AMERICAN PUBLIC POWER ASSOCIATION
Powering Strong Communities

Public Power Cybersecurity Roadmap

APRIL 2019

Acknowledgment

This material is based upon work supported by the Department of Energy under Award Number(s) DE-OE0000811.

Disclaimer: This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

The American Public Power Association (APPA) thanks the members of the Cybersecurity Roadmap Advisory Council for their essential role in developing this roadmap. The Council developed this roadmap to provide public power utilities with clear strategies to improve their cybersecurity and create a compelling business case for security investment to improve resilience. We thank them for taking the time to attend multiple workshops and conference calls to discuss their experiences, needs, and practices. All members of the Council deserve thanks and appreciation for their contributions. Members of the Council included:

Bernie Acre, Bryan Texas Utilities
Cheryl Anderson, Florida Municipal Electric Association
Bill Berry, Owensboro Municipal Utilities
Randy Black, Norwich
David Boarman, Owensboro Municipal Utilities
Kenneth Carnes, New York Public Power Authority
Jack Cashin, American Public Power Association
Chris Ching, American Public Power Association
Jason Christopher, Axio Global
Phil Clark, Grand River Dam Authority
Jim Compton, Burbank Water and Power
Josh Cox, City of Westerville
Adrian de la Cruz, Kerrville Public Utility Board
Colin Hansen, Kansas Municipal Utilities
Alex Hofmann, American Public Power Association
Tony Holstein, Gainesville Regional Utilities
Jennifer Keesey, Northwest Public Power Association
Branndon Kelley, American Municipal Power, Inc.
Christopher Kelley, Beam Reach Consulting Group
Lindsay Kishter, Nexight Group
Mike Klaus, Central Nebraska Public Power & Irrigation Dist.
Kurt Knettel, New Braunfels Utilities
Matt Knight, Owensboro Municipal Utilities
Melvyn Kwek, Guam Power Authority
Doug Landoll, Beam Reach Consulting Group
Matt Lee, Platte River Power Authority
Chris Lindell, Beatrice City Board of Public Works
Carter Manucy, Florida Municipal Power Agency
Robby McCutcheon, Kerrville Public Utility Board
Nathan Mitchell, American Public Power Association
Rob Morse, Platte River Power Authority
Michelle Nall, Glendale Water & Power
Erik Norland, Chelan Public Utility District
Sam Rozenberg, American Public Power Association
Steve Schmitz, Omaha Public Power District
Chad Schow, Franklin Public Utility District
Ken Simmons, Gainesville Regional Utilities
Scott Smith, Bryan Texas Utilities
Howard Wong, Glendale Water & Power
Giacomo Wray, American Public Power Association

About the Association

The American Public Power Association is the voice of not-for-profit, community-owned utilities that power 2,000 towns and cities nationwide. We represent public power before the federal government to protect the interests of the more than 49 million people that public power utilities serve, and the 93,000 people they employ. Our association advocates and advises on electricity policy, technology, trends, training, and operations. Our members strengthen their communities by providing superior service, engaging citizens, and instilling pride in community-owned power.

Table of Contents

Executive Summary

The cybersecurity landscape is complex and the threats posed to public power are real. Cyberattacks range in magnitude and impact and can occur in many forms, such as phishing attacks through employees' emails and gaining backdoor access to a utility's IT network through third-party vendors. These threats originate from a spectrum of malicious sources, ranging from individual actors to foreign powers seeking to disrupt critical infrastructure. Establishing and managing a cybersecurity program can be difficult with complex IT/OT systems and limits on technical staff, however, it is a necessary precaution against cyberattacks of any kind.

The Public Power Cybersecurity Roadmap is a strategic plan designed to help public power utilities develop a stronger, sustainable state of security that is continually monitored and improved upon. To ensure accuracy and applicability, the American Public Power Association developed the Roadmap using input from public power utilities' security, information technology, operational technology, and leadership experts.

The Roadmap builds on the Public Power Cybersecurity Scorecard, a tool to assess an organization's cybersecurity operations and practices. Using findings from the Scorecard, the Roadmap facilitates a path to an improved state of cybersecurity. It breaks down how to approach the broad and sometimes intimidating scope of cybersecurity practices into four distinct, manageable stages. As a utility moves through the Roadmap, the Scorecard can act as a useful standard by which to monitor and measure improvements to organizational cybersecurity practices.

The Roadmap's four stages help utilities to set and achieve meaningful program goals.

STAGE 1: EVALUATE internal and external factors influencing most pressing cybersecurity issues and identify two to three promising opportunities to target. In this stage, public power utilities must gain sponsorship and leadership support to bolster authority and secure funding for the cybersecurity initiative. Utilities should define the roles of leadership and relevant organizational divisions, identifying a member of senior leadership to act as the sponsor for the project. The sponsor should be aware of and understand applicable regulations, laws, and standards potentially impacting the cybersecurity program. The utility should also develop a list of stakeholders who have an interest in or can influence the outcome of a project. Having identified sponsors, stakeholders, regulations and standards, a public power utility must conduct an initial risk-based assessment to define the current security posture and determine necessary means for achieving the desired future state. Such activities include identifying a target profile (goal), gaining support from senior management, establishing a risk management plan, and establishing a project-based approach to cybersecurity. The Public Power Cybersecurity Scorecard can guide many of these activities.

STAGE 2: FORMULATE a project-based plan to improve cybersecurity in two to three identified areas, being sure to define: a cybersecurity strategy, a clear schedule, data and metrics, a resource management plan, and the role of project lead. The overall project management plan should include: a project scope, a communications plan, a schedule, a budget, and a risk plan. A public power utility should review information technology (IT), operational technology (OT), and security organization workforce by defining the impacted roles and responsibilities of personnel within the utility. This stage also includes standing up processes to check key staff and vendor backgrounds to help a utility reduce its exposure to cybersecurity threats. Distinct management training, technical staff training, and non-technical staff training can prepare individuals to fulfill particular needs within the organization.

STAGE 3: ACTIVATE the project-based plan. This entails conducting the steps outlined in the plan, which might include installation of tools and systems used to monitor and secure IT and OT systems, as well as implementation of new security policies and procedures. Public power utilities should adopt policies and practices that both the utility and individual personnel support to enable a culture of organizational security. Utilities can implement rewards to recognize good cybersecurity practices, as well as sanctions to provide corrective measures when practices are not executed. Utilities should also prepare for an incident response by putting in place the tools, practices, and communications to be deployed should an event occur. The Public Power Cybersecurity Incident Response Playbook facilitates the creation of an effective incident response for a utility. Implementing a series of risk management practices is key to performing advanced preparation for a cyber incident. Crucial steps for detecting and responding to cybersecurity incidents include: containing the incident, determining the impact the incident has on the utility, monitoring whether the incident is escalating, and reporting the incident. In this stage, utilities should develop a strong strategy for communicating with internal and external stakeholders to maintain buy-in and adherence to new practices. Accurate and frequent communication with customers and other audiences is necessary for building durable relationships that can withstand crises.

STAGE 4: INTEGRATE practices defined by the plan into the operation of the organization and make them a part of the organization's culture. If the project-based cybersecurity plan involved implementation of tools and systems to monitor and secure IT and OT, ensure these new tools are monitored regularly. Perform periodic tests and audits of these systems and conduct regular updates and maintenance. Share new processes and procedures with those responsible for maintaining them and those who must follow them. Have sponsors continue to reinforce the message of good cybersecurity hygiene. Consider performing security audits against new processes to ensure staff remain vigilant within the rewards and sanctions systems. Finally, revisit the Public Power Scorecard to reassess the organization's cybersecurity maturity and to prepare for further evaluation (and return to stage 1).

The Roadmap serves as a guide. This document provides insight into valuable and effective strategies for improved cybersecurity, but the success of any project lies in its execution. By providing a tested, collaborative baseline on which to build a cybersecurity program, the Association hopes that public power utilities can chart a path to an improved state. Tools and resources to engage peers and collaborate with the Association and subject matter experts are included in this document. The threat of a cyberattack may be very real, and the scope of cybersecurity may be daunting, but by working together we can improve the cybersecurity of the entire public power sector and continue to provide the best services to our communities and customers for years to come.

Introduction

Public power utilities face many evolving challenges. Prominent among these is the threat of cyberattack and the corresponding duties of developing and executing an effective cybersecurity program. Rapidly evolving technologies at all operational levels present potential targets for attack and substantial liabilities if compromised. Although organizational leadership is ultimately responsible for executing the strategy and securing the resources to appropriately address cybersecurity threats, all personnel must understand and appreciate their role in ensuring the security of their organization. This document provides materials and strategies by which to design, launch, and monitor a multi-year program to improve organizational cybersecurity.

The Cybersecurity Threat to Public Power

Cybersecurity is a growing global concern. Interconnected technological systems permeate our daily lives, increasing efficiency and modernizing our business operations. These systems also increase vulnerabilities through third parties, data breaches, supply chain practices, natural disasters, and unintentional employee disclosures.

Small and medium public power organizations face many of the same threats and vulnerabilities as larger utilities and yet must address these using limited resources. Public power utilities are responsible for critical infrastructure and are widely interconnected with many loosely affiliated (or completely unaffiliated) organizations. The U.S. electric grid has been cited as the world's largest single machine, and while this interconnectedness can help with reliability and resiliency, it also presents a potential challenge.

In addition to critical infrastructure, public power organizations also bear responsibility for securing a variety of sensitive personally identifiable information (PII). Public power organizations and their service providers maintain PII for customers (e.g., addresses, billing and financial information) and staff. These information stores can make public power organizations attractive targets for cyberattack.

Fortunately, public power organizations need not face these cyber risks alone. The Association's Cybersecurity for Energy Delivery Systems (CEDS) program offers resources for all sizes of organizations to help them evaluate, prioritize, and improve their cybersecurity. The Association offers resources to inform utilities about the latest in cybersecurity and risk awareness, including the Public Power Cybersecurity Scorecard (www.PublicPower.org/Resource/Cybersecurity-Scorecard). Based on the Department of Energy's Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), the Scorecard is an online self-assessment tool for public power utilities to assess cyber risk, plan improvements, prioritize investments, and benchmark their security posture.

About this Roadmap

The Public Power Cybersecurity Roadmap builds on the Scorecard by assisting organizations to develop a strategic plan that prioritizes and details appropriate elements of a cybersecurity program. Together, the Scorecard and the Roadmap provide a strategic framework to help utilities plan and deploy cybersecurity efforts over the next three to five years. This framework draws on peer organization experience and cybersecurity expert knowledge to distill the volume of cybersecurity information in to clear, tangible strategies to gain support, ensure buy-in, and create an organizational culture that embraces secure practices as part of everyday habits.

As with the ES-C2M2 and the Scorecard, this Roadmap uses the National Institute of Standards and Technology's Cybersecurity Framework (CSF) for guidance in developing appropriate and effective cybersecurity programs. Public power utilities use the CSF in accordance with other resources (e.g., the Center for Internet Security's Top 20 Critical Security Controls) and may conform to additional regulations (e.g., North American Electric Reliability Corporation critical infrastructure protection, Payment Card Industry Data Security Standard) to round out this guidance. In developing this Roadmap, representatives from public power utilities provided input drawn from elements of all these resources to tailor guidance to small and medium public power utilities. All NIST CSF function areas (identify, protect, detect, respond, and recover) are addressed, at least in part. However, part of the strategy for this Roadmap was to prioritize and emphasize certain elements, such as management approval and project planning, over others such as detect, to promote adoption of cybersecurity practices by smaller utilities.

This document is neither authoritative nor exhaustive, but provides tools to guide the next few years' efforts in improving cybersecurity. Doing so can help ensure public power organizations provide more reliable and cost effective services to their customers and communities.

The Roadmap is intended to be used both by public power utilities that are just beginning to address improvements in cybersecurity and those with more advanced cybersecurity efforts. The Roadmap provides recommendations in a prioritized manner, but allows for flexibility so that a utility can "join" at any point or tailor the implementation of recommendations in an order that suits its individual needs.

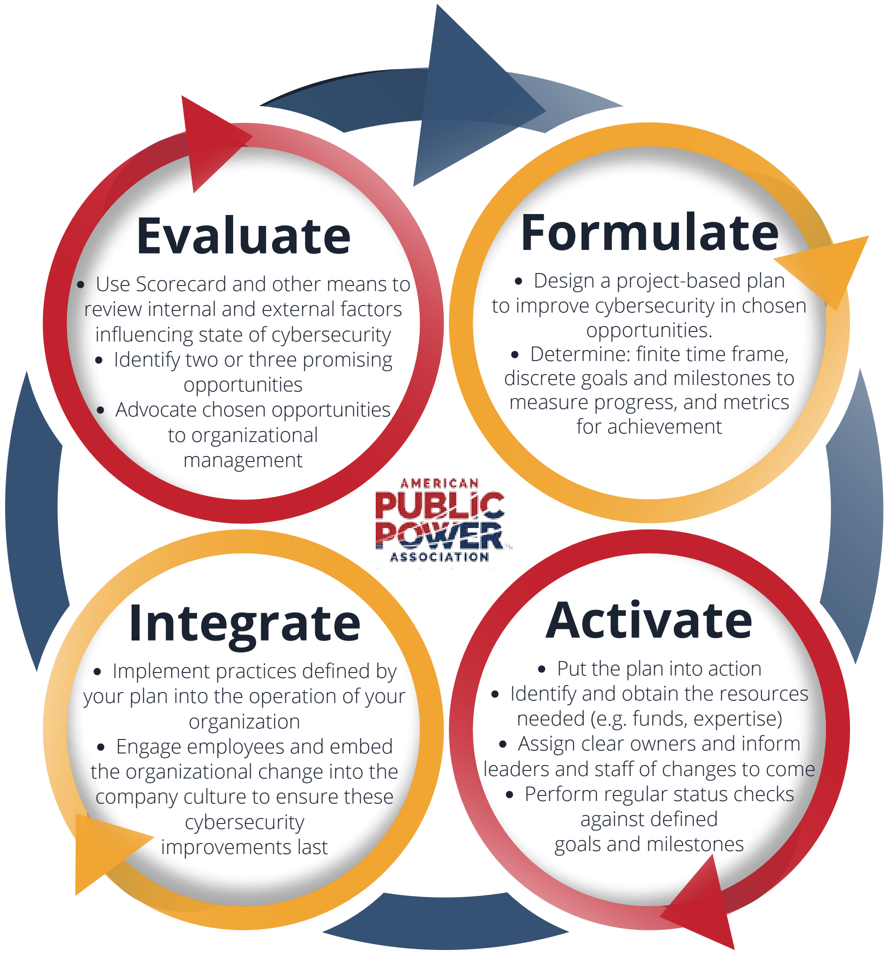
This document is the result of close collaboration between the Association and representatives from multiple public power utilities and joint action agencies. The Association corresponded with operational and technical personnel at multiple public power utilities to develop a complete view of the many layers of needs, responsibilities, and opportunities facing public power personnel. Association staff and representatives from public power utilities formed the Cybersecurity Roadmap Advisory Council (or "CRAC team"), which met biweekly (in-person or via teleconference) from summer 2018 through spring 2019 to develop this document. Team members discussed experiences with cyber threats and incidents as well as experiences collaborating with boards and management to bolster cybersecurity. Team members also discussed accounts of national and international events that offered insight into the scope and nature of cyber threats and countermeasures.

Roadmap Action Plan

Total cybersecurity can never be "achieved." Instead, an organization's cybersecurity program is a risk-based, necessary business process that requires constant, ongoing efforts at all levels. Achieving behavioral change is significantly more challenging than identifying and deploying a set of policies. Personnel and management must not only understand the necessary actions and reasons for them but must internalize them and integrate them into their regular behavior. To create successful improvements in cybersecurity, a utility needs to create an action plan that outlines clear steps for achieving a goal.

The success of turning action plans into meaningful and lasting improvements requires not only the implementation of activities but the adoption of additional roles, responsibilities and a change in processes. Be aware that current roles, responsibilities, and processes are based on past experiences and beliefs of the business. A combination of executive leadership, program management, training and awareness, risk-based revision and compromise, and rewards and discipline are required to implement meaningful change and a stable and appropriate cybersecurity program.

To successfully achieve the program goals, the CRAC team identified four stages through which organizations can build and deploy their efforts. Cumulatively, these efforts provide the framework for organizations to provide their communities with responsible, secure cyber practices and respond to incidents efficiently and effectively.



Evaluate

- Use Scorecard and other means to review internal and external factors influencing state of cybersecurity
- Identify two or three promising opportunities
- Advocate chosen opportunities to organizational management

Formulate

- Design a project-based plan to improve cybersecurity in chosen opportunities.
- Determine: finite time frame, discrete goals and milestones to measure progress, and metrics for achievement

Activate

- Put the plan into action
- Identify and obtain the resources needed (e.g. funds, expertise)
- Assign clear owners and inform leaders and staff of changes to come
- Perform regular status checks against defined goals and milestones

Integrate

- Implement practices defined by your plan into the operation of your organization
- Engage employees and embed the organizational change into the company culture to ensure these cybersecurity improvements last

Click the image to enlarge.

Stage 1: **EVALUATE** internal and external factors influencing most pressing cybersecurity issues (i.e. complete the Scorecard assessment); locate sponsors and leaders needed to achieve desired changes; generate a list of prioritized opportunities for improving cybersecurity; and consider the organization's strategy and risk tolerance.

Stage 2: **FORMULATE** a project-based plan to improve cybersecurity; use a risk-based approach to identify two or three promising opportunities for improving cybersecurity; appoint leadership and hire appropriate staff to carry out cybersecurity efforts; and implement managerial, technical, and general staff training.

Stage 3: **ACTIVATE** the project-based plan by creating ongoing, enforceable policies for all personnel; follow the activities or steps identified in the plan; acquire any necessary new tools or systems then install and test them; institute new policies and procedures needed to support tools and identified improvements to cybersecurity processes; develop a cyber incident response plan (using the Cyber Incident Response Playbook as reference); and design a communications strategy to handle potential cyber incidents.

Stage 4: **INTEGRATE** practices defined by the plan into the operation of your organization; move new tools or systems into the production environment; ensure any new systems are regularly monitored and regular patches and upgrades are maintained; operationalize and maintain the new process as part of business-as-usual practices. This turns the "new" practices into "standard" practices--making them part of your organization's culture is the final critical stage in improving cybersecurity and making sure the improvements last.

Implementation of the processes in the roadmap are based on common roles and organizational structures, but can be tailored to the perspectives and needs of management and personnel within a specific organization. Each of the stakeholder group roles and responsibilities is distinct, and so messaging for and engagement of each group will differ.

Each of the four stages is detailed below.

Stage 1 - Evaluate

Inputs:

- Public Power Cybersecurity Scorecard assessment
- Existing cybersecurity processes and procedures
- Personnel training and awareness

Processes:

- Gain initial support for cybersecurity efforts from sponsors and stakeholders
- Use Scorecard to evaluate organizational processes
- Generate a list of goals for improving cybersecurity and use a risk-based approach to identify two or three promising opportunities for improving cybersecurity from these goals
- Define the means to achieve these goals, and gain funding for and endorsement of the project process, goals, and scope from organizational management

Outputs:

- Two or three defined, achievable goals that will improve the organization's cybersecurity
- Endorsement of project by relevant sponsors

Sponsorship, Stakeholders, and Givens

Gaining support from leadership is an important first step in any major initiative and is especially critical for a cybersecurity program at a public power utility. The utility general manager or senior leader and elected officials who oversee investment in power operations and maintenance will need to understand the nature of cybersecurity threats that could impact grid reliability, security, and customer privacy. The CRAC team underscored the importance of this step many times, indicating that without leadership support, any cybersecurity improvement effort is unlikely to succeed.

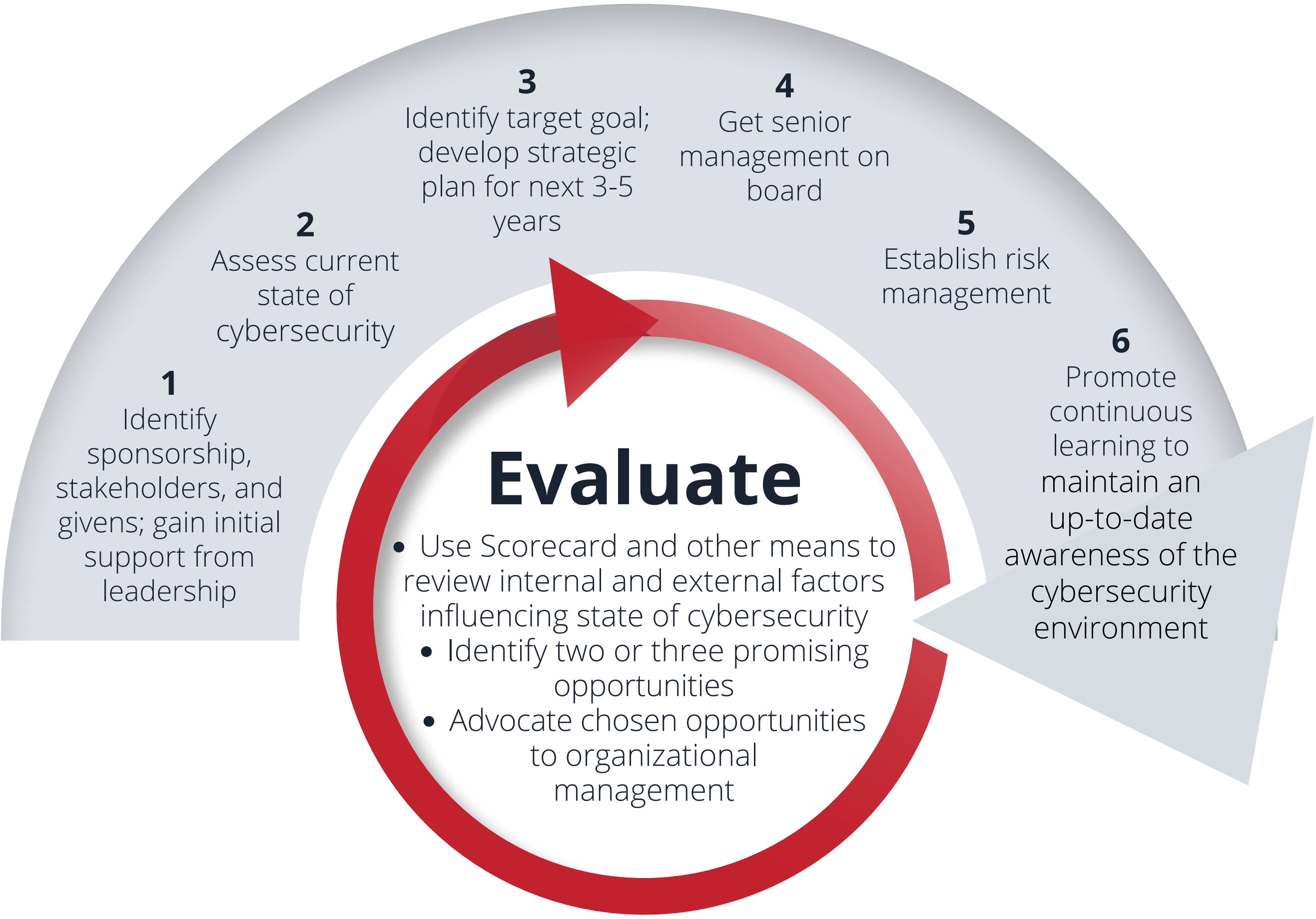
Identify a sponsor

As with many programs that introduce the potential for significant change, cybersecurity programs benefit greatly from a defined sponsor. This individual's primary role is to help garner support, overcome barriers, and serve as an interface for senior stakeholders who have an interest in the program. Additionally, sponsors can identify resources and provide clear delegation of cybersecurity duties among staff. Depending on the public power organization, the cybersecurity program sponsor may be the utility general manager or a designee such as a senior systems, engineering, or security leader. Ideally, given their role, the sponsor is positioned to assign resources across the organization. For example, while many utilities may organizationally separate Information Technology (IT) and Operations Technology (OT) departments, the CRAC team identified the importance of identifying a cybersecurity project sponsor with clear authority over resources in both IT and OT organizations.

While the sponsor does not initially need to have deep understanding of cybersecurity solutions, this individual can serve as a sounding board for the cybersecurity project leader. The sponsor can assist by using his or her experience with the utility and its strategic objectives and understanding of potential operational and customer impacts of any cybersecurity improvements suggested by the team. A utility might consider providing more advanced training for the sponsor to gain a stronger understanding of cyber risks (e.g., application vulnerabilities, third-party breaches, social engineering) and controls (e.g., open source intelligence, security assessments, vendor risk management).

Map out stakeholders

Like all significant utility projects, cybersecurity improvement projects have many stakeholders—individuals or groups who have an interest in or can influence the outcome of a project. Sponsors and identified project leads should spend time identifying any cybersecurity project stakeholders and consider their potential questions, positions, and reasons for support or resistance to the project. Understanding the objectives and concerns of the various stakeholders in the cybersecurity program


1
Identify sponsorship, stakeholders, and givens; gain initial support from leadership
2
Assess current state of cybersecurity
3
Identify target goal; develop strategic plan for next 3-5 years
4
Get senior management on board
5
Establish risk management
6
Promote continuous learning to maintain an up-to-date awareness of the cybersecurity environment
Evaluate
• Use Scorecard and other means to review internal and external factors influencing state of cybersecurity
• Identify two or three promising opportunities
• Advocate chosen opportunities to organizational management

development is important for it to succeed. Examples of stakeholders include elected officials such as the city council, regulators, consumer advocacy groups or key customers in the service territory, vendors who provide cybersecurity services or technology (if known), and staff who will need to abide by new policies or processes. Building even a short list of these stakeholders and considering their positions and objectives on cybersecurity investment and process changes will aid the team immensely as proposals for projects and initiatives are considered and reviewed with utility decision makers.

Research givens: regulations, laws, and standards
Getting to know the "lay of the land" for cybersecurity will help to set the tone of and understanding for the activities to come. The sponsor or project lead should have an initial understanding of the regulations, laws, and standards that could impact a cybersecurity program. Resources from previous projects that address cyber or physical security are a good place to start. For example, a utility that has recently deployed advanced metering infrastructure (AMI) might have explored and decided upon communication security and customer data privacy. Or perhaps a recent distribution automation project identified new OT security processes. Understanding the decisions made during these projects will help guide the direction of any new cybersecurity program. If no examples like this exist, public power entities can explore other initiatives within their municipality or government (e.g., police department initiatives related to improving secure communications or patient data privacy compliance required for first responders). Finally, the sponsor or project lead can look to peer utilities that have recently begun cybersecurity initiatives or to conferences such as the Association's Public Power Cybersecurity Summit for examples. This stage will help a utility understand the state of its cybersecurity, identify what steps it needs to take to develop a clear plan to improve cybersecurity, gain the support it needs to put the plan into action, and manage an ongoing cybersecurity project.

Initial Assessment Activities

Assess cybersecurity posture

Before launching a project to bolster organizational cybersecurity, it is essential to develop a clear and complete understanding of an organization's cybersecurity environment. This entails both the internal and external environments. The internal environment addresses the organization's operations, including relevant personnel, their responsibilities, and the hardware, software, and infrastructure they engage with while working. The external environment includes relevant regulations, interconnections with other organizations, and any other outside factors that might influence operations. The Public Power Cybersecurity Scorecard provides a clear measure of organizational operations and identifies gaps that are good targets for initial improvement efforts.

Baseline Assessment Activities

- Identify and engage other business units
- Define scope of assessment: physical buildings, systems, applications, external services, and staff members
- Inform all involved of the purpose of the effort and what is expected of them
- Schedule document and interview requests
- Engage existing tool: Public Power Scorecard, C2M2; perform Public Power Scorecard (C2M2) Assessment
- Enlist a professional, independent, and onsite assessment
- Perform independent penetration test
- Perform any additional current state assessment of IT, OT, user management (access control), profiles, and passwords

Identify Target Profile Activities

- Utilize existing MIL-2 target profile
- Consider APPA-defined Public Power
- Cybersecurity Center of Excellence Program
- Benchmark against similar utilities
- Estimate costs/benefits for target
- Review existing standards; identify milestones (1/2 year to annual frequency)

Develop a target profile (goal)

Once the initial assessment is completed, the project can be mapped. This involves developing a strategic plan for improving an organization's cybersecurity over the next three to five years. The plan must include clear, actionable steps and strategies and means of accountability to ensure it is used. Members of the CRAC team recommend that utilities consider using an outside consultant to ensure an efficient, successful project, unless the utility has in-house personnel with advanced knowledge of cybersecurity concerns and strategies and who can dedicate adequate time to the effort. Expect the overall effort to require 80 to 200 working hours to complete.

Outline a business case and seek buy-in

A plan has no value unless it is put into action. Buy-in from senior management, the board, and other members of the guiding coalition helps to address two of the largest concerns for project success: 1) organization personnel and other internal stakeholders will resist the plan, and 2) organization leadership will not sufficiently support or enforce the plan. Engaging organizational leadership requires careful definition of the goals and scope of the plan and a clear business case for the project.

Making the Case

- Define what we are trying to protect
- Develop business case
    - Outcomes of penetration test
    - Examples of incidents
    - Include benchmark assessment
- Use Scorecard to identify target for cyber program (end-goal for phase)
- Identify budget and resource needs
- Identify peer/mature utilities for guidance
- Enlist outside consultants/SMEs to present/ build case to management
- Identify and recruit "cyber council" steering committee (management, tech management, ops, physical security, technicians)

Begin by clearly defining what the cybersecurity project seeks to protect: critical systems and applications and sensitive data. This extends beyond hardware and software, and includes corporate data, system settings, customer data, and other sensitive assets. Describe the cascading effects of increased cybersecurity, such as more reliable service and customer data protection. Such benefits — particularly those related to the organization's relationship with customers and regulators — clearly tie in with the business case.

The business case should frame any potential benefits with established, quantifiable data. Results of a penetration test and assessment of systems' robustness or vulnerability against established standards and best practices can provide a tangible demonstration of need. Examples of peer organizations encountering and overcoming or suffering the effects of a cyber event can provide a useful cautionary perspective.

Providing clear achievements and milestones for measuring progress toward the desired end state enables articulation of budget justification and resource requirements. Be sure to articulate that reaching the goal of the initial project plan does not mean that the cybersecurity program is complete — rather, it must evolve over the life of the organization.

Other organizations can provide valuable input into the plan. Peer organizations can provide insight and lessons learned from similar efforts. Both positive and negative examples are valuable input to a project plan. Once a program gets established, utilities can also engage peer organizations in a mutually beneficial, ongoing collaboration to ensure awareness of and help with integration of new cyber practices and technologies. External consultants and subject matter experts could help build a persuasive case to present to management, pulling from their experience in similar projects. A consultant or SME could also guide and improve projects and provide direct oversight. Outside assistance does not need to be undertaken in perpetuity, but might ensure an efficient, swift, and effective deployment of new practices and technologies.

Risk Management Checklist

- Integrate with Enterprise Risk Management
    - Consult or develop risk register
    - Rank cyber risks relative to enterprise risks
    - Identify a champion in the existing Enterprise Risk Management process
- Perform risk assessment
    - Define threats
    - Identify assests
    - Review vulnerabilities
    - Analyze risks
    - Prioritize risks analyzed (high/medium/low)
    - Create risk remediation recommendations

Once the plan is developed and vetted by organizational management, present the plan to the board. This presentation should include: 1) the rationale for undertaking each priority, 2) the actionable steps that will ensure timely achievement of each priority, 3) an estimate of the resources needed to complete the effort, and 4) personnel responsible for each priority and their motivation for success. Breaking down the plan in this way makes it more comprehensible for the board. Including these details for each priority also helps management think through whether the relevant staff within the organization have the means, incentive, and understanding of how to put the plan into action.

Engaging different levels of leadership should continue once the project is launched. A "cyber council" steering committee could be made up of representatives from senior leadership, management, technology management, operations, legal, physical security, employee/union representative, and technicians. By spanning all levels of the organization, such a council also offers multiple views of oversight of the cyber program, from the business and regulatory impacts to individual functional requirements. A three- to five-year timeframe allows room for adaptation and learning, but is also sufficiently immediate to spur action. Regular meetings (e.g., monthly) to review milestones and discuss progress can spur accountability and allow adjustments in schedule or personnel if the initial framework is not effective or priorities shift.

Establish risk management

Cybersecurity functions analyze and address a type of risk. Making risk management a part of organizational culture will help make cybersecurity a part of the culture as well. An ongoing cybersecurity program should align with an organization's other risk management functions. One good place to start is by making sure that the cybersecurity plan complements existing risk management processes. If an enterprise risk register exists, use it. Otherwise, develop an enterprise risk register and engage other relevant personnel in its use. When populating the enterprise risk register, rank identified cyber risks along with other enterprise risks to illustrate prominence and priority and further embed cybersecurity into organizational psyche. A risk champion, either a consultant or an internal risk expert, can be valuable in providing ongoing assistance and ensuring effective processes.

Risk Analysis Checklist

- Assess "brand risk" exposure
- Assess compliance/regulatory risks
- Create realistic risk measures
- Define risk in business/management terms
- Examine corporate risk tolerance
- Review policies (e.g. access policies) to determine non-negotiable risk exposure
- Consider quick-wins

Risk analysis should consider regulatory and compliance drives as well as operational and customer service concerns. Defining these risks in business management terms can improve leadership and customers' appreciation of their impacts. Risks should be analyzed in a framework of organizational risk tolerance, which can differ from utility to utility. Degrees of acceptable risk exposure should be both calculated and articulated in terms of cost and benefit. This can help achieve a common understanding of what risk reduction practices are trying to limit. Prioritizing risks (e.g., high/medium/low) can further delineate between acceptable and unacceptable levels of risk. Once all risks are identified, prioritized, and articulated, the final essential step is defining a risk remediation plan.

Another element to consider is continuous learning. Cybersecurity is a rapidly evolving field, and encompasses new developments in technology and changing risks. Staying aware of the cybersecurity environment demands a dedicated, but not overwhelming, effort. Conferences, exercises, and training are essential to continuous learning. Online training programs can be schedule- and budget-friendly ways to learn about best practices and newest developments from industry experts. Include all levels of staff in these trainings to underscore the importance of cybersecurity in the organization's culture. The Association can guide utilities to proven and current training resources. Though more expensive and demanding of time, attending conferences and in-person trainings provides unparalleled value in interaction with peers from other organizations and cybersecurity experts, which can improve one's understanding and ability to apply the latest tools and techniques. The project lead should attend at least one such event per year, and other project leads and/or task leaders should be encouraged and enabled to attend as well. The camaraderie that can develop in such an experience is invaluable to a constructive and enthusiastic organizational culture.

Stage 2 - Formulate

Inputs:

- Defined goals for improving cybersecurity
- Support from sponsors and leadership

Processes:

- Generate a project-based plan by which to achieve the priority goals
- Build plan starting with the current state of cybersecurity
- Identify relevant milestones by which to mark and measure progress

Outputs:

- An actionable plan project leaders and process-level personnel can use to understand the goals, purposes, and needs for each stage of the project

Establish a Project-based Approach

Applying project management techniques and concepts to a cybersecurity improvement effort can provide utilities with a familiar framework and proven methodology for implementing a new program. Using the familiar touchstones of project management — articulating goals, setting a schedule to achieve those goals, developing tools to facilitate the plan, and continuing to learn about the pursuit — can demystify cybersecurity and better ensure success.

Develop a cybersecurity strategy

A strategy requires a goal, and setting cybersecurity-centric goals builds cybersecurity into both the organization's aspirations and culture. Integrating cybersecurity into the utility's culture might require disentangling it from IT, which will afford a broader oversight and governance from across organizational leadership and prevent perception of cybersecurity being "someone else's problem."

Create a clear schedule

Create a clear schedule to guide the maturation of the project and provide clear milestones by which to mark progress. Strategies with the greatest likelihood of success seem to build on a timeframe of three to five years — long enough for a program to mature and develop, but immediate enough to afford urgency and limit scope to a tangible set of activities. Prioritize actions and then develop a schedule to reach desired milestones within the set timeframe. Starting with easy-to-achieve goals (i.e., "low-hanging fruit") can lead to a series of quick wins that show early progress and bolster morale. Assign responsible parties for each point to ensure accountability. Estimate what's needed for each stage to aid in budgeting and allocation of resources.

Define the metrics

Define the metrics that will measure progress. Gauging progress demands a method by which to measure that progress. Choose task-level metrics that are clear, defined, and direct products of successful completion of the task. The task-level metrics can provide milestones for achieving program goals. These program goals, in turn, aggregate to definable, quantitative measures of program success. Measuring and communicating progress shows both leadership and personnel that the project is valuable and successful. Report milestones and measures quarterly to both organizational personnel and management to reinforce project progress and celebrate success.

Develop a resource management plan

Management plans are tools to guide timely and efficient allocation of resources to a project. A resource management plan influences the management of how financial, personnel, and vendor resources get applied to a project. Allocation of human resources requires a clearly defined set of responsibilities and roles for each staff member and for vendors and outside consultants. As cybersecurity is a feature of organizational culture, all personnel should play some role, and all vendors and suppliers identified should likewise have a clear role to play for which they will be held accountable. Aggregating personnel with collaborative responsibilities into teams eases the management of and reporting by such groups. Ideally, the teams span operational and technical capacities to improve organizational communication and coordination.

Project-Based Approach

- Define cybersecurity strategy as a corporate goal
- Develop prioritized action list with dates, responsible parties, and resource estimations
- Define data and metrics for security program
- Develop resource management plan (budget, personnel and vendors)
- Create cyber project management plan
  - Communications plan
  - Scope
  - Schedule
  - Budget
  - Risk plan
- Engage in continuous learning
  - Ongoing training programs (all levels of personnel)
  - Exercises/conferences/training

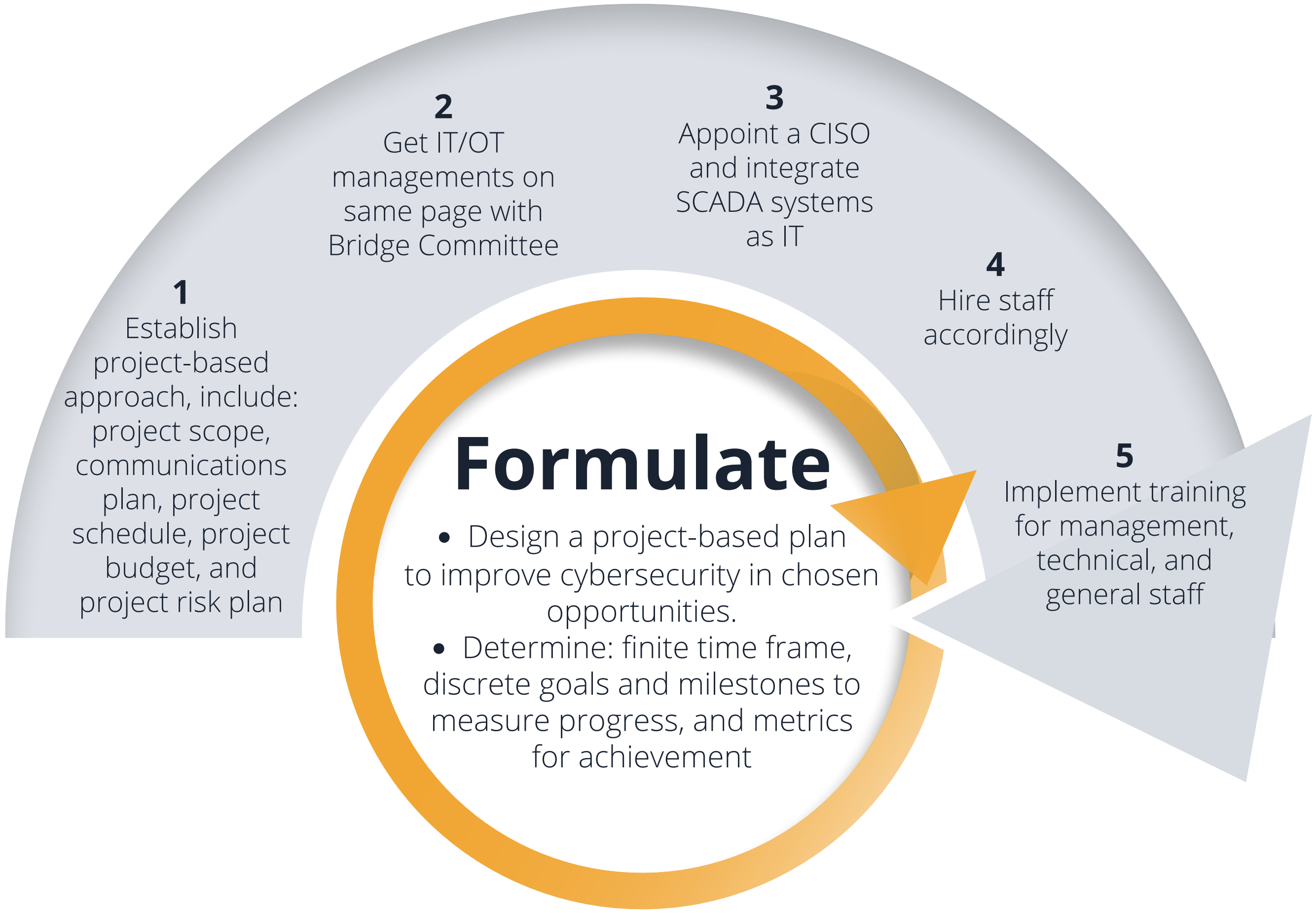
Define the role of the project lead

The resource management plan should also define the role of the project lead. The project lead is responsible for ensuring the project teams' activities and goals align with the overall project plan. The project lead is responsible for identifying cybersecurity mutual aid options, bringing them to the organization, and enrolling in them if/as appropriate. The project lead should also monitor continuing education opportunities, such as low- or no-cost cybersecurity seminars and training, government publications, and online resources such as threat intelligence feeds.

Assemble the cybersecurity project management plan

The cybersecurity project management plan defines what personnel will do and how those activities aggregate into the overall cybersecurity program. The features of this plan include:

- A detailed description of the *project scope*, clearly defining the bounds of the project. This is important in understanding what activities are essential and what those activities entail. Defining the project scope can avoid undertaking tangential tasks that draw resources away from the identified priorities. Scope creep — unintentional increase in project work due to acceptance of tangential work — impedes progress and efficiency and can compromise the success of the project. The statements of project scope should include all technology to be engaged by the project; cyber assets and means of protecting them (e.g., SCADA, data, means of access and protocols for access); and the systems, policies, and procedures that will produce the desired project outcome.
- A *communications plan* that defines project stakeholders and the role of each business unit in the organization, project reporting intervals and standards for reporting, networks of communication engaged, how project teams will coordinate their activities, and how concerned personnel can report issues or suggest changes to the plans, methods, or scope.
- A *project schedule* that defines the phases of the projects at the task level, and illustrates how those tasks will be achieved within a certain timeframe. Gantt charts or similar graphic presentations are useful to show how tasks overlap without compromising progress and provide an at-a-glance reference of the current point in a project and the expected next steps. Including updated schedules in regular progress meetings (e.g., quarterly) can assure leadership that the project is achieving its target goals and reward personnel with clear illustration of the value of their work.
- A *project budget* defining the financial resources and how those resources will be allocated over the course of the project. Again, break this plan down to the task level, to clearly illustrate where all funds will be applied and how those funds are necessary to achieve the goals of the project. Task-level budgeting can help avoid the need for additional funding requests, barring unforeseen developments, and improve accounting and accountability of those distributing and applying funds. The final budget should receive approval and support from senior management before the launch of the project. It is helpful to align the budget priorities with the project's goals for senior management.



Formulate

- Design a project-based plan to improve cybersecurity in chosen opportunities.
- Determine: finite time frame, discrete goals and milestones to measure progress, and metrics for achievement

1 Establish project-based approach, include: project scope, communications plan, project schedule, project budget, and project risk plan

2 Get IT/OT managements on same page with Bridge Committee

3 Appoint a CISO and integrate SCADA systems as IT

4 Hire staff accordingly

5 Implement training for management, technical, and general staff

- A *project risk plan* aimed at anticipating events that could impact the project scope, schedule, communications, and budget. All projects entail risks, and identifying potential risks in advance improves project performance. The risk management plan should first consider the degree of risk an organization is willing to undertake. More ambitious projects provide more impressive results, but also assume greater risks. Consider the degree of uncertainty the organization is willing to assume in pursuit of greater gains, the amount of risk personnel will tolerate, and the level of uncertainty versus level of impact that will define the point where a utility will determine a risk is too high to pursue.

Review IT, OT, and Security Organization Workforce

Deployment of the cybersecurity strategy begins with organizational personnel. Without internal stakeholder buy-in, the effort will not succeed. This must go beyond making a compelling argument. Adopting a culture of cybersecurity requires fundamental behavior change, which first requires shifting beliefs and attitudes. If personnel do not clearly understand the need and wholeheartedly embrace the necessary measures, then short term shifts are unlikely to persist in the long term. The steps below must be presented as the logical and achievable way to accomplish an essential goal for ensuring the future of the utility and maximizing the benefits to customers and communities.

Workforce Development Checklist

- Review IT, OT, and Security Organization
  - Found an IT/OT Bridge Committee
  - Designate a Cybersecurity Information Security Officer
  - Integrate SCADA systems as IT
  - Put federal resources into use, e.g. C2M2, NERC-CIP
- Hiring Practices
- Supply Chain Risk (Vendor) Management
  - Background checks
  - Vendor tracking
  - Security Controls in Contracts
  - Review SLA Adherence
  - Security Controls for Communications

Each utility has needs and considerations unique to its size, structure, infrastructure, organization, service community, regulatory environment, and other characteristics. Since a single prescription does not fit all utilities, active, critical engagement with the tools of this roadmap is necessary to tailor the actions appropriately. To ensure application of the principles of this Roadmap and cultivate a culture of cyber awareness and responsibility, a utility should first define the roles and responsibilities of personnel, beginning with management.

Form an IT/OT bridge committee

Some organizations distinguish IT management from OT management, and the personnel for these divisions might not interact. To begin unifying cybersecurity efforts, the CRAC team recommends founding an IT/OT bridge committee that meets regularly to exchange information. These meetings can build a culture of collaboration that improves information sharing and response coordination.

Designate a Cybersecurity Information Security Officer (CISO) and SCADA systems as IT

Organizations should designate a Cybersecurity Information Security Officer (CISO) to lead, monitor, and control cybersecurity efforts and operations. The CISO maintains a broad view and has sole authority of the organization's cyber posture to ensure efforts are comprehensive and efficient. In organizations with distinct IT and OT capacities, the CISO can chair the IT/OT bridge committee. To improve situational and operational awareness, organizations should integrate supervisory control and data acquisition (SCADA) systems as IT, so they fall under the cybersecurity umbrella.

Many federal resources can aid these efforts. C2M2 can improve insight for senior leadership. The North American Electric Reliability Corporation Critical Infrastructure Protection (NERC-CIP) program provides detailed and frequently updated guidance on best practices. NERC-CIP standards for improved infrastructure mark an essential benchmark for public power organizations and a touchstone for aligning practices and lexicon between organizations. The U.S. Department of Homeland Security Protective Security Advisors (www.dhs.gov/protective-security-advisors) and Regional Resiliency Assessment Program (www.dhs.gov/regional-resiliency-assessment-program) can inform, guide, and assess organizational initiatives.

Hiring and Vendor Management Practices

Careful consideration of new personnel and vendors can have an immediate impact on a culture of cybersecurity. Vendor services or products that provide access to organizational systems can be attacked. In addition, new staff, particularly those in sensitive capacities, might provide ingress.

The following actions can help a utility address vendor and staff risks:

1) Implementing background checks for new vendors and personnel to screen for potential threats

2) Monitoring third party services with access to a utility's system

3) Ensuring appropriate security controls are incorporat ed into vendor contracts

4) Including a review of vendor service level agreement (SLA) adherence with contract requirements

5) Establishing minimum security controls for vendors and incident response communication

6) Reviewing vendors' implementation of security controls through third party assessments, interviews, or questionnaires

For personnel, establishing an internship program with the opportunity for hiring can provide a longer vetting process and help to integrate potential staff into the organizational culture over a longer term. The DOE national laboratories' hiring practices provide a useful model for vetting and integrating technical staff (e.g., challenge potential hires to secure a system within one month and test their results).

Training

Training can improve staff capabilities and integrate newly hired staff into the organization's culture of cybersecurity. The content and emphasis of training must be developed for different specialties within the organization due to the different responsibilities of divisions among organizational personnel. Distinct management training, technical staff training, and nontechnical general staff training can prepare employees for the particular needs of their organizational capacity.

Management training
Management training must prepare those in leadership positions to both guide and set an example for the rest of the organization, as well as interact with community and regulatory agencies. Board-level workshops using C2M2 processes can build intra-organizational cyber literacy and improve interaction between organizational leadership and technical and operational personnel. Organizational leadership must be sufficiently fluent in the types and nature of cyber threats, and of operational capabilities and limitations for robust security and timely and effective response following an event. Leadership must also be prepared to communicate on behalf of the organization with media; peer organizations; and local, state, and federal governments. Workshops held in conjunction with community, city, county, or state government agencies can improve coordination and collaboration, and ensure that necessary relationships and avenues of communication are in place before a cyber-related event.

Technical staff training
Technical staff training for roles most closely associated with the critical processes and points of vulnerability. Aligning the efforts of OT, IT, and security staff during standard operations can better prevent crises, as well as speed and streamline responses to them. Establishing informal "lunch and learn" sessions as part of organizational operations can foster collaboration between these subdivisions, encourage professional relationships, and promote more frequent and open communication. Weaving security awareness into the social fabric of the organization normalizes the state of preparedness and shifts perception of cybersecurity efforts from additional duties to

Workforce Development Checklist: Management-Level Workshops

- Cybersecurity literacy
- Operational capabilites and limitations
- Communication strategies during an incident
- Held in conjunction with local government stakeholders

business-as-usual. Organizational leadership should seek out external opportunities for training that multi-divisional groups could pursue, such as National Exercise and Grid Ex training. Program-wide training should comprise cyber, operations, maintenance, engineering, and physical and cybersecurity. The DHS Industrial Controls Systems Cyber Management Response Team (ICS-CERT, https://ics-cert.us-cert.gov/) offers many relevant resources, including free video training.

General staff training

General staff training reinforces the example set by leadership, cultivates an organization-wide culture of cybersecurity, raises organizational awareness, and promotes good practices in all technical processes. Online cybersecurity training can introduce concepts and practices, and is well suited to be part of onboarding for new personnel and an annual "refresher" training for continuing personnel. Quarterly workshops can address rotating specialized topics, such as appropriate responses to phishing campaigns, and serve as key performance indicators. Excellence in these training efforts and demonstration of good "hygiene" in daily practice by individual personnel can be recognized through a certificate or similar rewards. Compliance with cybersecurity policies and awareness of vulnerabilities and threats are the core of such a training program. Stakeholders' awareness of their role and consequences of their behaviors is essential to ensuring a robust organizational posture.

Establishing this volume of training may seem daunting, but many free and plug-and-play resources are available to supplement a training program. CRAC participants noted that Equifax has particularly valuable video resources. Peer collaboration can also lead to exchange of useful resources. Just as the CRAC team shared examples and personal experiences for this roadmap, the Association will continue to foster inter-organizational sharing.

As public power utilities deploy and refine cybersecurity programs, sharing stories among peers will reinforce and improve each other's efforts. Having the opportunity to learn from each other can ensure efforts are efficient and effective, show that challenges and missteps faced are not unique to any one organization, and improve morale. Real-world anecdotes of shortfalls and successes can provide tangible, valuable information for personnel, management, and board members.

Workforce Development Checklist: Technical Staff Training

- Lunch and learn sessions to align efforts of OT, IT, and security staff
- External training: National Exercise and Grid Ex
- Free video training from DHS
- General Staff Training
    - Online training to introduce (and refresh) cybersecurity basics
    - Quarterly workshops to address specialized topics
    - Compliance and good "hygiene" are rewarded

Stage 3 - Activate

Inputs:
- Project-based plan to improve cybersecurity

Processes:
- Use the plan as a guide to launch new practices, policies, and protocols; conduct activities noted in the plan
- Review and revise policies to enforce new practices, including rewarding compliance and penalizing noncompliance

Outputs:
- New organizational standards for practice and behavior that help the organization achieve its cybersecurity goals
- New tools and/or systems to enforce standards and reduce risk

Policies

A comprehensive, policy-driven approach is necessary to enforce the desired shift in organizational culture. Even with trained and vetted personnel, the organization must afford and bolster its commitment to security with ongoing, enforceable policies that all personnel adopt and follow. Policies must ensure that practices by both the utility and individual personnel support and enable a comprehensive and effective culture of organizational security.

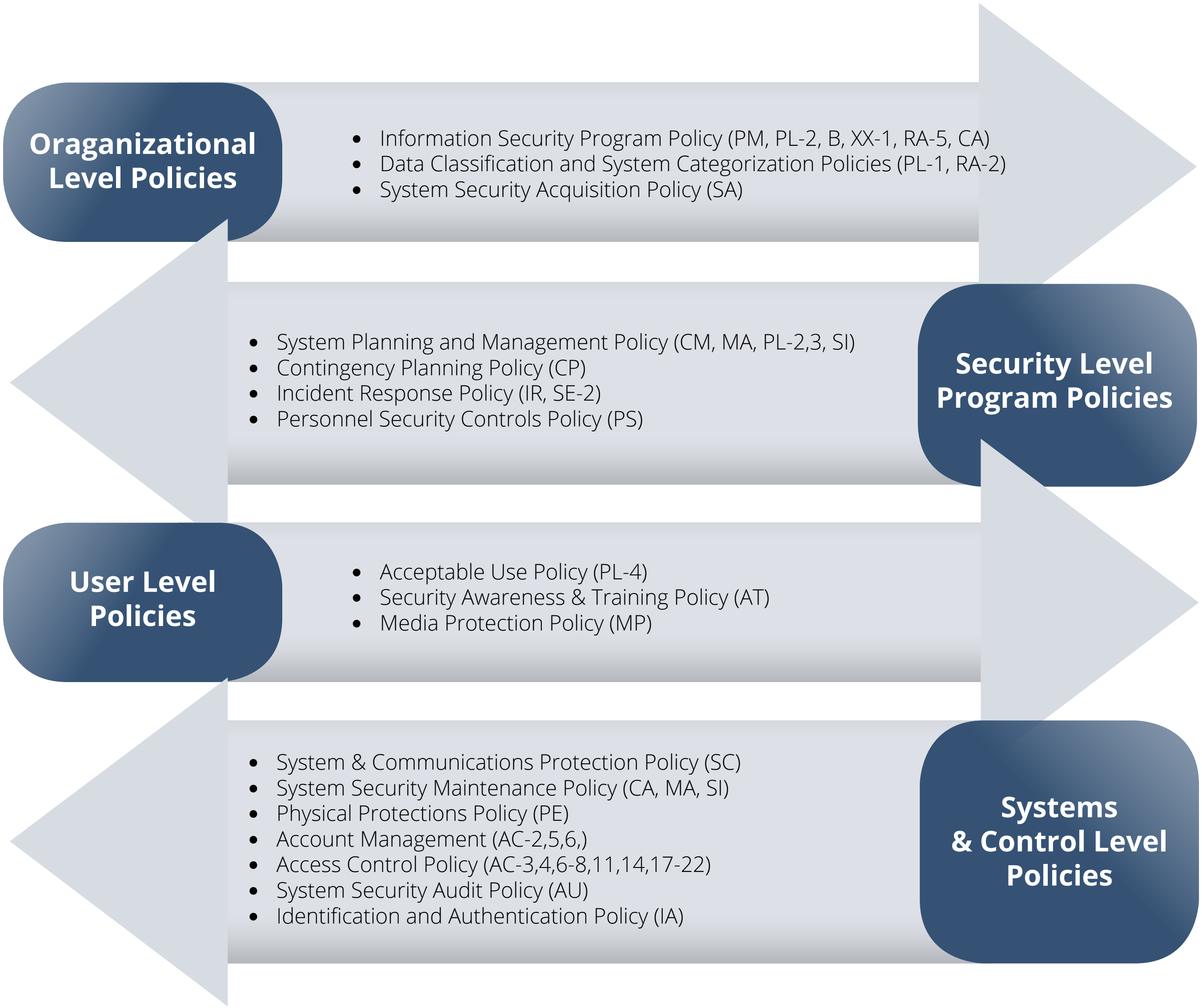
Thoroughly test any new tools or systems to be installed and used, both for functionality and for system impact. Each new system will include a new set of policies and procedures that must be developed for adoption by the organization. This includes procedures for system use (e.g., monitoring system logs) and plans for system maintenance to ensure it continues to offer appropriate monitoring and security.

The organization must underscore the importance of the culture of security and foster an environment where behaviors are not just expected, but embedded in all practices. The cybersecurity policy appropriate for one utility might vary greatly for another to address the specific environmental, cultural, technical, and organizational needs. However, an organized approach to policy development should start with the recognition or adoption of a cybersecurity framework. If an organization adopted the Federal Information Security Management Act (FISMA) and the NIST Special Publication 800-53, the policy set would look similar to the FISMA-Based Information Security Policy Framework graphic on the following page (pg. 22) .

Document all knowledge generated from these new policies for use by relevant personnel. Maintaining knowledge and accountability of practices can improve communication and awareness among relevant employees and aid future forensic investigations.

Workforce Development Checklist:
Policies, Rewards, and Sanctions

- Policies
  - Security Assessments
  - Scanning kiosks
  - Cybersecurity newsletter
  - Strengthen personnel password policies
  - Document all new policies for easy reference
- Rewards and Sanctions
  - Recognition of good “hygiene” practices presented with an audience
  - Corrective measures communicated in confidence



Oraganizational Level Policies

- Information Security Program Policy (PM, PL-2, B, XX-1, RA-5, CA)
- Data Classification and System Categorization Policies (PL-1, RA-2)
- System Security Acquisition Policy (SA)

Security Level Program Policies

- System Planning and Management Policy (CM, MA, PL-2,3, SI)
- Contingency Planning Policy (CP)
- Incident Response Policy (IR, SE-2)
- Personnel Security Controls Policy (PS)

User Level Policies

- Acceptable Use Policy (PL-4)
- Security Awareness & Training Policy (AT)
- Media Protection Policy (MP)

Systems & Control Level Policies

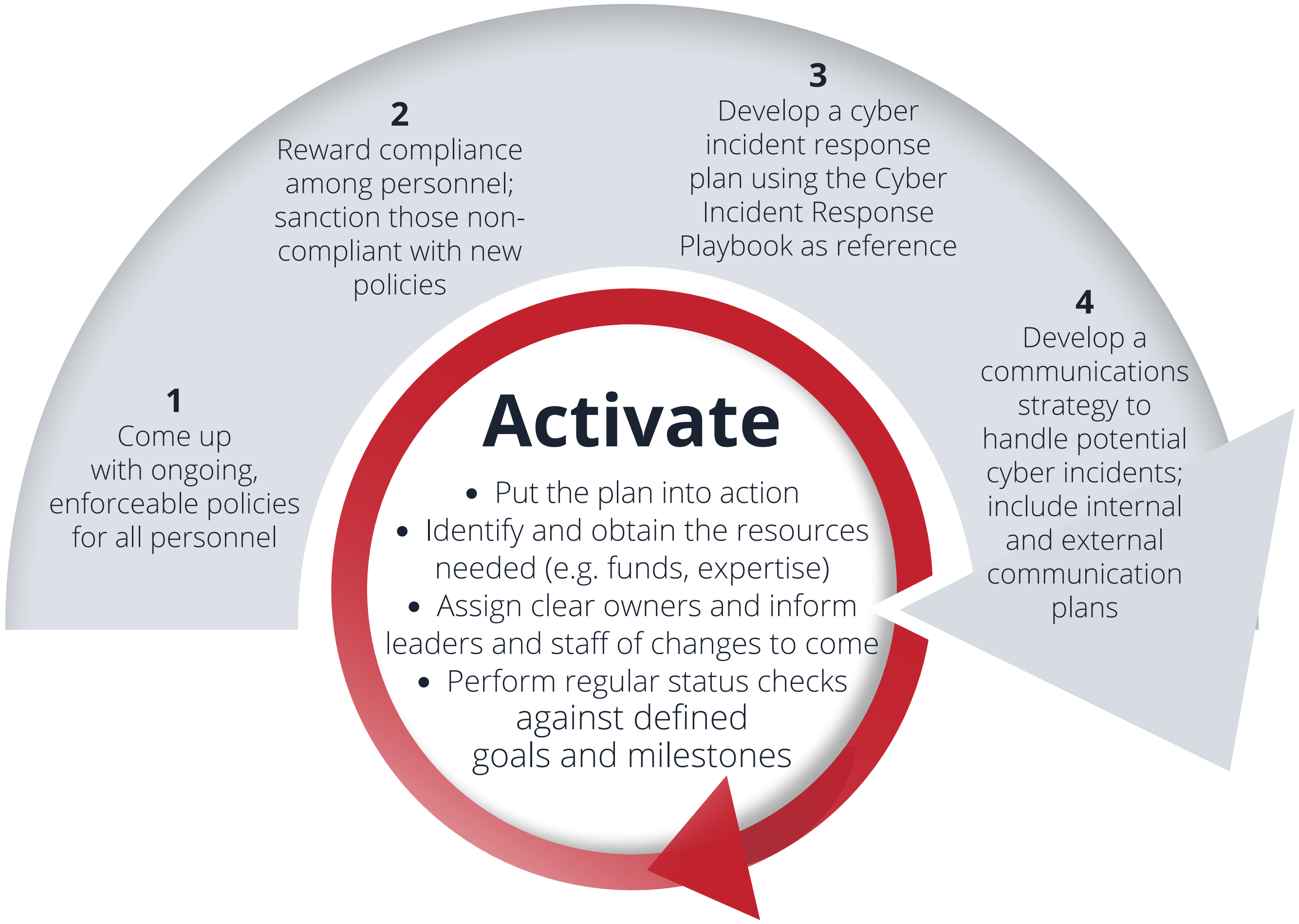
- System & Communications Protection Policy (SC)
- System Security Maintenance Policy (CA, MA, SI)
- Physical Protections Policy (PE)
- Account Management (AC-2,5,6,)
- Access Control Policy (AC-3,4,6-8,11,14,17-22)
- System Security Audit Policy (AU)
- Identification and Authentication Policy (IA)

FISMA-Based Information Security Policy Framework example.

Rewards and sanctions

Generating the initial momentum necessary to shift organizational practices depends upon both the proverbial "carrots" and "sticks." As mentioned in the "Training" section, certificates or similar recognition of good hygiene and practices offer useful means of rewarding compliance and communicating that leadership are monitoring compliance (and lack thereof). This underscores the need for everyone in the organization to honor and respond to policies and practices. Other methods of rewarding compliance or sanctioning non-compliant personnel can be tailored to the culture of an organization. Members of the CRAC team mentioned offering premier parking spaces, gift certificates, and "cybersecure employee of the month" recognition.

Some manner of sanctions must also be devised and clearly communicated to all employees to enforce that compliance is not optional or limited to a select subset of personnel. CRAC team members recognized that public power utilities are generally supportive organizations, so sanctions might be more difficult to implement. However, if infractions continue, corrective action needs to occur. Sanctions should begin with private, one-on-one conversations when inappropriate activities are recognized, and escalate as needed. The purpose of sanctions is to correct behavior, not to publicly shame personnel. Rewards seem to be most effective when presented with a wide audience, and corrective measures appear to be most effective when presented in confidence.



1 Come up with ongoing, enforceable policies for all personnel

2 Reward compliance among personnel; sanction those non-compliant with new policies

3 Develop a cyber incident response plan using the Cyber Incident Response Playbook as reference

4 Develop a communications strategy to handle potential cyber incidents; include internal and external communication plans

Activate

- Put the plan into action
- Identify and obtain the resources needed (e.g. funds, expertise)
- Assign clear owners and inform leaders and staff of changes to come
- Perform regular status checks against defined goals and milestones

Incident Response

The true test of a cybersecurity program is incident response to an actual breach. A utility is either prepared for an incident or it is not. Developing and executing a cyber incident response plan is a key component for any organization, especially an electric utility. The Cyber Incident Response Playbook details the steps necessary for a utility to be prepared for a cyber incident. Below is a summary of the Playbook and additional suggestions for performing advanced preparation and detecting, responding to, and communicating during cyber incidents.

Perform Advanced Preparation for Cyber Incident
Implementing a series of risk management best practices will lay the foundation for preventing cyber-related attacks. Assembling the right people with a clear chain of command, procuring the right tools and support, and liaising with key outside stakeholders is crucial for success. This suite of actions helps secure a utility's network and build trust within and outside its organization, as well as prepares the utility's team to handle any cyber threat that may come its way.

The team should include an overall team manager and technical staff, plus individuals who can maintain and update all lists, strategies, and the overall cybersecurity plan. It is important to designate a communications lead to develop a communications plan prior to an incident and act as a main point of contact for internal and external stakeholders during an incident. This will help keep communication among all stakeholders clear, consistent, and timely, and eliminate duplicative efforts. Critical individuals to keep your business running during an incident might include designated financial representatives who can help ascertain funds and coordinate with those who handle business continuity interactions, and a logistical lead for food and lodging. A utility might also wish to designate a compliance officer to ensure adherence to policies and reporting procedures. Vendors and SMEs for IT, OT, generation, and distribution can provide a team with expert know-how during emerging threats or in an emergency. Outside groups might also be necessary to communicate with stakeholders such as union liaisons and, depending on the type of attack, the U.S. Department of Energy or an Information Sharing and Analysis Center.

Incident Response Checklist

- Perform Advance Preparation
- Implement *Incident Response Playbook* risk management best practices:
  - Assemble a team with a clear chain of command. Designated members should cover:
    - General team manager
    - IT technical staff
    - Communications
    - Finances
    - Business continuity
    - Logistical lead
    - Compliance officer
    - Subject matter experts
    - External organizations
- Asset Inventory
- Execute Training Exercises
- Develop a continuity plan for backup and restore
- Employ risk management best practices

Other key elements when performing advanced preparation for a cyber incident may include identifying and taking inventory of business-critical IT and OT assets, executing training exercises, and developing a continuity plan for backup and restoration. Consider outlining additional checklists, other personnel, strategies, and agreements when developing an incident response plan. This includes developing a 24/7 contact list for response personnel and partners, identifying a cyber mutual aid coordinator, establishing agreements, developing a communication strategy, and creating an action item checklist.

A utility needs to employ a multitude of risk management best practices for a robust cyber incident response program. Best practices can range from maintaining network, systems, and application security to conducting regularly scheduled training for employees. Primary actions should include adopting and implementing the Playbook, including ensuring organizational adoption of expected response during an incident. Finally, when applying a holistic approach to incident response, adopt basic cybersecurity language in procurement contracts. (See the document Cybersecurity Procurement Language for Energy Delivery Systems).

Detect and Respond to Cybersecurity Incidents

The Playbook details the steps required to detect and identify potential cyber incidents. Containing an incident is a utility's immediate priority, the Playbook includes metrics to help a utility categorize and prioritize (ranging from Levels 0 to 5) the incident to determine the type of impact it made on the utility.

The Playbook outlines the steps necessary to escalate and report an incident, including engaging internal stakeholders, gathering evidence, and conducting initial containment. Investigating, developing resource solutions, and eradicating an incident are also key actions when responding to an incident. In addition to the actions described in the Playbook, a utility might also consider using a form to track an incident from start to finish to assist with lessons learned during debriefing and, when recovering from an incident, developing specific actions for fixing, patching, and/or stopping the security breach.

Incident Response Checklist:
Detect and Respond

- Implement *Incident Response Playbook* steps required to detect and identify potential cyber incidents:
  - Contain the incident
  - Escalate and report the incident
  - Investigate the incident
  - Eradicate the incident

Communicating During a Cyber Incident

A strong communications structure to be used during a cyber incident can mean the difference between an effective and an ineffective response. The Playbook recommends beginning with developing a communications strategy prior to a cyber incident. In addition to the Playbook recommendations, a utility should establish clear, consistent vocabulary and definitions of terms to alleviate confusion during an incident. The Playbook stresses legal and security considerations, such as consulting with the legal department on a communication plan and considering a partner organization's information sharing processes. In addition to Playbook guidance, determining legal reporting requirements is also recommended.

The flow and content of communications during a cyber incident will likely be different for internal and external stakeholders. Communications functions are essential both in normal operation and crisis response, and must be carefully planned in advance for quick and effective deployment. Building cyber awareness and related topics into regular communications can project subject authority to internal and external audiences and introduce the subject as an important and carefully considered undercurrent to organizational operations.

Incident Response Checklist: Communications

- Establish consistent vocabulary and definitions
- Involve your legal department
- Develop internal and external communications strategies
  - Internal Employees:
    Define communicative roles within the utility to ensure clear understanding of responsibilities and limits of acceptable authority
  - External Stakeholders:
    Establish a checklist for the types of information to be disclosed and when; notify customers
  - Media statements should:
    Confirm the incident; report cooperation with law enforcement or mutual assistance groups; emphasize the priority to ensuring continuing or restoring service

Internal communications focus on how to address the board, management, and personnel. Communications with these stakeholders should foster a culture of cyber awareness and security, and occur frequently to help integrate the subject into the organization's culture. An internal communications plan is necessary to keep employees and other key stakeholders abreast of the happenings of a cyber incident. Preparing (perhaps separate) statements to personnel and regulatory organizations is necessary depending on actions required from each group. Crisis communications with internal audiences must stress that they are representatives of the organization when speaking with anyone not directly affiliated with the organization, even casually. Organizations should define communicative roles for all personnel, management, and board positions, to ensure clear understanding of responsibilities and limits of acceptable authority.

External communications address customers, communities, interconnected peer organizations, and regulatory and oversight agencies, among others. Regular business-as-usual communication with customers and communities can cultivate a robust relationship better able to weather a crisis event. To ensure crisis communications address the needs and interests of each of the stakeholder groups, checklists for communications should be developed in advance, and procedures outlined for the type information to be disclosed and when, and the frequency at which stakeholders should be updated throughout an event.   If a statement to the media is necessary, it should: 1) confirm the incident; 2) report cooperation with law enforcement or mutual assistance groups; and 3) emphasize the organization's priority to ensuring continuing or restoring service. Following the initial statement to the media, provide frequent operational updates. If notifying customers is necessary, the announcement should include a range of information, including but not limited to contact information for further information, a short description of the data breach incident, the type and nature of the data compromised, and measures taken by the utility to prevent a future data breach.

Stage 4 - Integrate

Inputs:

- New policies, procedures, tools, or systems that enforce the desired improvements to cybersecurity from the project-based plan

Processes:

- Move new tools and systems into production environment and continue to operate and maintain them
- Operationalize and maintain the new processes as part of business-as-usual practices; this turns the "new" practices into "standard" practices
- Make the new behaviors part of the organization's culture to ensure changes last

Outputs:

- Achievement of the goals of the project-based plan
- New culture of cybersecurity ready for assessment via Scorecard and other tools to identify additional improvements to target

Systems

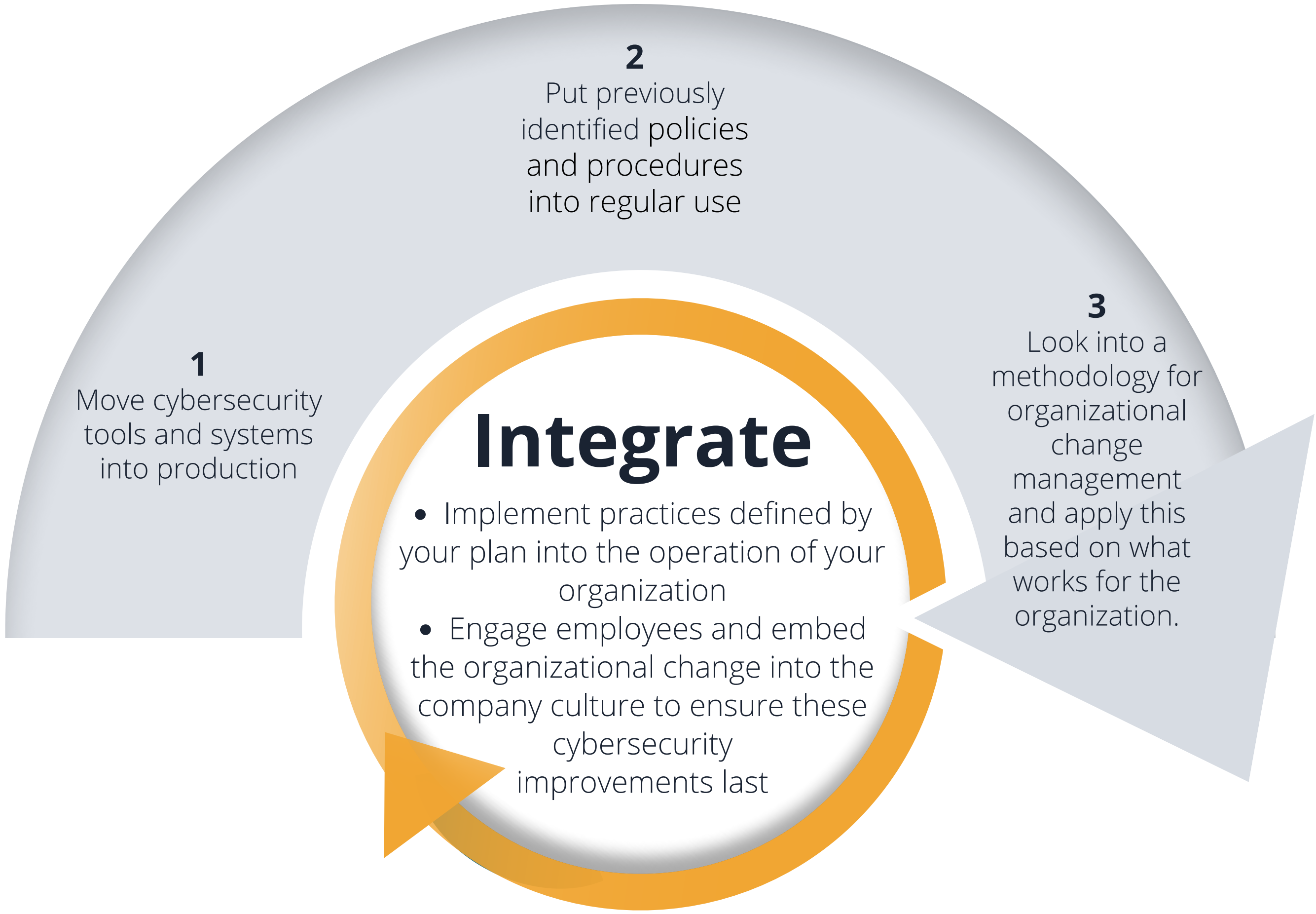
Cybersecurity protection, monitoring, or maintenance systems that have been tested and installed into the organization's IT or OT environment should be moved into production at this stage. Pay special attention to the impact that monitoring tools have on existing operational systems in a production environment. Some solutions include so-called "passive" monitoring to limit interference with standard operations. During integration and activation of any tool, it is critical that the project team assure there are no undue impacts on operations.
At this stage, the project team hands operation of new tools over to operations staff or maintains systems that are its responsibility.

Policies and Procedures

At this point, the policies and procedures identified and laid out earlier are moved into regular use. Given the operational nature of public power utilities, many organizations maintain written policies and procedures for IT, OT, and business and personnel functions. These procedural repositories are also appropriate locations for cybersecurity policies and procedures. However, given the novelty of these procedures, relevant stakeholders that haven't been exposed to the new practices will need training, and organizations will need to implement practices for sharing these procedures with new staff and vendors.

Organizational Adoption and Culture Change

As mentioned earlier in this Roadmap, perhaps the most challenging aspect of any significant project, especially one as far-reaching as organization-wide cybersecurity, is behavior change. The CRAC team recommended that public power utilities look into and apply a methodology for organizational change management based on what works for their organization. One example includes Prosci's ADKAR approach, which includes elements of awareness of the need for change, desire to support the change, knowledge of how to change, ability to demonstrate skills and behaviors, and reinforcement to make the change stick. Other change management methods offer approaches that may work in different organizations. In the context of a cybersecurity improvement plan, this Roadmap acknowledges these recommended change management steps from the beginning by engaging management and enrolling assistance (and endorsement) from across the organization. Training and development steps identified in earlier stages build knowledge and skills among staff. Ultimately, and most important to any cybersecurity improvement program, reinforcement of the changes can occur through continued staff awareness and training, as well as by revisiting the Public Power Cybersecurity Scorecard to determine the organization's next risk-based targets.



2
Put previously identified policies and procedures into regular use

1
Move cybersecurity tools and systems into production

3
Look into a methodology for organizational change management and apply this based on what works for the organization.

Integrate

- Implement practices defined by your plan into the operation of your organization
- Engage employees and embed the organizational change into the company culture to ensure these cybersecurity improvements last

Roadmap Next Steps

The guidance provided via this Roadmap is intended to promote improvement and ongoing maintenance and vigilance of critical infrastructure and private customer data. The Roadmap's stages and recommendations reflect input from individuals representing public power utilities that have prepared for, been exposed to, or addressed security threats in the hopes that others may learn and take action. The CRAC team members recommend maintaining a posture of continuous cybersecurity improvement, no matter the size of the public power utility. A utility can follow this recommendation by taking advantage of the resources and tools referenced in this document, including the Public Power Cybersecurity Scorecard and ES-C2M2. For the latest recommendations, visit the Association's website at www.PublicPower.org or email Cybersecurity@PublicPower.org.

Reading this document can provide insight into valuable and effective strategies for improved cybersecurity, but the success of any project lies in its execution. By providing a tested, collaborative baseline on which to build your cybersecurity program, the Association hopes that your organization is able to chart a path to an improved state. Communication among peers and collaboration with the Association and experienced subject matter experts might be necessary, and the tools to engage those resources are included in this document. The threat of a cyberattack may be very real and the scope of cybersecurity may be daunting, but by working together, we can improve the cybersecurity of the entire public power sector and continue to provide the best services to our communities and customers for years to come.

Appendix A: Example CISO Job Description

A Chief Information Security Officer (CISO) is the executive-level manager who directs the organization's cybersecurity strategy and budget and governs the cybersecurity information and system operations protection. The scope of responsibility encompasses policy, communications, training, procurement, development, infrastructure, systems, and applications.

Related Position Title

Other titles used to describe this position include:

- Chief Security Officer (typically also includes physical security responsibilities)
- Corporate Security Executive
- Information Security Director (may not be an executive-level position)
- Corporate Security Officer (may not be an executive-level position)
- Information Security Officer (typically not an executive-level position)
- Information Security Manager (not an executive level-position; may not have budget)
- Information Systems Security Manager (responsibility typically limited to systems)

In small- to medium-sized organizations, the CISO responsibilities may be part of an existing executive level position such as CEO or CIO.

CISO Responsibilities & Duties

The CISO and the CISO team typically are responsible for the following:

- Strategy: Create, manage, and update the organization's cyber security strategy to address organizational cybersecurity concerns, threats, regulations, and technology.
- Policy: Direct, create and manage information security policies and standards; direct and approve information security procedures.
- Requirements: Define and advise regarding the implementation of cybersecurity requirements for existing and developed applications and outsourced services.
- Design: Consult and advise how to incorporate adequate security controls into system designs.
- Assess: Ensure adequate cybersecurity assessments of existing controls, including security risk assessments, vulnerability scanning, penetration testing, code review, user rights reviews, and compliance gap assessments.
- Mitigate Risk: Design, advise, and oversee the revision or creation of cybersecurity controls adequate to address known cybersecurity risks consistent with the risk appetite of the organization.
- Log and Monitor: Ensure appropriate application and system logging takes place and that these logs are reviewed for cybersecurity incidents.
- Investigate: Direct cybersecurity incidents, disclosures, or breach investigations, including impact analysis and appropriate internal notifications.
- Response: Ensure effective response and lessons learned to cybersecurity incidents, disclosures, and breaches.
- Communicate: Appropriately communicate externally in response to disclosures and breaches.
- Continuity: Ensure disaster recovery and business continuity plans incorporate adequate cybersecurity controls and are tested and updated.
- Compliance: Ensure cybersecurity compliance with relevant laws, regulations, standards and contracts
- Vendor Management: Manage cybersecurity requirements and oversight of vendors providing services to the organization.
- Threat Intelligence: Maintain a current understanding of relevant cybersecurity threats impacting the industry and the organization.
- Security Awareness: Ensure all personnel receive effective security awareness training and updates.
- Inform Board: Communicate cybersecurity risks and strategy to board members and executive committee and address concerns.

Appendix B: Resources and References

Resources

1. U.S. Department of Energy Cybersecurity Capability Maturity Model (C2M2): https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity-0-0

2. APPA Cybersecurity Resources page: https://www.publicpower.org/topic/cybersecurity

3. Public Power Cybersecurity Scorecard: https://www.publicpower.org/resource/cybersecurity-scorecard

4. For additional analyses of FISMA security controls, see: Landoll, Douglas J., *Information Security Policies, Procedures, and Standards: A Practitioner's Reference*, CRC Press 2016

All photos courtesy of Pixabay

AMERICAN PUBLIC POWER ASSOCIATION
Powering Strong Communities

2451 Crystal Drive
Suite 1000
Arlington, VA 22202-4804

www.PublicPower.org

#PublicPower

Public Power Cybersecurity Roadmap

General Overview

The cybersecurity landscape is complex, and the threats posed to public power are real. Establishing and managing a cybersecurity program can be a daunting task, which is why the American Public Power Association worked with experts to develop the Public Power Cybersecurity Roadmap. The Roadmap is a strategic plan to help public power utilities define their journey of cybersecurity improvement and work to form a stronger, consistent state of security for their organization.

The Roadmap builds on the Public Power Cybersecurity Scorecard, which helps assess an organization's maturity in cybersecurity operations and practices. Using findings from the Scorecard, the Roadmap facilitates a utility's path to an improved state of cybersecurity. It breaks down the broad-ranging and sometimes intimidating scope of cybersecurity practices into four distinct, manageable subdivisions. As a utility moves through the Roadmap, the Scorecard can provide a useful standard for monitoring and measuring improvements to organizational cybersecurity practices.

Together, the Scorecard and the Roadmap provide a strategic framework designed to help utilities plan and deploy cybersecurity efforts over the next three to five years. The Roadmap is intended to be used both by public power utilities that are just beginning to address improvements in cybersecurity and those with more advanced cybersecurity efforts. The Roadmap provides recommendations in a prioritized manner, but allows for flexibility so that a utility can "join" at any point or tailor the implementation of recommendations in an order that suits its individual needs.

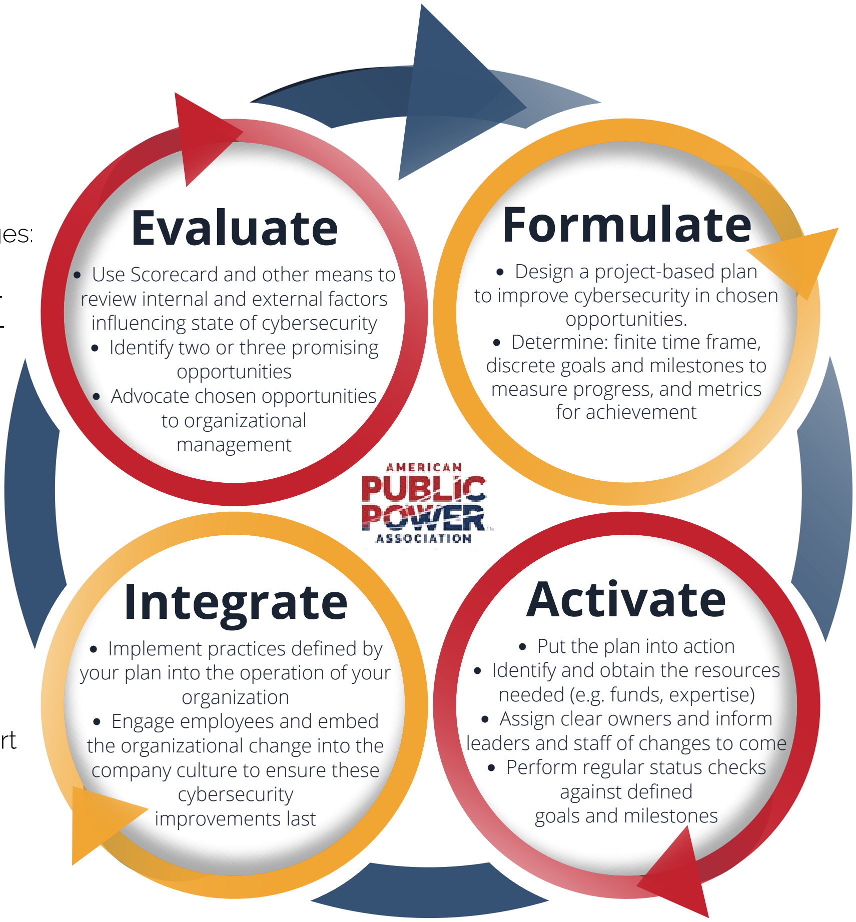
The Roadmap helps utilities to successfully achieve their program goals through four stages:

STAGE 1: EVALUATE internal and external factors influencing the most pressing cybersecurity issues and identify two to three promising opportunities to target.

STAGE 2: FORMULATE a project-based plan to improve cybersecurity in the two to three identified areas.

STAGE 3: ACTIVATE the project-based plan by conducting the plan's activities.

STAGE 4: INTEGRATE practices defined by the plan into the operation and risk management of the organization and make them a part of the organization's culture.



Evaluate

- Use Scorecard and other means to review internal and external factors influencing state of cybersecurity
- Identify two or three promising opportunities
- Advocate chosen opportunities to organizational management

Formulate

- Design a project-based plan to improve cybersecurity in chosen opportunities.
- Determine: finite time frame, discrete goals and milestones to measure progress, and metrics for achievement

Integrate

- Implement practices defined by your plan into the operation of your organization
- Engage employees and embed the organizational change into the company culture to ensure these cybersecurity improvements last

Activate

- Put the plan into action
- Identify and obtain the resources needed (e.g. funds, expertise)
- Assign clear owners and inform leaders and staff of changes to come
- Perform regular status checks against defined goals and milestones

Click the image to enlarge.

Stage 1: Evaluate

Inputs:

- Public Power Cybersecurity Scorecard assessment
- Existing cybersecurity processes and procedures
- Personnel training and awareness

Processes:

- Gain initial support for cybersecurity efforts from sponsors and stakeholders
- Use Scorecard to evaluate organizational processes
- Generate a list of goals for improving cybersecurity and use a risk-based approach to identify two or three promising opportunities for improving cybersecurity from these goals
- Define the means to achieve these goals, and gain funding for and endorsement of the project process, goals, and scope from organizational management

Outputs:

- Two or three defined, achievable goals that will improve the organization's cybersecurity
- Endorsement of project by relevant sponsors

Stage 2: Formulate

Inputs:

- Defined goals for improving cybersecurity
- Support from sponsors and leadership

Processes:

- Generate a project-based plan by which to achieve the priority goals
- Build plan starting with the current state of cybersecurity
- Identify relevant milestones by which to mark and measure progress

Outputs:

- An actionable plan project leaders and process-level personnel can use to understand the goals, purposes, and needs for each stage of the project

Stage 3: Activate

Inputs:

- Project-based plan to improve cybersecurity

Processes:

- Use the plan as a guide to launch new practices, policies, and protocols; conduct activities noted in the plan
- Review and revise policies to enforce new practices, including rewarding compliance and penalizing noncompliance

Outputs:

- New organizational standards for practice and behavior that help the organization achieve its cybersecurity goals
- New tools and/or systems to enforce standards and reduce risk

Stage 4: Integrate

Inputs:

- New policies, procedures, tools, or systems that enforce the desired improvements to cybersecurity from the project-based plan

Processes:

- Move new tools and systems into production environment and continue to operate and maintain them
- Operationalize and maintain the new processes as part of business-as-usual practices; this turns the "new" practices into "standard" practices
- Make the new behaviors part of the organization's culture to ensure changes last

Outputs:

- Achievement of the goals of the project-based plan
- New culture of cybersecurity ready for assessment via Scorecard and other tools to identify additional improvements to target