, the demand for sector-specific guidance to help inform PUC's cybersecurity-related interactions with utilities is growing. Establishing a cybersecurity strategy enables commissions to better understand how their utilities prepare for, respond to, and recover from cybersecurity incidents. It may also assist commissions in identifying additional activities that might be taken to minimize cybersecurity risk to electric distribution systems.

This guide aims to enumerate and explain the steps that regulators can follow to develop their own cybersecurity strategies to engage with utilities. It identifies key issues for regulators to address in establishing their own structured strategies and provides examples of how some states' PUCs have approached each of the given processes. **Figure 1** outlines the steps commissions might take to effectively interface with utilities regarding cybersecurity process implementation. The most effective strategies establish clear PUC priorities and identify relevant stakeholders to inform strategic planning initiatives.

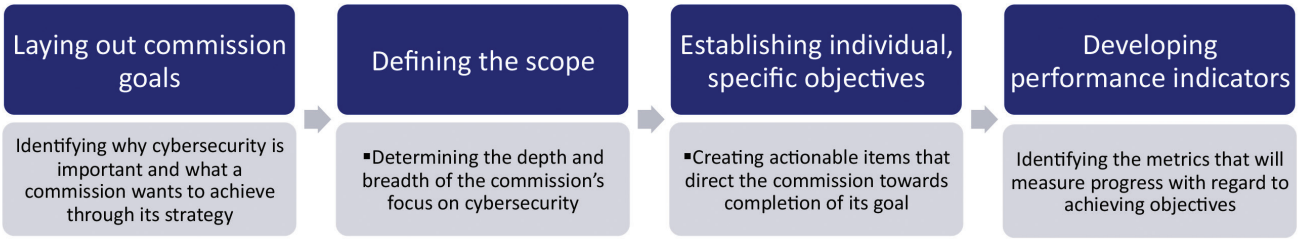


Figure 1. *Initial Steps to Develop a Cybersecurity Strategy*

Commissions face different realities and have varying priorities and resources. As such, each commission benefits from tailoring cybersecurity efforts and strategies according to their specific needs and available resources. Additionally, commissions can use this guide to periodically review and update their cybersecurity strategies to ensure that it continues to address evolving threats and hazards posed by the ever-changing cyber landscape and the associated needs of the PUC and its stakeholders.

Template Structure: Cybersecurity Strategy & Plan

This guide provides a template for a Cybersecurity Strategy & Plan. It is comprised of nine components that commissions can customize and adapt as appropriate, based on their individual needs, priorities, and region-specific circumstances. This structure uses a top down approach that begins with broad, strategic concepts that the commission can then refine into actionable activities. By first identifying key priorities, the PUC can build an effective business case for acquiring new or redistributing existing resources. Doing so serves to focus efforts on what is most important.

To facilitate strategy development, this guide poses leading questions for consideration in each of the nine component areas. However, each commission will ultimately determine the structure that is most useful for them. Note that not every commission will approach its strategy and plan using these steps in this order.

1. Develop Strategic Goal

This section contains an articulation of why a commission values cybersecurity, what the commission's goals are, how those goals will be addressed, and how the commission will define success, based on the individual circumstances of the commission such as stakeholders, gaps, and needs. Key considerations in this step include:

- What is the commission's cybersecurity mission and how should this strategy reflect it?
- What is the commission's vision for success and how will this strategy help achieve it?
- What are the commission's priorities with respect to developing a cybersecurity strategy?

2. Define Scope

This section defines the scope of the strategy. It outlines the utility sectors that the strategy will include as well as the range of cybersecurity activities it will cover and the extent to which specific activities will be emphasized. Key decisions to be made in this step include:

- What are the key requirements of this strategy, as determined by the commission's goals?
- What are the boundaries of this strategy?
- What resources are or will be available to support cybersecurity efforts at the commission (e.g., staffing considerations)?
- How will the commission identify and document its expectations of cybersecurity for the utilities under its jurisdiction?

3. Identify Cybersecurity Needs and Develop Objectives

This section includes a list of objectives that will define, at a high level, the PUC's cybersecurity activities. Before developing objectives, the PUC should consider assessing its own cybersecurity capabilities and identifying any gaps in its current engagement with utilities on this subject. The outcome of these assessments will help to guide the development of achievable, actionable objectives that support the strategic goal of the commission and fit within its scope. Key considerations in this step include:

- What is the commission's current level of cybersecurity awareness and capabilities?
- What are the most pressing threats and hazards that the commission's utilities face?
- Where can PUC efforts have the most impact on the preparedness of its utilities?
- What steps must the PUC undertake to achieve its goals?

4. Establish Performance Indicators

This section identifies the parameters that will be used to evaluate progress toward the specific objectives and overarching goal of the cybersecurity strategy. The indicators would be formulated based on the outcomes of the assessments and objectives described in Section 3. Key decisions in this step include:

- What is the commission's baseline for measuring the effectiveness of its cybersecurity engagement with utilities?
- Does the commission have access to the information it needs to measure progress and assess performance of the utilities in its jurisdiction?
- How will the commission measure progress (e.g., quantitative vs qualitative measures)?

5. Identify Key Stakeholders

This section documents all relevant cybersecurity stakeholders and defines the relationships that the commission will have with and roles played by those stakeholders. These internal and external stakeholders include federal, state, local, and private-sector entities. Stakeholder mapping helps address and minimize any uncertainty, areas of overlap, and gaps while reinforcing the responsibilities of the regulator's cybersecurity role.

***Note:** Commissions may find it useful to identify and work with key stakeholders early in the strategy development process. Doing so may help the commission gain insights regarding its cybersecurity mission and strategic goals.*

In this step, key considerations include:

- With which federal, state, local, and private-sector entities does the commission currently work?
- Which stakeholders have the greatest impact on the commission's cybersecurity capabilities and the cybersecurity capabilities of utilities within the commission's jurisdiction?
- How should the commission engage with stakeholders both within and outside its jurisdiction?

6. Determine Resource Needs

This section identifies the amount of time and level of resources that will be invested in the commission's cybersecurity efforts. Some points to address may include how the commission initially plans to approach cybersecurity concerns, and which staff at the commission will focus on cybersecurity. Key considerations include:

- How will the commission use its resources to meet its cybersecurity goals and objectives?
- Does the commission have the necessary subject-matter expertise to address its cybersecurity needs and, if not, how will it acquire or develop additional capabilities?

7. Develop a Communication Plan

This section identifies the types of communications a commission expects to have with utilities and stakeholders regarding cybersecurity. This includes everyday communication guidelines, mandatory reporting requirements and responsibilities for utilities, and incident communications. Also outlined would be the process by which commissions will interact with their utilities when handling or discussing sensitive information. Key considerations include:

- How does the commission currently communicate with its utilities regarding cybersecurity?
- Are there unmet communication needs that the commission has identified and, if so, what additional steps will the commission need to take to address them?
- Has the commission prepared templates for internal and external communication regarding cyber incidents? (Sample templates are included in Appendix B.)

8. Implement Strategy

This section outlines the process for accomplishing the strategic goals and objectives laid out in the cybersecurity strategy. Whereas the previous sections outline what the plan entails and why it is important, this section details the specific steps of how the strategy will be implemented. Considerations for the PUC include:

- Who in the commission will be responsible for ensuring the execution of the cybersecurity strategy?
- What are the major milestones on the path to strategy implementation?
- What is the schedule for reporting implementation progress?

9. Review Progress

This section outlines a process for regularly updating the commission's cybersecurity strategy, addressing findings related to the performance measures, and capturing and incorporating corrective actions, improvement planning, and lessons learned. Key considerations:

- How will the commission measure the success of its strategic approach?
- How often will the commission review and update its strategy?
- From what sources will the commission identify and incorporate lessons learned for the purposes of strategy improvement?

Strategy Development

Cybersecurity strategy development is a complex and often lengthy process. To begin, PUCs may consider **1) Forming a multi-disciplinary team** within the commission, comprised of personnel with a baseline level of cybersecurity familiarity to help inform the development process; and **2) Determining the action plan for developing the strategy**, recognizing that the timeline for development can vary between organizations. Simple plans may take only a few months to complete whereas complex plans could take years to fully develop. Much of this depends on the size, complexity, and number of utilities overseen. Some of the following factors also contribute to the duration of development:

- Executive support
  - > Early input from leadership can ensure continuing support throughout the strategy development.
  - > With leadership buy-in, it will be easier to institutionalize the idea that cybersecurity is a priority and can result in more readily available resources.
- Team size and resource availability
  - > Teams too large risk a slowed pace of development from internal disagreement, whereas teams too small can lead to issues while trying to balance existing responsibilities.
  - > The more resources made available to the team will allow for a more comprehensive approach to developing the strategy.

Commissions may want to consider inviting key stakeholders to participate in its cybersecurity strategy development efforts. Doing so enhances the process and provides for effective strategic outcomes. Additionally, stakeholder mapping is an important step in the strategy development process itself (see **Section 5. Identify Key Stakeholders**).

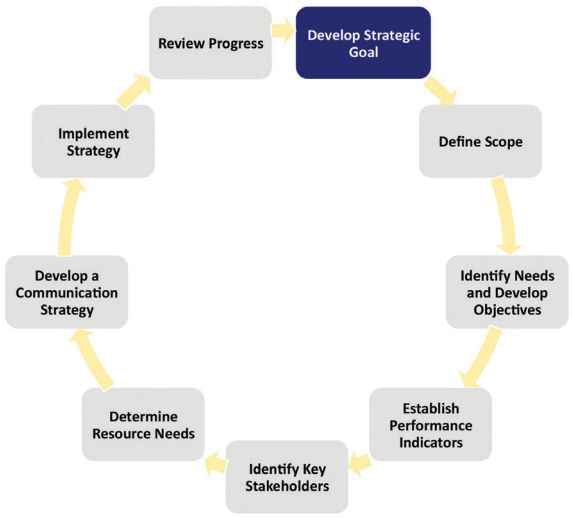
The following sections outline specific processes that PUCs can take to develop a cybersecurity strategy. Each of the sections correspond to and provides guidance relating to each of the nine cybersecurity strategy development components described earlier.

Sensitivities Regarding Cybersecurity

Before beginning work on a cybersecurity strategy or related documents, consideration should be given to the importance and sensitivity of the information involved, especially concerning utilities' cybersecurity plans and preparedness. Some organizations may be reluctant to share such information for fear it exposes attack vectors. Developing and maintaining trusted relationships with key stakeholders through a transparent cybersecurity strategy design process that addresses information protections helps to assuage those concerns about sensitive information. For more information on sensitive information, see **Section 7.1: Handling and Communicating Sensitive Information**.

1. Develop a Strategic Goal

This section of the strategy contains an articulation of why a commission values cybersecurity, what the commission's goals are, how those goals will be addressed, and how the commission will define success, based on the individual circumstances of the commission such as stakeholders, gaps, and needs.



The first step to developing an effective cybersecurity strategy is to assess your commission's motivations for developing one. Motivation may come from an external source, such as direction from a state governor in response to a significant cyber event within the commission's jurisdiction, or it may come from internal sources such as the arrival of a new commission chair with a background or expertise in cybersecurity matters. In either case, the motivation provides a purpose that drives the creation of the strategy and provides an opportunity for the commission to identify and address key cybersecurity issues by providing valuable direction to the commission that will enable it to focus resources through the development and adoption of cybersecurity goals.

When developing a cybersecurity strategy, each commission should clearly define one or more strategic cybersecurity goals that outline why strong cybersecurity measures are important and what they want to achieve in addressing it. Establishing a strategic goal is a critical first step that sets the tone for the entire process of drafting the strategy. Before developing a goal, a commission may want to do an internal inventory of key stakeholders; conduct blue-sky thinking exercises; and do an environmental assessment and literature review to identify near-, mid-, and long-term drivers of change that may affect its goals.

Although they can vary significantly across organizations, strategic goals should provide a sense of purpose, identity, and long-term direction for the commission and clearly communicate internally and externally what the commission values with respect to cybersecurity.

Specifically, a strategic goal allows a commission to define the intent of its cybersecurity strategy in clear, succinct language and highlight the key priorities of the organization with respect to the strategy. While drafting goals, a commission will want to consider its role in supporting the preparedness and mitigation functions of cyber incident management:

- **Preparedness and Mitigation:** Commissions determine how they will validate cybersecurity incident capabilities and what role they will serve in supporting utility preparedness prior to a cyberattack, recognizing potential threats and hazards as they develop.

Washington Utilities and Transportation Commission (UTC) Case Example[6]

The cybersecurity strategy developed by the Washington UTC succinctly incorporates its strategic cybersecurity goals into its overarching mission statement:

Our Mission *is to protect the people of our state by ensuring that investor-owned utility and transportation services are safe, available, reliable, and fairly priced. To assure our mission when considering cybersecurity, the [goals] of this strategy are to facilitate risk-based decision making that weighs trade-offs and supports action that:*

- *Prevents cyberattacks against critical infrastructures;*
- *Reduces vulnerability to cyberattacks; and*
- *Minimizes damage and recovery time from cyberattacks that do occur.*

The language used by the UTC in this example underscores that the UTC will use a **risk-informed approach** when making decisions about balancing interests. The Washington UTC's goal emphasizes its supporting role in cybersecurity. The focus is on helping utilities prevent cyberattacks against critical infrastructures ***before*** they occur, and to encouraging activities that serve to minimize damage and recovery time ***after*** *a* cyberattack has occurred.

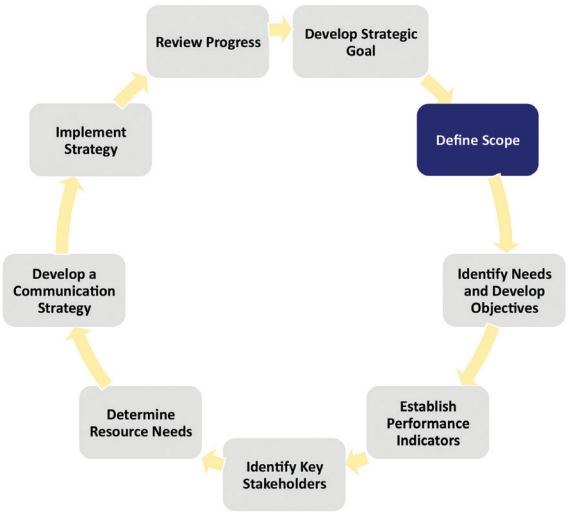
As the example suggests, the primary group tasked with securing critical infrastructure assets are the utilities that own those assets, not regulators. A useful analogy was made by speakers at a recent European cybersecurity workshop: regulators are not castle-builders, but they need to be able to analyze and know what constitutes a strong, well-built castle. As such, a commission does not need to have the engineering and carpentry skills to build a proverbial castle, but they will want to be able to support the process to ensure its goals are achieved. This sentiment is reflected in WUTC's cybersecurity strategy.

The last three bullet points in the example are written to ensure that the goal is achievable. By casting the end state as reducing vulnerability and minimizing damage, the UTC is recognizing that cyberattacks cannot be entirely eliminated but that their associated risks can be mitigated.

6 https://www.utc.wa.gov/aboutUs/Pages/default.aspx and WUTC email communications to Matthew Acho (NARUC), August 15, 2018.

2. Define Scope

This section defines the scope of the strategy. It outlines the utility sectors that the strategy will address as well as the range of cybersecurity activities it will cover and the extent to which the activities will be emphasized.



Scope refers to the **breadth** and **depth** of a commission's focus and attention towards cybersecurity concerns. Defining scope is fundamental to the development of a cybersecurity strategy. **Breadth** refers to the range of sectors (e.g., electricity, water, natural gas) and hazards that the regulator will address. Conversely, **depth** refers to the degree and regularity of engagement a commission expects to have with their regulated utilities and the degree to which the commission will examine various aspects of the utilities' systems. The commission can expand the breadth or depth of its scope as circumstances evolve. There is no "one size fits all" strategy; rather, commissions will want to tailor their strategies based on their prioritized assessment of risks to critical utility assets and their stated goals and objectives.

An important factor to consider when determining scope is the advancement of technology and the range of new, unforeseen cyber threats (or solutions) that it may present. The evolution of the smart grid is transforming how utilities use IT and OT, creating interdependencies between different technologies and their functions. Systems that previously operated in isolation are being brought together via network modernization, such as SCADA network monitoring systems supported by geographic information system (GIS) tools to model and visualize networks. Considering these developments, cybersecurity does not refer only to IT assets, rather it must also include OT assets. Consequently, a PUC will want to decide the scope of its strategy in the context of a broad range of technological elements that must independently be secure to minimize vulnerability.

Although there are many examples, the scopes described in the cybersecurity strategies of the Washington UTC and the Kentucky Public Service Commission (PSC) serve as helpful examples.

The Washington UTC began with a narrow and shallow scope.[7] This approach simplified the process of developing an initial cybersecurity strategy and enabled progress to be made despite limited resources. The initial scope was limited to 12 cybersecurity related questions for jurisdictional utilities to address. Over time, the scope grew to include additional questions and foster closer engagement. Starting with a narrow scope that expedited the implementation process, and helped to further develop the Commission's cybersecurity capabilities.

The Kentucky PSC started with a much wider and deeper scope, including all its utilities in the strategy development process.[8] Leveraging its trusted relationships across the sectors, the Kentucky PSC established buy-in from the utilities that strengthened their interactions and provided valuable information and access. While this approach required a significant investment of time and resources at the outset, it produced comprehensive results in a short amount of time.

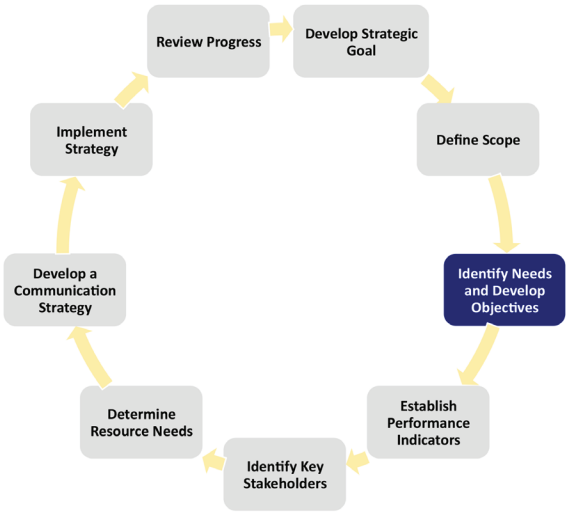
7 Verified by Matthew Acho (NARUC) during phone call with WUTC staff, September 12, 2018.

8 Verified by email between John Lyons (Kentucky PSC) and Matthew Acho (NARUC), September 11, 2018.

3. Identify Cybersecurity Needs and Develop Objectives

This section includes a list of objectives that will define, at a high level, the PUC's cybersecurity activities. Before developing the objectives, the PUC will want to assess its cybersecurity capabilities and perform an analysis of the gaps in commission engagement with utilities. The outcome of these assessments will help to guide the development of achievable, actionable objectives that support the strategic goal of the commission and fit within its scope.

After developing the strategic goal and scope, the commission will be ready to identify the specific activities that it will undertake within the context of its strategy. By developing strong objectives, the commission will be able to communicate its motivations and provide a snapshot of its priorities with respect to cybersecurity.



3.1 Conduct Current Performance Assessment and Gap Analysis

To design a cybersecurity strategy, a commission should develop an understanding of the major threats and hazards that could affect utilities within its jurisdiction as well as familiarize itself with the general level of their cyber capabilities and any major gaps that exist between the two. By considering the utilities' capabilities and identifying gaps, the commission can prioritize its engagement activities to accordingly respond to the needs of the threat landscape.

Determining the threat landscape involves working with regulated utilities to identify the following:

- Critical utility IT and OT assets that may be disrupted as a result of a cyberattack;
- Potential threats to these critical assets; and
- Impacts incurred if threats are realized.

By working closely with their utilities and building strong relationships, commissions can gain a better understanding of the evolving threats that utilities face and their general level of preparedness. Commissions can also encourage utilities to use available resources to conduct internal cybersecurity assessments.

Many tools exist for this purpose. However, as explained in NARUC's 2017 Cybersecurity Primer for Regulators,[9] a simple checklist or demonstrated compliance to mandatory standards may be insufficient. Although the NERC CIP Standards are a good resource to identify the topical areas where standards have been applied in the bulk power system, it should be noted that there are presently no mandatory, enforceable, or comprehensive standards in place at the distribution level in the United States.

Considering this, a regulator's strategy may involve emphasizing that the commission understands the distinction between standards and best practices, will work with utilities and governmental agencies to establish appropriate expectations and will use a risk-informed approach to motivate good, effective cybersecurity performance. Another effective strategy could also convey a commission's approach to developing cybersecurity rules.

9 National Association of Regulatory Utility Commissioners. *Cybersecurity: A Primer for State Utility Regulators, Version 3.0, 2017,* https://pubs.naruc.org/pub/66D17AE4-A46F-B543-58EF-68B04E8B180F.

3.2 Develop Objectives

Although regulators may not have a comprehensive understanding of its utilities' gaps or shortfalls, it should work closely with them to identify areas where utilities and regulators can work together to improve the jurisdiction's cybersecurity. Once a commission has identified key areas on which to focus their efforts, it will want to develop a series of objectives that outline the activities it will undertake to help utilities fill the gaps and remedy shortfalls. The objectives should be specific, realistic, and actionable, combining what the commission values, with the realities they face. An objective of being "100% fully cyber secure," for example, would be unrealistic as both the commission and utilities would be unable to achieve this goal considering the continuously evolving nature of cyber threats. Instead, a commission might choose to define their objectives as "the capability to measure and improve the outcomes of cyber investments by utilities, regularly exercising communication channels with companies, and developing more transparent and useful reporting."[10] These objectives make it clear what the commission is attempting to do and they are measurably achievable.[11]

Objectives further define a commission's strategic goals and outline the major activities that it will undertake as part of its cybersecurity strategy. The following is an example of how cybersecurity objectives can support a strategic goal:

Goal: Increase cybersecurity preparedness among critical infrastructure operators.

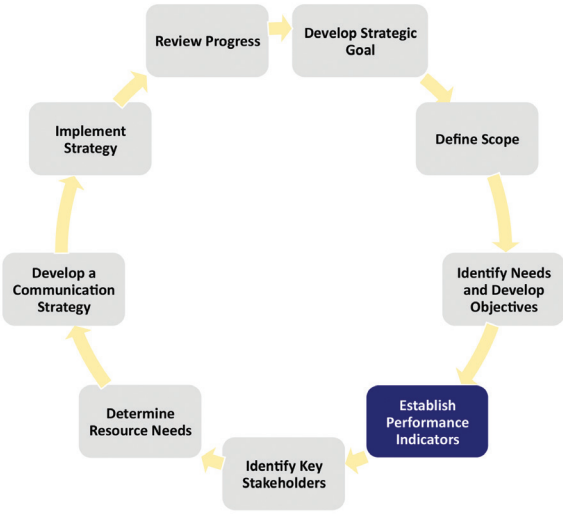
- **Objective 1:** Increase the cybersecurity subject-matter expertise within the commission.
- **Objective 2:** Identify cybersecurity investments that have demonstrable value for preparedness.
- **Objective 3:** Support and encourage annual cybersecurity exercises throughout the jurisdiction.

10 DOE is continuing to support utility regulators in improving resilience to widespread and long-duration power interruptions, focusing mainly on analysis of cost recovery for security investments. DOE's analysis examines current regulatory practices and processes for enhancing cybersecurity and resilience across states.

11 Section 4 discusses establishing a time frame and performance indicators for the objectives that help to measure progress toward the strategy goal.

4. Establish Performance Indicators

This section identifies the parameters that will be used to evaluate progress toward the specific objectives and overarching goal of the cybersecurity strategy. The indicators would be formulated based on the outcomes of the assessments and objectives described in Section 3.



Performance indicators are a tool for tracking implementation of the objectives established in a cybersecurity strategy. For PUCs to assess whether their cybersecurity activities are having a demonstrable impact, the commission must develop a method for tracking and measuring progress, based on cyber-specific performance indicators.[12] These performance indicators should be specific, measurable, attainable, relevant, and timely (SMART), further detailed in **Figure 3**.

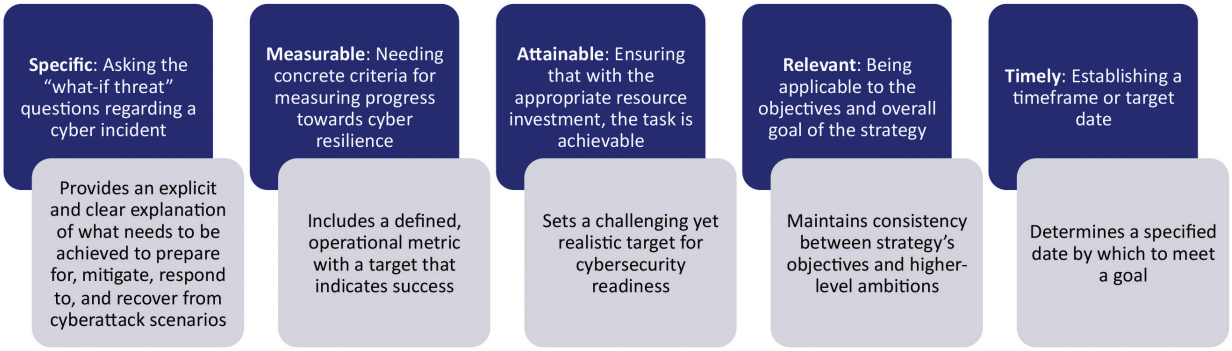


Figure 3. *SMART Performance Indicators*

Performance indicators will vary based on each commission's goals and objectives. Regardless, all indicators should focus on outcomes, rather than activities. The following are some examples of effective performance indicators:

- **Performance Indicator:** By 2023, all utilities within the commission's jurisdiction have a cybersecurity incident response plan that has been exercised at least once.
- **Performance Indicator:** By 2023, all utilities within the commission's jurisdiction have conducted a cyber risk or vulnerability assessment of its information systems, control systems, and other networked systems.

12 The Electric Power Research Institute (EPRI) is developing metrics that will represent the status of a utility's security posture. For more information, see EPRI's 2017 report *Cyber Security Metrics for the Electric Sector,* https://www.epri.com/#/pages/product/3002011685/?lang=en.

4.1 Establish a Timeframe

To ensure that performance indicators are actionable and timely, the commission will want to establish a timeframe with milestones for achieving strategic goals. Devising a timeline helps the commission maintain its course toward accomplishing the established objectives of its strategy. As in all good practices, the following items should be considered:

- **PUCs will want to recognize their limitations,** remaining realistic and pragmatic as they establish a timeframe for developing and implementing their individual strategy. Considerations typically include:
  - > Technical considerations, such as technological expertise, response capabilities, or deployable resources; and
  - > Managerial considerations, such as staffing capacity, personnel workload, and third-party vendors.
- In addition to other milestones, PUCs will at least want to establish timelines for the development of the commission's strategy and for engagement with the utilities it assesses.
- Development of a commission-specific cybersecurity strategy varies depending on the scope of the strategy, and may take a number of months or even years to complete.
- As a rule of thumb, the timeframe for cybersecurity strategy implementation is typically around five years, depending on the strategy's scope and the availability of commission resources, which aligns with strategic planning best practices used at the federal level and from major businesses.
  - > This proposed timeframe is long enough to achieve progress on complex goals, while still being relevant to the changing cybersecurity landscape. After this period, the strategy should be re-evaluated and expanded upon, as discussed in Section 9.
  - > A strategy with a larger scope, or a commission with fewer resources, may be better suited with a longer timeline as the strategic goal will be slow to manifest itself.
  - > A strategy with a smaller scope, or a commission with more available resources, could accommodate a shorter timeframe for achieving objectives as the strategic goal will be more explicit and faster to manifest itself.
- **PUCs will want to determine frequency of engagement with utilities**, which will depend on the scope and objectives of their individual strategy.
  - > Organizing annual formal engagements between PUCs and utilities is typically the minimum initiation for establishing a relationship, though some commissions engage more frequently.

5. Identify Key Stakeholders

This section identifies all relevant cybersecurity stakeholders, as well as define the relationships that the commission will have with and roles played by such organizations and agencies. These internal and external stakeholders include federal, state, local, and private-sector entities. Stakeholder mapping helps address and minimize any uncertainty, areas of overlap, and gaps in regulatory jurisdiction, and reinforces the responsibilities of the regulator's cybersecurity role.

Key stakeholders in a cybersecurity strategy include **law enforcement agencies, technical services and equipment vendors, the intelligence community, the Governor's office, state emergency management agencies/offices, state energy offices, and neighboring utilities**. These key stakeholders have a pivotal part in developing and implementing cybersecurity safeguards, with responsibilities varying across jurisdictions. By clearly outlining what those roles and responsibilities are, the commission can improve internal processes, establish accountability, and increase preparedness.

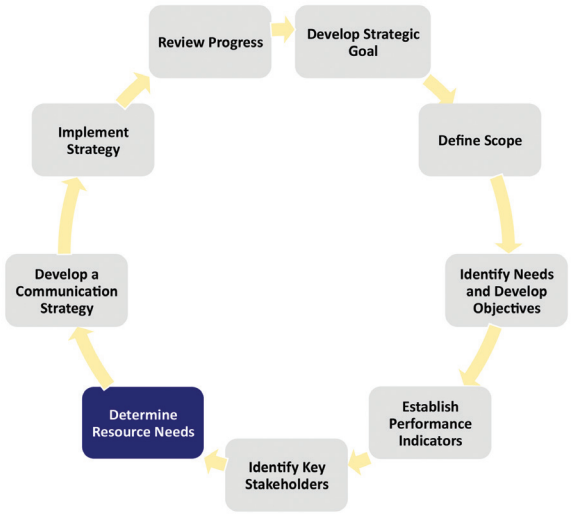
Defining roles is specific to each regulatory commission and is based on their circumstances. For example, utilities engaging with third-party vendors and/or contractors will want to operate under the "principle of least privilege" and will want to ensure that external parties are managing their own cybersecurity landscape by using a "zero-trust" model to avoid third-party penetration, while also benefiting from any of their lessons learned.[13,14] Additionally, large, interstate utilities will likely have a wider range of stakeholders and operate under a greater number of authorities. For instance, utilities that operate generation and transmission infrastructure are regulated at the federal level and fall under the jurisdiction of FERC. However, any local distribution that they operate would be managed at the state level by the PUC.

Although it is important for commissions to holistically recognize a network of stakeholders, it is especially recommended for each PUC to assess the aforementioned stakeholder groups to identify which of them will ultimately provide essential capabilities to support the PUC in its effort to achieve its strategic objectives.

13 The "principle of least privilege" refers to granting only the minimum necessary rights of access to a resource. For more information, see US-CERT's publication *Least Privilege* accessible here: https://www.us-cert.gov/bsi/articles/knowledge/principles/least-privilege.

14 The "zero-trust" model refers to the concept that all incoming information and data packets must be verified, regardless of whether the come from an internal or external network. For more information, see NIST's publication *Developing a Framework to Improve Critical Infrastructure Cybersecurity* accessible here: https://www.nist.gov/sites/default/files/documents/2017/06/05/040813_forrester_research.pdf.

6. Determine Resource Needs



This section identifies the amount of time and level of resources the commission is willing to invest in cybersecurity. Some points to address may include how the commission initially plans to approach cybersecurity concerns, and which staff at the commission will focus on cybersecurity.

Each commission will want to determine the types of resources necessary to achieve their cybersecurity strategy's desired level of preparedness, assessing the extent of investment that will be required. To that end, commissions could consider the following:

- What level of staff time should commissions dedicate to learning about cybersecurity and developing skills necessary to achieve stated goals?
- Do staff need to become subject-matter experts, or is it enough that they are familiar with the language and terms?
- Do any staff need one-time training, ongoing training, certifications, or security clearances?
- Does the commission have enough personnel to build and maintain relationships with utilities?

Answers to these questions will vary for each commission depending on their priorities and objectives. In order for a cybersecurity strategy to comprehensively recognize and address all resource priorities and objectives, it must recognize the commission's organizational structure, including funding and personnel capacity, as well as the cyber team personnel's qualifications and offerings.

6.1 The Commission

Although technical knowledge is important to a cybersecurity strategy, the approach and focus should be cross-cutting and involve several departments within a commission. At its core, effectively managing cybersecurity is about process and collaboration for commissions.

To prepare its cybersecurity strategy, the commission will want to:

- **Identify the personnel** who will engage in cybersecurity efforts on behalf of the commission.
  - > Given collaboration is paramount for cybersecurity, it is important to assign the right staff or commissioners to interact and build trust with their utility counterparts on sensitive issues—it is unlikely to be the same staff who engage with utilities in other, less-collaborative contexts.
- **Establish dedicated funding** for the cyber team to function effectively.
- **Develop a working group** with people who can bridge interest groups and understand how to manage both operational processes and competing interests.
  - > States have found value in cybersecurity working groups that have an inter-departmental makeup.
- **Institutionalize cybersecurity defenses** through executive support, creating a culture of safety, security, and awareness and focusing on the human aspect of cybersecurity as vulnerabilities can come in the form of uninformed staff, not just technological weakness.

- **Identify a champion** within leadership who can help drive the strategy development process, as well as a few other staff in different functional areas of the commission.
- **Incorporate both technical and policy expertise** to ensure efficiency from both an operational and administrative perspective.

The specific organization and structure of existing working groups have varied widely, and commissions should choose a structure that best fits their priorities and organizational makeup, identifying a single commissioner to own and drive the process.

Although a commission will want to allocate staff and funding for cyber teams, the levels of both vary widely by commission.

For an entry-level cybersecurity role, a commission may want to consider the following qualifications:

- A degree in engineering, computer science, or a related field.
- Academic or professional cybersecurity experience, preferably with a focus in industrial control systems or power systems.
- Working knowledge of cybersecurity principles.
- Relevant professional security certifications preferred (e.g., SANS Institute or International Information Security System Certification Consortium).
- Ability to obtain a security clearance.

Qualifications that commissions may want to consider for advanced cybersecurity roles include:

- An advanced degree in electrical engineering, computer science, or a related field.
- Several years of professional cybersecurity experience, preferably within a regulated industry.
- Working knowledge of NERC CIP standards.
- Relevant professional security certifications (e.g., SANS Institute or International Information Security System Certification Consortium).
- Security clearance

Due to a wide-spread shortage of qualified cybersecurity personnel, it is essential to find a way to incentivize those who are qualified to gravitate toward the commission-level positions, rather than going to competitors, including their own utilities. Cybersecurity in the utility sector is especially complicated because of the convergence of IT and OT—although the technologies may use the same hardware, the application of cybersecurity techniques is different, so expertise is not automatically transferrable from one to the other. For this reason, commissions (or utilities) may need to bolster their internal cybersecurity training practices.

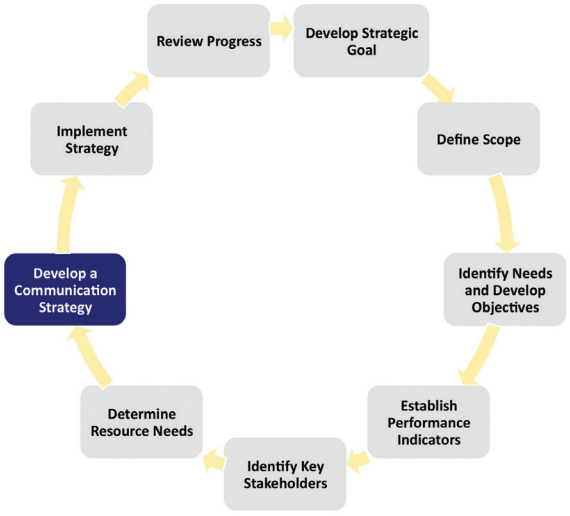
Rather than hiring new staff, regulators can also choose to build the capacity of existing staff members to take on cybersecurity roles and responsibilities in addition to their current duties. As such, cybersecurity roles do not necessarily need to be full-time dedicated positions, but it is essential to identify the staff responsible for cybersecurity functions.

Computer experts are generally comfortable discussing the technical aspects of cybersecurity. However, financial and regulatory specialists also must be able to understand the language of cybersecurity and the corresponding issues to evaluate utilities. As such, commissions will want to ensure that technical, financial, and regulatory specialists are talking to and understanding each other. Although each group has differing interests, goals, and concerns, developing a level of consistent communication and understanding across them will allow for more comprehensive and effective planning and implementation.

Assigning the right personnel to lead a PUC's engagement with utilities on cybersecurity is an important decision. The commission will want to determine whether it is better to assign cybersecurity roles and responsibilities to individuals who already engage with utilities on other issues or to identify new personnel for the job. At the federal level for example, FERC splits its Office of Enforcement from its Office of Energy Infrastructure Security to ensure open cooperation from utilities. Communication and sharing of actionable information are key, and commissions will want to ensure that they select people who are best suited to build collaborative relationships and work effectively with their counterparts at utilities.

7. Develop a Communications Plan

This section identifies the types of communications a commission expects to have with utilities and stakeholders. This includes everyday communication guidelines, mandatory reporting requirements and responsibilities for the utilities, and incident communications. Also outlined would be the process by which commissions will interact with their utilities when handling or discussing sensitive information.



Effective communication—both within a commission and between regulators and utilities—is essential to a cybersecurity strategy. As commissions develop their cybersecurity strategies, they will also want to determine internal and external communications plans for cybersecurity that may include differences from their standard communications protocol. These procedures include templates for internal emails and letters, as well as external press releases and talking points. **Appendix B** includes sample templates for internal and external communications.

Internally, commissions will want to develop a communication plan that allows different departments representing varied interests to convene and discuss their priorities and concerns regarding various issues related to cybersecurity. As with other issues, different departments within a commission will have different priorities for cybersecurity. To ensure understanding and avoid significant pushback from finance departments, IT staff may want to prepare clear explanations of the cost-benefit analysis for cyber investments to justify the resource expenditure. It is important for groups with competing interests within a commission to voice their priorities and concerns to develop a more complete understanding of the risks posed by cybersecurity and the options available in developing a commission's strategy.

Externally, commissions should determine the means and methods for communication that are most effective for them given their relationships with utilities. As mentioned earlier, successful commissions have found that a different approach is needed in communicating and engaging with utilities on cybersecurity. Cooperation and engagement are keys to effective security, and they are crucial for the relationship between regulators and utilities in addressing cybersecurity. Successful PUCs have found that, to develop an effective working relationship with utilities, it may be necessary to develop a communication plan around staff that do not interact with utilities regarding other issues. Instead, designating staff that are involved in the cybersecurity working group, such as technical or policy staff, to communicate with their counterparts at utilities can create a more collaborative environment and increase trust between stakeholders. Opening different pathways for communication sends a message to utilities that regulators want to engage in a productive relationship, apart from more contentious issues.

Levels of engagement with different stakeholders will vary and PUCs will want to determine which entities are most connected to the success of the strategic goal, and how they could best collaborate and communicate with them. For example, the Indiana Utility Regulatory Commission invites the Indiana Department of Homeland Security, the Indianapolis office of the FBI, the Indiana National Guard, and the Governor's Executive Council on Cybersecurity to cybersecurity briefings it holds with utilities.[15]

15 Verified via email with Commissioner Sarah Freeman, September 11, 2018.

Additionally, PUCs will want to ensure that members of their internal organizational structure are included during their outreach and are aware of the policies and procedures outlined in the cybersecurity strategy. Internal stakeholders that PUCs will want to keep informed include **executive leadership, regulatory and security personnel, legal departments, and others**.

Establishing a forum for stakeholder group discussions is an opportunity to identify key partnerships for the strategy. The Mid-Atlantic Conference of Regulatory Utility Commissioners convenes a stakeholder group on a quarterly basis to, among other things, exchange information and facilitate informative discussion on regulatory, legislative, and policy interests.[16]

During a cybersecurity incident, communication should focus on the estimated time to restoration/recovery from attacks. Determining a containment date for each breach not only helps to manage expectations for stakeholders, but it also sets a baseline from which they can learn lessons, evaluate performance, and establish an improvement plan made-up of corrective actions. This review cycle is discussed in Section 9.

7.1 Handling and Communicating Sensitive Information

Commissions will need to identify how they will interact with their utilities with regard to sensitive information. This includes how utilities can or will brief regulators, how often and what kind of communication the PUC prefers, who will be part of reviews, and how the utilities will report incidents. Open government "sunshine" laws allow citizens access to meetings of commissions; however, more than half of state legislatures have created exemptions to restrict the release of sensitive information, protecting the privacy and national security interests of critical infrastructure operators.[17] Commissions will want to be familiar with their particular state laws and any exemptions as this may affect the type, extent and means by which utilities will be willing to share information.

Commissions should critically assess their relationships with utilities and their capacity to obtain information through these relationships. Information exchange and information management is essential to success. The commissions with the most effective cybersecurity strategies have found that, due to the highly sensitive nature of cybersecurity, regulators and utilities must engage differently on cybersecurity matters than they might on other issues. PUCs serve a fundamental role in safeguarding such sensitive information and need to ensure that their cybersecurity strategy accounts for all necessary procedures to do so, which may include adopting new encryption methods and limiting personnel access.

Utilities are often concerned with how the information they share will be protected. As a result, commissions have consistently found informal communications and reporting practices to be the most effective approach to working with utilities toward greater cybersecurity, as they allow for more transparent discussion and information sharing. However, establishing a formal process for reporting is essential for timely sharing of information. As such, regulators and utilities must agree to some standards on what critical information must be protected. Another measure to consider is not just protecting information when it has been shared but ensuring the method through which the information is shared is secure. By establishing policies for communication network security, including device password requirements and encryption of sensitive information, PUCs may be able to mitigate some of their utilities' concerns.

16 Mid-Atlantic Conference of Regulatory Utility Commissioners. *About MACRUC* (n.d.), http://macruc.org/About/.

17 For more information on open government laws and state exemptions, see National Conference of State Legislatures' 2018 publication *Open Government Laws and Critical Energy Infrastructure,* http://www.ncsl.org/research/energy/open-government-laws-and-critical-energy-infrastructure.aspx.

Connecticut Public Utilities Regulatory Authority (PURA) Case Example[18]

Connecticut PURA regulators consider confidentiality important to the success of their cybersecurity strategy. They hold annual meetings with their utilities to review cybersecurity defense with no records and no notes allowed. Participants at the annual meeting also enter into non-disclosure agreements. Connecticut PURA's cybersecurity strategy details how reporting and communications should take place, which are broadly summarized in the bullet points below:

- An annual report is released regarding the state of cybersecurity defense capacity at state electricity, natural gas, and major water utilities;
- Given that no notes and records are kept (in addition to the non-disclosure agreements), regulators and utilities agreed that there would be significant disclosure during the meeting;
- Regulators and utilities will come to an agreement on a summary report of the annual meeting afterwards. The summary report will not cite results or sensitive information for any individual utility; and
- The summary report will then be submitted as a final report to the Governor, legislature, and Consumer Counsel outlining the high-level results of the annual meeting;
- The agreement provides that there will be four State of Connecticut participants; and
- Utilities may select the standard by which to measure their progress in cybersecurity defense. All four utilities, acting separately, have chosen to use the Cybersecurity Capabilities Maturity Model (C2M2).

18 Art House (Connecticut Chief Risk Officer), email message to Matthew Acho (NARUC), September 13, 2018.

8. Implement Strategy

This section outlines the process for accomplishing the strategic goals and objectives laid out in the cybersecurity strategy. Whereas the previous sections outline what the plan entails and why it is important, this section should detail the specific steps of how the strategy will be implemented.

Once the cybersecurity strategy has been developed, PUCs need to ensure that the strategy is proactively implemented and **overseen by a formal project manager**. A typical implementation and monitoring process will include:

- Initializing change processes;
- Evaluating milestones for success or concerns;
- Implementing any necessary ad hoc revision; and
- Finalizing processes and reporting data for evaluation purposes.

While developing this implementation process, commissions should balance the costs of driving risk-based cybersecurity measures (e.g., time, personnel, training) with the potential impacts—financial and otherwise—to ensure that they make the greatest use of resources and have the most impact for consumers. Additionally, commissions should have a general sense of the severity of threats to its jurisdiction, the likelihood of an attack, and work with stakeholders to determine the cost of implementing mitigation efforts before determining how to implement their strategy. For instance, a small utility with limited resources may find more value in providing basic training on cyber hygiene for its employees than investing in expensive new firewall software or firmware.[19]

Some type of advocacy on the part of the commission is often necessary, as utilities often think that any issues regulators do not overtly encourage will not be allowed. Finding the right balance, however, is important so that utilities do not see this as an invitation for profligate spending. As in nearly every decision regulators must make, encouraging prudent investment and cybersecurity measures is the best approach.

19 For more information, see NARUC's publication *Risk Management and CI Protection,* https://pubs.naruc.org/pub/D10AF40A-AD04-3983-7421-9FBE970D87F3.

Connecticut PURA Case Example[20]

The 2014 Connecticut PURA strategy produced a 2016 action plan concurred by both PURA and the participating utilities. That action plan has produced two annual cybersecurity reviews. The 2016 framework reflected the following:

- Recognition that threats posed by potential cyber breaches and the state of cybersecurity in Connecticut's public utilities were of concern to PURA, the Governor, General Assembly, Consumer Counsel, and to the general public. Cybersecurity issues could no longer be exclusively a matter of company confidentiality, and some form of annual assessment and understanding of the state of cyber defense capabilities was necessary;
- Recognition that reporting on critical infrastructure cybersecurity needed to include prevention (e.g., corporate culture, education, and training); defense systems including firewalls, software, the use of consultant services, and trade association assistance; and plans for response and recovery from possible damage after a breach; and
- That Connecticut would proceed with a collaborative approach of annual reviews between state authorities and utilities using standards selected by the utilities that would protect confidential information. The resulting report would be a consensus document cleared and approved by all participants.

As commissions consider cybersecurity investment strategies, there are not yet industry-wide established practices. However, areas of investment that commissions can expect utilities to focus on include:

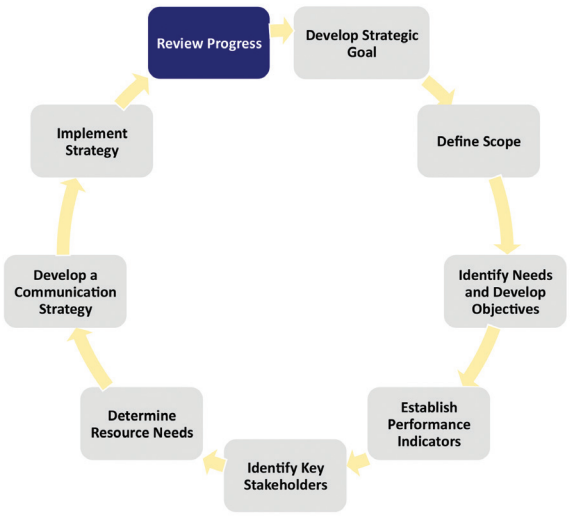
- Cybersecurity drills, training, and exercises as well as insider threat programs to increase the culture of cybersecurity;
- Resources for hiring cybersecurity professionals;
- Costs associated with developing/maintaining emergency response, disaster recovery, and business continuity plans; and
- IT/OT asset management systems, and data loss and leak prevention, defensible deletion of data to reduce threat space, mobile security, and cloud security systems.

Historically, utilities have invested in industrial control systems (ICS) under the expectation that the technology will last several decades and will not necessarily be subject to cybersecurity attack. However, the interconnectivity of IT and OT requires that ICS systems operate under the assumption that the interconnected IT could be corrupted and should be updated regularly to meet the standards necessary to keep the systems secure. The complexity of the interconnectivity between IT and OT can make assessing vulnerabilities challenging, and so often simpler network configurations are often easier to secure.

20 Art House (Connecticut Chief Risk Officer), email message to Matthew Acho (NARUC), September 13, 2018.

9. Review Progress

This section outlines a process for regularly updating the commission's cybersecurity strategy; addressing findings related to the performance measures; and capturing and incorporating corrective actions, improvement planning, and lessons learned.



Evaluation and improvement are a significant part of the cybersecurity strategy's lifecycle. Evaluation of the performance indicators is the first step to reviewing progress, but consideration should be given to establishing a regular process for reviewing and updating the cybersecurity strategy. Additional testing procedures and tools can be used to monitor strategy effectiveness and allow commissions to evaluate their progress toward their objectives. The result of evaluation can be used to maintain the parts of the strategy that are effective and adjust the components that are not achieving the desired results.

Consideration also should be given to establishing a process whereby utilities comprehensively analyze its management of a cybersecurity incident, gather evaluation materials and prepare an **"after-action report"** (AAR) following the event. The AAR also would incorporate lessons learned and define an improvement plan comprised of corrective actions. This utility-specific report may provide the commission with useful information regarding how the event happened, what actions the utility could have been taken to prevent the incident from taking place, and what steps the commission and utility can take to address the vulnerabilities exposed. **(**See Section 7.1 – Handling Sensitive Information.) For additional guidance on structuring an AAR, commissions and utilities can adapt the Homeland Security Exercise and Evaluation Program (HSEEP) AAR Template to address real-world incidents.[21,22]

The NIST CSF suggests that strategies should be adaptive, based on previous and current cybersecurity activities. Strategies and processes can be continually improved by incorporating lessons learned into future activities. Through this cycle of evaluation and improvement, commissions can incorporate evolving threats and changing technologies into their cybersecurity strategies as they emerge.

21 Federal Emergency Management Agency. *Homeland Security Exercise and Evaluation Program (HSEEP) After Action Report/Improvement Plan Template,* 2013, https://preptoolkit.fema.gov/documents/1269813/1269865/AAR-IP_Template_Apr-13-2_Clean.docx/d754c3f4-bf45-42ed-aec9-d1a7370c0e57.

22 Federal Emergency Management Agency. *Homeland Security Exercise and Evaluation Program (HSEEP),* 5-5, 2013, https://www.fema.gov/media-library-data/20130726-1914-25045-8890/hseep_apr13_.pdf.

Appendix A. Reference Documents and Resources

This appendix highlights some of the key cybersecurity resources available for commissions to reference when developing and implementing cybersecurity strategies.

North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP)
https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

The NERC CIP standards are a set of requirements designed to secure the assets required for operating North America's Bulk Electric System. NERC's CIP efforts include standards development, compliance enforcement, dissemination of critical information, and raising awareness regarding key security issues. The committee consists of industry experts and reports to NERC's board of trustees in the areas of cybersecurity, physical, and operational security.

National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

The NIST CSF consists of industry standards and best practices to help organizations reduce and better manage their cybersecurity risks. The framework was developed with a focus on industries vital to national and economic security, including energy, banking, communications, and the defense industrial base. It has since proven flexible enough to be adopted voluntarily by large and small companies and organizations across all industry sectors, as well as by federal, state, and local governments. It uses common language to address and manage cybersecurity risk in a cost-effective way, without placing additional regulatory requirements on businesses.

Department of Energy (DOE) Cybersecurity Capability Maturity Model (C2M2)
https://www.energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf

The C2M2 is a voluntary evaluation process utilizing industry-accepted cybersecurity practices that can be used to measure the maturity of an organization's cybersecurity capabilities. The C2M2 is designed to measure both the sophistication and sustainment of a cybersecurity program. The goal of the C2M2 is to develop a logical understanding and measurement of the policies, processes, and procedures involved in the development of an organization's cybersecurity posture. The model provides maturity indicator levels (MILs) designed to discuss an organization's operational capabilities and management of cybersecurity risk during both normal operations and times of crises.

Electric Power Research Institute (EPRI) Cyber Security Technical Assessment Methodology: Vulnerability Identification and Mitigation
https://www.epri.com/#/pages/product/3002008023/?lang=en

The EPRI Cyber Security Technical Assessment Methodology provides an efficient "bottom up" method to assess and mitigate cybersecurity vulnerabilities in equipment used in modern power plants. This report can be used by design engineers and cybersecurity specialists with utility and vendor organizations to assess plant digital assets in a cost-effective and sustainable manner. Utilities and vendors can apply the Technical Assessment Methodology at any point in the asset's lifecycle, from inception, through the supply chain, to the operational phase.

Appendix B. Communication Templates

Appendix B provides communication templates that commissions can adapt to convey information related to a cyber breach clearly and transparently to internal commission employees and to external stakeholders.

Internal Communication: PUC "All Users" Email – Utility Incident

Dear PUC employees,

On [date], the PUC learned of a security incident involving [Utility X]. As this time, we do not believe any employee or utility data on any PUC systems has been compromised. [Utility X] is working with law enforcement and other government agencies to mitigate any further damage.

The Commission is [aware/not aware] of [a/any] compromise of [Utility X's] customer data. If asked, we instruct customers to contact [Utility X] at [phone number] for more information on the issue and any possible breach of their data. Due to the sensitive nature of this incident and the potential for law enforcement action, we cannot provide any further details.

Our Emergency Response staff and other key personnel are working with the utility and our state and federal partners to limit the damage to customers. We plan to conduct a thorough review of this incident to reduce the risk of a similar incident in the future.

The Commission employs multiple layers of security to protect our networks and systems. We offer the following cyber tips to keep in mind, to help protect your personal and Commission-related information:

- Create a strong and long password with a combination of uppercase and lowercase letters, numbers, and symbols, and change it frequently;
- Do not share your password with anyone or store it in a public place;
- Do not leave your computer or smart phone open and unlocked when you leave your desk, or when travelling in public;
- *Do not click a link or open an attachment in an email from a sender that you do not recognize and call the Help Desk at [NUMBER] to verify anything that raises concern or suspicion;
- Do not plug in your cell phone, a non-Commission-issued thumb drive, or any another item with a USB plug into a Commission computer; and
- Do not perform sensitive, Commission-related, or personal financial transactions off site on an unsecured network, such as a hotel or coffee-shop Wi-Fi network.

If you believe your work computer or a Commission system has been affected by this event in any way, please contact [MIS contact] at [phone number] or [email].

We will provide any further updates as necessary.

Example Incident:

External Utility Security Incident/Breach – loss of personally identifiable information (PII)

Key message 1: We are aware that an incident occurred at [Utility X].

- We are in close communication with the affected utility.
- We are receiving regular updates from the utility.
- We are working with the utility and other relevant state and federal agencies to determine the cause and impact of this incident.

Key message 2: We are actively monitoring the incident.

- We are monitoring the impact on consumers
- We are monitoring the safety and reliability of the utility system.
- We are encouraging the use of all available resources to address this incident and restore service as quickly as possible.

Key message 3: We want to ensure that this does not happen again.

- We plan to conduct a thorough review of this incident.
- Based on the findings, we will take appropriate measures to reduce the risk of a similar incident occurring in the future.
- *[if an inside job]* We cannot comment on whether any employment or disciplinary actions will be taken.

Secondary messages

- The PUC requires regulated utilities to develop and use cybersecurity plans.
- We encourage information sharing and cooperation between utilities to improve our defense against cyberattacks.
- We promote and support best practices and work diligently with other agencies and utilities planning for multi-agency incidents.

Media statement 1

"The safety and reliability of utility systems is a major concern for the PUC – and we work closely with utilities companies, other state and federal government agencies, law enforcement, emergency-response organizations, and other concerned parties to address threats to our utilities' infrastructure. The Commission has underscored the importance of collaboration among agencies and utilities to enhance our preparation and response to any attack on our essential systems, and will continue working with all parties involved in this incident to help our communities recover as quickly as possible."

Appendix C. Acronyms

C2M2	**Cyber Capability Maturity Model**
CIP	Critical Infrastructure Protection
CSF	Cybersecurity Framework
EPRI	Electric Power Research Institute
FERC	Federal Energy Regulatory Commission
GIS	Geographic Information System
HSEEP	Homeland Security Exercise and Evaluation Program
ICS	Industrial Control Systems
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
IT	Information Technology
NARUC	National Association of Regulatory Utility Commissioners
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
OT	Operational Technology
PII	Personally Identifiable Information
PSC	Public Service Commission
PUC	Public Utility Commission
PURA	Public Utilities Regulatory Authority
SCADA	Supervisory Control and Data Acquisition
SMART	Specific, Measurable, Attainable, Relevant, and Timely
UTC	Utilities and Transportation Commission

Appendix D. Glossary

Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Critical Assets	Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the bulk electric system.
Critical Infrastructure	The assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof.
Cyber Asset	Programmable electronic devices, including the hardware, software, and data in those devices.
Cybersecurity Incident	A malicious act or suspicious event that: 1) compromises, or was an attempt to compromise, the ESP or PSP, or 2) disrupts, or was an attempt to disrupt, the operation of a BES cyber system.
Impact	Damage to an organization's mission and goals due to the loss of confidentiality, integrity, or availability of system information or operations.
Incident	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of a system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
Information Security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability.
Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. [Note: information systems also include specialized systems such as industrial/process controls systems, telephoneswitching and private branch exchange (PBX) systems, and environmental control systems.]
Information Technology (IT)	A discrete set of electronic information resources organized for collecting, processing, maintaining, using, sharing, disseminating, or dispositioning information.
Malware	A malicious software program that can infect your computer or other electronic devices, causing harm. Examples of malware are viruses, worms, Trojans, and spyware.
Network (computer network)	A collection of hardware components and computers interconnected by communication channels that allow for the sharing of resources and information
Resilience	Robustness and recovery characteristics of utility infrastructure and operations, which avoid or minimize interruptions of service during an extraordinary and hazardous event.

Risk	Measure of the extent to which an entity is threatened, typically a function of: (1) the adverse impacts that would arise if the circumstance or event occurs; and (2) the likelihood of occurrence. Security risks related to information security arise from the loss of confidentiality, integrity, or availability of information or information systems with potential adverse impacts on operations.
Risk Management	The process of conducting a risk assessment, implementing a risk mitigation strategy, and employing techniques and procedures for the continuous monitoring of the security state of the information system. Risk management incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place – synonymous with risk analysis.
Risk Severity	A combination of the likelihood of a damaging event actually occurring and the assessed potential impact on the organization's mission and goals if it does occur.
Sensitive Information	Information of which the loss, misuse, unauthorized access, or modification could adversely affect the organization, its employees, or its customers
Smart Grid	Modernization of electricity infrastructure through added technology, allowing the grid to gather and store data, to create a "dialogue" between all components of the grid, and allowing for automatic command and response within the function of the grid.
Supervisory Control and Data Acquisition (SCADA)	Systems that monitor and control industrial, infrastructure, or facility-based processes, such as automatic (and often remote) control devices. They include simple functions such as "on/off" and sensor capability, communications capability, and the human-machine interface (HMI) that connects them to people operating the system.
Supply Chain	A network between a company and its suppliers, to produce and distribute a product. The supply chain refers to the organizations, people, and other resources involved in getting the product or service from the supplier(s) to the customer.
Threat	The potential for an actor, circumstance, or event to adversely affect assets, people, or organizational operations of the system.
Traffic	The information moved over a communication channel, including the quantitative measurement of the total messages and their length, expressed in CCS or other units, during a specified period.
Virus	An unwanted computer program that replicates itself and spread from one computer to another. "Virus" is often used incorrectly to refer to malware, including adware and spyware programs, which do not have a reproductive ability.
Vulnerability	A specific weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.


NATIONAL ASSOCIATION OF REGULATORY UTILITY COMMISSIONERS
DEDICATED TO PUBLIC SERVICE
1889