# POWER SECTOR CYBERSECURITY BUILDING BLOCKS

Maurice Martin, Tami Reynolds, Anuj Sanghvi, Sadie Cox, and
James Elsworth

*National Renewable Energy Laboratory*

March 2021

A product of the USAID-NREL Partnership
Contract No. IAG-17-2050

## NOTICE

This work was authored, in part, by the National Renewable Energy Laboratory (NREL), operated by Alliance for Sustainable Energy, LLC, for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308. Funding provided by the United States Agency for International Development (USAID) under Contract No. IAG-17-2050. The views expressed in this report do not necessarily represent the views of the DOE or the U.S. Government, or any agency thereof, including USAID.

*Cover photo from iStock 538144351.*

NREL prints on paper that contains recycled content.

# Acknowledgements

The authors would like to thank Jamila Amodeo from the U.S. Agency for International Development for her thought leadership and instrumental guidance in developing the power sector cyber security building blocks as well as for her thoughtful review and input to this publication.

# List of Acronyms

| | |
|---|---|
| CEO | chief executive officer |
| CTI | cyber threat intelligence |
| DER-CF | Distributed Energy Resource Cybersecurity Framework |
| ICS | industrial control system |
| IDS | intrusion detection system |
| IEC | International Electrotechnical Commission |
| ISACS | Information Sharing and Analysis Centers |
| ISO | International Organization for Standardization |
| NIST | United States National Institute of Standards and Technology |
| NREL | National Renewable Energy Laboratory |
| SCADA | supervisory control and data acquisition |
| USAID | U.S. Agency for International Development |

# Table of Contents

# List of Figures

# List of Tables

# 1 Power Sector Cybersecurity Building Blocks

The Power Sector Cybersecurity Building Blocks, developed through the U.S. Agency for International Development (USAID)-National Renewable Energy Laboratory (NREL) Partnership[1] and the partnership's Resilient Energy Platform,[2] are designed to help a variety of stakeholders improve security for the electrical grid. This effort grows out of USAID and NREL's discussions with utilities around the world, as well as past cybersecurity assessments performed by NREL on dozens of utilities and government agencies, with a focus on the cybersecurity challenges faced by small and under-resourced utilities.

This document outlines eleven **building blocks** for power sector cybersecurity (Figure 1). It functions as a guide to help organizations develop a robust cybersecurity defense program. Individually, each building block represents a cluster of related activities within cybersecurity on which an organization should focus. Using the building blocks, organizations can effectively prioritize their cybersecurity efforts to best thwart a wide range of potential cyberattacks.

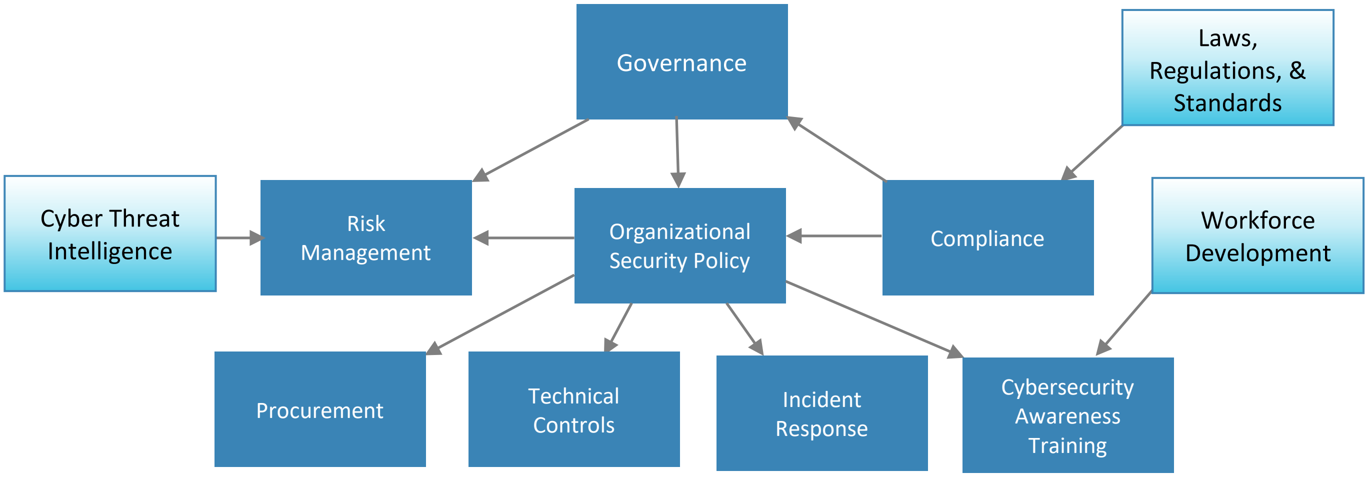

Governance
Laws, Regulations, & Standards
Cyber Threat Intelligence
Risk Management
Organizational Security Policy
Compliance
Workforce Development
Procurement
Technical Controls
Incident Response
Cybersecurity Awareness Training

**Figure 1. Power sector cybersecurity building blocks**

Note: Solid color blocks are internal to the utility; shaded blocks are external to the utility.

## 1.1 About the Building Blocks

### *1.1.1 The Need*

There are already many excellent guides, standards, and frameworks for organizations seeking to improve cybersecurity. Some are produced by standards bodies, such as the International Organization for Standardization (ISO). Others are produced by government agencies, such as the United States National Institute of Standards and Technology (NIST). Equipment vendors,

[1] USAID-NREL Partnership: https://www.nrel.gov/usaid-partnership.

[2] Resilient Energy Platform: https://resilient-energy.org.

consultants, and nonprofits have also created useful resources. Selections from and references to these guides, standards, and frameworks appear throughout this document.

However, many organizations still struggle to create a cybersecurity program that is balanced across all areas required to protect their assets from attack. They may have heavy investments in one area, with little investment in another. For these organizations, the "building block" approach will hopefully prove useful. **The building blocks define clusters of related activities within a balanced cybersecurity program** and provide references and resources for each area. Since the building blocks correspond to activities, staff time and resources need to be allocated to them in the same way that staff time and resources are allocated to noncyber activities (such as accounting).

The building blocks are interconnected, with some building blocks feeding information to others, and mutually supporting, in that each depends on others to facilitate a holistic approach to cybersecurity. The building blocks and their interconnections are depicted in Figure 1.

**Box 1: The Resilient Energy Platform**

The Resilient Energy Platform helps countries and localities address power system vulnerabilities by providing strategic resources and directing country support to enable planning and deployment of resilient energy solutions. This includes curated reference material, training materials, data, tools, and direct technical assistance in planning resilient, sustainable, and secure power systems. Ultimately, these resources enable decision makers to assess power sector vulnerabilities, identify resilience solutions, and make informed decisions to enhance energy sector resilience at a range of scales, including local, regional, and national. To learn more, visit the Resilient Energy Platform website at: https://resilient-energy.org/.

The clusters of related activities defined by the Power Sector Cybersecurity Building Blocks span multiple stakeholders. In the figures throughout this document, the solid color rectangles correspond to building blocks within a utility, while the shaded rectangles are external to a utility. The arrows show major categories of information passing between building blocks. (These arrows are labeled in Figures 2–12 and discussed in the accompanying text.)

Organizations in the early stages of cybersecurity maturity will likely get the most benefit from these building blocks, because they are likely to struggle with the question of what a complete cyber program looks like. More "cyber mature" organizations can also use the building blocks to gain a fresh perspective on their efforts and fill in gaps in their existing cyber programs.

The Power Sector Cybersecurity Building Blocks are not meant to be the final word on cybersecurity for the power sector, as this field is evolving rapidly with the introduction of new power grid technology and an ever-changing threat landscape. USAID and NREL welcome discussion regarding updates to future iterations of these building blocks.

### 1.1.2 Brief Descriptions

- **Governance:** The processes that direct a utility-wide cybersecurity effort and provide accountability for that effort. Cybersecurity governance requires the understanding and action of those at the very top level of the utility, such as the executive director, chief executive officer (CEO), board of directors, and others.

- **Organizational Security Policy:** This building block focuses on the high-level document that captures the essential elements of a utility's efforts in cybersecurity and includes the effort to create, update, and implement that document.
- **Risk Management:** Activities that identify and evaluate cybersecurity risk, with the goal of reducing that risk to a level appropriate to the utility's business objectives.
- **Cyber Threat Intelligence (CTI):** Cyberattack tools and adversaries that might constitute a threat and the vulnerabilities they could exploit. Utilities need CTI to understand the threat landscape and take action to mitigate cyber risks.
- **Laws, Regulations, and Standards:** Laws and regulations are the compulsory host country directives that a utility must comply with regarding cybersecurity. Regulations sometimes enforce standards created by nongovernmental entities that capture best practices.
- **Compliance:** The effort within a utility to remain in compliance with laws, regulations, and standards.
- **Procurement:** The processes used to monitor and improve the cybersecurity of devices, applications, and services as they are acquired and integrated into utility operations, as well as efforts to manage supply chain risk.
- **Technical Controls:** The hardware and software components that protect a system against cyberattack. Firewalls, intrusion detection systems (IDS), encryption, and identification and authentication mechanisms are examples of technical controls.
- **Incident Response:** The actions taken by a utility to prepare for cyberattacks. This includes creating plans for response, rehearsing the response prior to an attack, continuous monitoring to identify attacks, and the actual response.
- **Cybersecurity Awareness Training:** Steps taken by utilities to educate all employees (including nontechnical staff) about potential cyber threats and their roles in preventing them.
- **Workforce Development:** The efforts by multiple organizations, such as government, industry, or academia, to ensure an adequate supply of workers with specialized cybersecurity knowledge and skills.

### 1.1.3 Structure

Each building block includes an introduction, as well as the following subsections:

- **Importance.** Why the building block deserves attention.
- **Intersections with Other Building Blocks.** Major categories of information passed between this building block and others. (Includes a diagram zooming in on part of Figure 1.)
- **Processes and Actions.** Key activities within each building block.
- **Essential Data.** The information that an organization needs to collect or generate to be effective in each building block.
- **Recommended Reading.** A short list of reports and articles that address the key activities defined in the building blocks.

Note that the appendix at the end of this document includes references (citations that appear in the text) and more resources for each building block.

# 2 Governance

Power sector cybersecurity *governance* provides oversight for a utility's cybersecurity efforts. Through governance, the utility board of directors, chief executive officer (CEO), executive leadership, and other decision makers seek to balance resource allocation, risk, and business objectives. These leaders must factor in the risk associated with cyberattacks, as well as the need to comply with national, regional, provincial, or state cybersecurity regulations. Their role is to look at cybersecurity holistically, factoring in data about current cyber vulnerabilities as well as the impact of anticipated system upgrades, increased digitalization, and system expansion.

## 2.1 Importance

If the upper levels of an organization do not demonstrate commitment to cybersecurity, the utility's efforts to improve cybersecurity will enjoy little success (if any). One way to demonstrate that commitment is through allocation of resources to pay for staff time, tools, and, possibly, outside consultation. Cybersecurity governance needs to ensure those resources go where they are really needed—it is easy for organization-wide cybersecurity programs to become "lopsided," investing too much in one area and not enough in another. Cybersecurity governance includes the work of making sure overall security efforts effectively meet the needs of the utility.

Another way for utility leadership to demonstrate commitment is by impressing on staff that everyone has a role to play in cybersecurity. They must communicate this through words as well as actions, leading by example. If staff see leadership ignoring cybersecurity policies and guidelines, they will quickly realize that leadership is not serious about this topic. By "walking the walk" as well as "talking the talk," leaders can foster a culture of cybersecurity that will help protect the utility from future cyberattacks. (For more on this topic, see the **cybersecurity awareness training** building block.)

## 2.2 Intersections with Other Building Blocks

The **governance** building block provides input (through executive directives) that informs the development of the organizational security policy, the document that defines the utility's cybersecurity efforts. The decision makers of the governance building block determine what cybersecurity will look like; the organizational security policy captures these decisions and presents them as actionable measures to be taken.

Governance must include compliance with all applicable regulations, so a high-level summary of regulatory requirements is provided by the **compliance** building block.

Governance must set the risk objectives and business requirements that define the scope of the utility's **risk management** building block.

These organizational security policy, compliance, and risk management building blocks have the most interaction with governance; however, the governance building block also relies on data, reports, and other types of information from all other building blocks that might inform high-level decision-making.

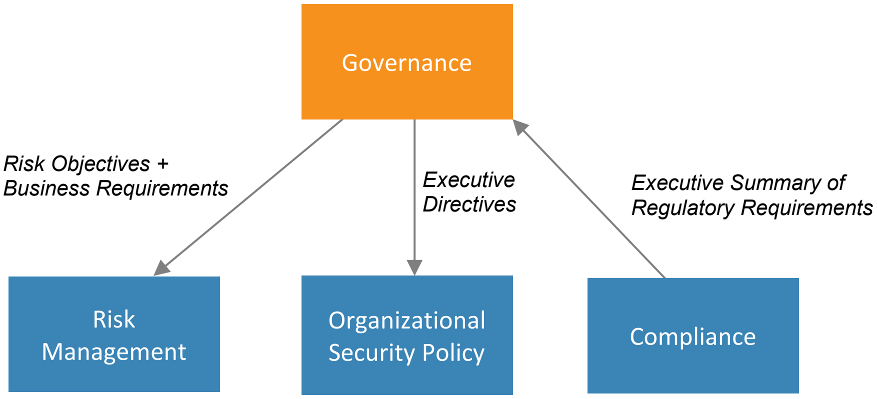

Governance
Risk Objectives + Business Requirements
Executive Directives
Executive Summary of Regulatory Requirements
Risk Management
Organizational Security Policy
Compliance

**Figure 2. Information passed to and from the governance building block**

## 2.3 Process and Actions

The **governance** building block integrates the work of other building blocks, so there is overlap between the governance processes and actions and those in other building blocks throughout this document. Table 1 maps governance processes from the NIST's *Framework for Improving Critical Infrastructure Cybersecurity* (NIST 2018) to the building blocks that provide detail on each. In the context of the NIST framework, these processes are subcategories within the category of governance.

**Table 1. NIST Governance Processes**

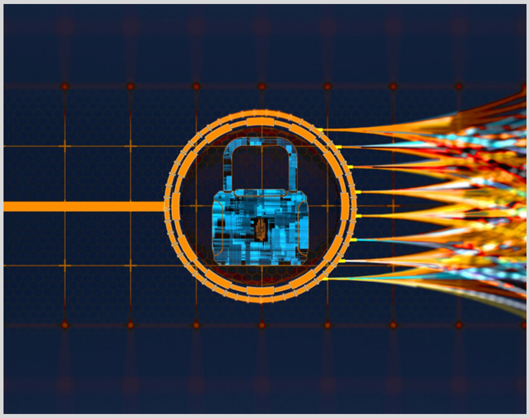
| From the NIST *Framework* | Mapping to Building Blocks |
|---|---|
| "Organizational cybersecurity policy is established and communicated." | Organizational Security Policy |
| "Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners." | Governance |
| "Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed." | Compliance |
| "Governance and risk management processes address cybersecurity risks." | Risk Management |

Assigning roles and responsibilities (second row in Table 1) is uniquely a cybersecurity governance activity. The utility's high-level decision makers must determine who will execute which parts of their cybersecurity policy and set up the necessary reporting and oversight structures needed to ensure those responsibilities are fulfilled.

This oversight requires a certain level of cybersecurity knowledge on the part of those decision makers. Unfortunately, not all leaders have the necessary knowledge in this area (Rothrock, Kaplan, and Van der Oord 2017). CEOs or board directors do not need to be experts in cybersecurity, but they need enough understanding to make informed decisions. Some commercial entities offer executive and board cybersecurity readiness programs (Tyler Cybersecurity n.d.). Some associations also offer guidance to boards of directors (NACD 2020) with select excerpts from those resources available online (Bew n.d.). These resources offer some ways these decision makers can acquire the requisite knowledge for executing their cybersecurity responsibilities.

For utilities that wish to benchmark the state of their cybersecurity governance, an assessment is available from the NREL. The Distributed Energy Resource Cybersecurity Framework (DER-CF) assessment tool covers three areas, one of which is governance (NREL n.d.). See box at right for details.

**Box 2: DER-CF**



DER-CF assessments address governance, technical management, and physical security. DER-CF can be used for free as a self-assessment tool, and users can take the assessment as an anonymous guest of the system. (In that case, the utility does not need to identify itself by name, and no data associated with the assessment is stored on the DER-CF system.) NREL can also guide utilities through DER-CF assessments; some utilities appreciate the participation of an outside party that can facilitate the process and communicate results to utility leadership. To learn more about DER-CF, visit **https://dercf.nrel.gov.**

## 2.4 Essential Data

Utilities should collect or generate the data below for effective governance.

- High-level information on regulatory requirements. This is generated in the **compliance** building block.
- High-level information on risk, threats, and vulnerabilities affecting the utility. This is collected from CTI and distilled by the **risk management** building block.
- Budget information. How much can the utility spend on cybersecurity? How much will compliance cost, and how much is left over to mitigate risks not covered by compliance efforts?
- Internal equipment resources. What tools and technology does the utility have for their cybersecurity efforts?
- Internal human resources. What cybersecurity expertise does the utility have in-house for the various cybersecurity activities that need to be performed? Also, how well do all the

staff understand the basics of responsible, cyber-safe use of computers? (See the **cybersecurity awareness training** building block.)

- External resources. Where might the utility get outside help such as advice, consultation, and training? These resources could include government agencies, academics, commercial training enterprises, consultants, or not-for-profit entities.

***References and more resources for this building block appear in the appendix under "Governance."***

# 3 Organizational Security Policy

The *organizational security policy* is the document that defines the scope of a utility's cybersecurity efforts. It serves as the repository for decisions and information generated by other building blocks and a guide for making future cybersecurity decisions. The organizational security policy should include information on goals, responsibilities, structure of the security program, compliance, and the approach to risk management that will be used.

## 3.1 Importance

The organizational security policy serves as a reference for employees and managers tasked with implementing cybersecurity. What has the board of directors decided regarding funding and priorities for security? What new security regulations have been instituted by the government, and how do they affect technical controls and record keeping? Which approach to risk management will the organization use? How will the organization address situations in which an employee does not comply with mandated security policies?

The organizational security policy serves as the "go-to" document for many such questions. It expresses leadership's commitment to security while also defining what the utility will do to meet its security goals.

## 3.2 Intersections with Other Building Blocks

Because the organizational security policy plays a central role in capturing and disseminating information about utility-wide security efforts, it touches on many of the other building blocks. The **governance** building block produces the high-level decisions affecting all other building blocks. The **compliance** building block specifies what the utility must do to uphold government-mandated standards for security. The organizational security policy captures both sets of information.

The utility's approach to risk management (the framework it will use) is recorded in the organizational security policy and used in the **risk management** building block to develop a risk management strategy. Objectives defined in the organizational security policy are passed to the **procurement**, **technical controls**, **incident response**, and **cybersecurity awareness training** building blocks.

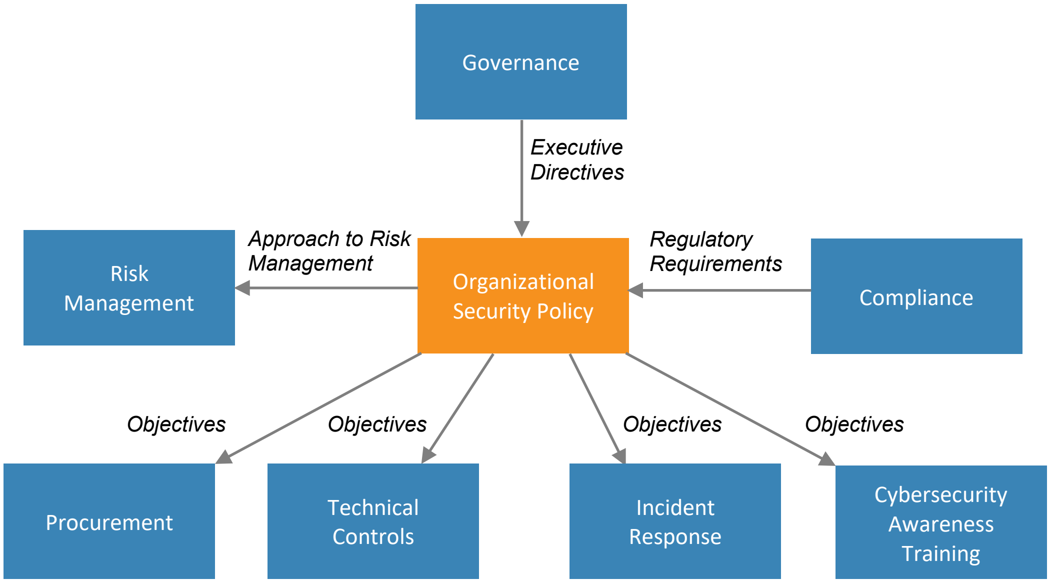


**Figure 3. Information passed to and from the organizational security policy building block**

## 3.3 Process and Actions

Developing an organizational security policy requires getting buy-in from many different individuals within the organization. The policy needs an "owner"—someone with enough authority to get the right people involved from the start of the process and to see it through to completion. The owner will also be responsible for quality control and completeness (Kee 2001). Appointing this policy owner is a good first step toward developing the organizational security policy.

The policy owner will need to identify stakeholders, which will include technical personnel, decision makers, and those who will be responsible for enforcing the policy. Ideally, the policy owner will be the leader of a team tasked with developing the policy. Everyone must agree on a review process and who must sign off on the policy before it can be finalized.

The utility decision makers—board, CEO, executive director, and so on—must determine the business objectives that the policy is meant to support and allocate resources for the development and implementation of the policy. Business objectives should drive the security policy—not the other way around (Harris and Maymi 2016, 88).

The utility will need to develop an inventory of assets, with the most critical called out for special attention. Threats and vulnerabilities should be analyzed and prioritized. Mitigations for those threats can also be identified, along with costs and the degree to which the risk will be reduced.

The policy will identify the roles and responsibilities for everyone involved in the utility's security program. The utility leadership will need to assign (or at least approve) these responsibilities. Objectives for cybersecurity awareness training objectives will need to be specified, along with consequences for employees who neglect to either participate in the training or adhere to cybersecurity standards of behavior specified by the organization (see the **cybersecurity awareness training** building block for more details).

The policy can be structured as one document or as a hierarchy, with one overarching master policy and many issue-specific policies (Harris and Maymi 2016, 88). The SANS Institute offers templates for issue-specific policies free of charge ("Security Policy Templates" n.d.); those templates include:

- Acceptable encryption policy
- Data breach response policy
- Internet usage policy
- Remote access policy
- Risk assessment policy
- Social engineering awareness policy
- Virtual private network policy.

When the policy is drafted, it must be reviewed and signed by all stakeholders. A cycle of review and revision must be established, so that the policy keeps up with changes in business objectives, threats to the organization, new regulations, and other inevitable changes impacting security.

## 3.4 Essential Data

The following information should be collected when the organizational security policy is created or updated, because these items will help inform the policy.

- A list of stakeholders who should contribute to the policy and a list of those who must sign the final version of the policy
- An inventory of assets prioritized by criticality
- Historical data on past cyberattacks, including those resulting from employee errors (such as opening an infected email attachment). This will supply information needed for setting objectives for the **cybersecurity awareness training** building block.
- Threats and vulnerabilities that may impact the utility.

In addition, the utility should collect the following items and incorporate them into the organizational security policy:

- Business objectives (as defined by utility decision makers)
- Laws, regulations, and standards applicable to the utility, including those focused on safety, cybersecurity, privacy, and required disclosure in the case of a successful cyberattack.

***References and more resources for this building block appear in the appendix under "Organizational Security Policy."***

# 4 Risk Management

*Risk management* is the practice of organizing and prioritizing risk reduction throughout an organization. The needs and mission of the organization will determine the priority in which the risks are addressed. Risk cannot be eliminated entirely; there will always be some level of residual risk, even after mitigation. Determining how much risk the organization is willing to assume is a challenge every organization faces.

## 4.1 Importance

Managing cybersecurity risk is critical to the operation of an energy system and everything that relies on it. The risks an organization faces determine key areas that need special attention to avoid potential threats. Being aware of the risks will help an organization determine how much risk they are willing to assume. Once risks have been identified and prioritized, a plan of action can address and help mitigate vulnerabilities. (For a definition of "risk" and other risk management terms, see Box 3)

Risk management is a time- and labor-intensive process. Having a cybersecurity risk management strategy focused on avoidance, assessing, and mitigating risk will help provide structure and continuity to the organization.

## 4.2 Intersections with Other Building Blocks

Decisions about risk objectives are business decisions and thus are made at the highest level of the utility (by the board of directors, CEO, executive director, and so on). Is the objective of the utility to increase service reliability? Decrease incidents involving malware? Reduce cost? Decisions like these are part of the **governance** building block and are shared with the **risk management** building block in the form of risk objectives and business requirements.

Cybersecurity risk management touches every aspect of an organization and is dependent on good policies and procedures. The organizational security policy captures the utility's approach to cyber risk management. This includes clearly identified roles and responsibilities, which create accountability for risks across the organization.

Risk management must take into account the changing threat landscape as expressed by CTI. Most utilities depend on outside sources for this information, which includes details of emerging threats (e.g., new hacking groups), new vulnerabilities (e.g., a newly discovered operating system security flaw), and new cyberattack tools (e.g., new malware).

Incorporating CTI into risk management enables a utility to identify possible threats and vulnerabilities and create a plan to mitigate them. This plan should include prioritizing the threats based on the level of risk identified by the organization. The higher the risk to mission-critical operations, the higher that threat should appear on the prioritized list.

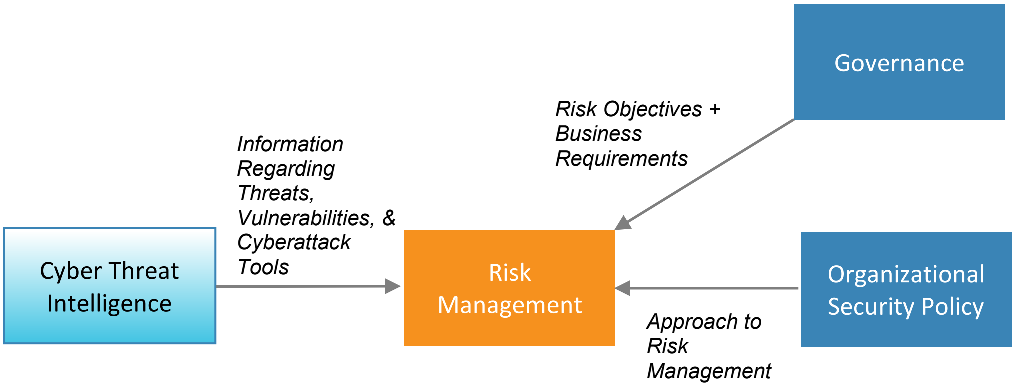

Governance
Risk Objectives + Business Requirements
Information Regarding Threats, Vulnerabilities, & Cyberattack Tools
Cyber Threat Intelligence
Risk Management
Organizational Security Policy
Approach to Risk Management

**Figure 4. Information passed to and from the risk management building block**

## 4.3 Process and Actions

Organizations have four choices when deciding how to handle risk:

- *Avoid the risk.* If an application or staff behavior introduces a risk, simply disallow it. For example, if employees checking their personal email on work computers is allowing malware onto the network, then do not allow personal email on work computers.
- *Accept the risk.* Access whether the risk is one that can be "lived with." In making this decision, organizations need to carefully consider the potential harm that the risk represents and the likelihood of that risk coming to pass.
- *Mitigate the risk.* Put in place security controls that lower the amount of risk. For example, placing a firewall between an internal network and the public internet lowers the risk of a network-based attack. Note that it does not eliminate the risk completely; the intention is to bring the risk down to a level where it can be accepted. The risk remaining after a security control is added is referred to as *residual risk*.
- *Transfer the risk.* Make another party responsible for the risk. The classic example of this is purchasing insurance, which transfers the risk to an insurance company.

Decisions about how to handle different types of risk and other risk-related choices are best addressed through a *risk management strategy*. This will identify proper placement cybersecurity controls throughout the information technology (IT) and industrial control system (ICS) environments. The strategy should include regular vulnerability and risk assessments that will help determine which risks are present; these risks are then captured in a document called the *risk register*. Part of the risk management strategy is to select risk metrics to rank or prioritize risks. Creating the risk management strategy requires effort, but the payoff is streamlined business processes and decision making.

There are several different models and methodologies to aide in the risk management process. The items below are adapted and abridged from the *Electricity Subsector Cybersecurity Risk Management* Process (U.S. Department of Energy 2012).

A well-documented cybersecurity risk management strategy should include, but is not limited to, the following:

- Identify key stakeholders with their respective roles and responsibilities. The U.S. Department of Energy's Risk Management Process lists many possible stakeholders including senior leaders, business process owners, chief information or security officers, and information system owners. However, not all of these are likely to have the availability and/or interest to participate in risk management activities.
- Define techniques and methodologies for assessing and prioritizing cybersecurity risks and vulnerabilities.
- Identify and prioritize the organization's risks based on the mission and what is most critical, the likelihood the risk will be realized, and the severity of the impact if the risk is realized. This requires an understanding of systems and assets, their interconnections, communication parameters, and behaviors.
- Establish the organization's risk tolerance. How much risk is the organization willing/able to assume? The organization's risk tolerance should consider what it will take for the organization to recover should an event occur.
- Create a risk-aware business processes that account for cybersecurity threats and risks and recommend preventive actions.
- Identify and prioritize IT and ICS assets necessary to support the risk-aware business processes.
- Establish a process to routinely reassess a system's cybersecurity posture based on new threat information, vulnerabilities, or system changes.

For a more detailed approach and description of the Risk Management Process, refer to the *Electricity Subsector Cybersecurity Risk Management Process*s (U.S. Department of Energy 2012).

## 4.4 Essential Data

The utility should collect the following information as the cybersecurity risk management strategy is developed:

- A list of key organizational stakeholders
- Organization-wide risk management strategy: In other words, any existing strategies for risk management that are not specific to cybersecurity. The cybersecurity risk management strategy will need to be harmonized with these other strategies.
- Organization's mission
- Organization's strategic goals and objectives
- Current business processes for IT and ICS assets
- Asset inventory prioritized according to mission criticality
- Defined roles and responsibilities pertaining to cybersecurity.

**Box 3: Risk Management Terminology**

- **Threats.** Anything that can damage, destroy, or disrupt the power sector. Threats can be natural, technological, or human-caused. Threats are not typically within the control of power system planners and operators. They can include wildfires, hurricanes, storm surges, cyberattacks, and more.
- **Impact.** The extent to which a threat affects power sector infrastructure, systems, or processes (e.g., a tornado causes wind damage to transmission lines).
- **Vulnerability.** A weakness within infrastructure, processes, and systems, or the degree of susceptibility to various threats. Different measures can be taken to reduce vulnerability or improve adaptive capacity to threats to the power sector.
- **Risk.** The potential for loss, damage, or destruction of key resources or power system assets resulting from exposure to a threat. Risk is sometimes evaluated as the product of the threat likelihood and the system vulnerability.

A discussion of these terms and a resource for quantifying and ranking risks can be found at **https://resilient-energy.org/guidebook**.

***References and more resources for this building block appear in the appendix under "Risk Management."***

# 5 Cyber Threat Intelligence

*Cyber Threat Intelligence (CTI)* is information about the threats, vulnerabilities, and cyberattack tools that an organization needs to understand to better defend itself. CTI is collected by government agencies, nonprofits, academics, and commercial entities. These organizations publish notifications and alerts as threats evolve, new vulnerabilities are discovered, and new attack tools are identified. CTI is sometimes made available free of charge and sometimes requires a paid subscription. Information Sharing and Analysis Centers (ISACs) provide CTI for specific industries (e.g., electricity, aviation, and financial services).

## 5.1 Importance

By keeping up to date on CTI, an organization can optimize their cybersecurity efforts and better allocate their cybersecurity budgets to assess and address vulnerabilities that may be the target of specific cyber threats. When ransomware is on the rise, for example, investments in more staff education focused on cybersecurity awareness training will reduce the vulnerability of an undereducated staff (who might, for instance, open a malware-infected email attachment). If network-based attacks are increasing, consider more network isolation and intrusion detection. Knowing who might attack, how they might attack, and the vulnerabilities they might exploit makes an organization more prepared to defend itself.

## 5.2 Intersections with Other Building Blocks

The **cyber threat intelligence** building block shares with the **risk management** building block information about emerging threats (e.g., new hacking groups), new vulnerabilities (e.g., a newly discovered operating system security flaw), and new cyberattack tools (e.g., new malware). This gives risk management a more complete picture of risks facing the organization and is used to focus and prioritize security resources.

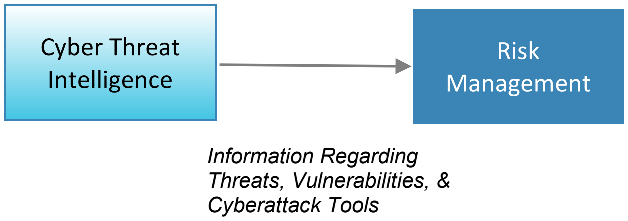

Cyber Threat Intelligence
Risk Management
Information Regarding Threats, Vulnerabilities, & Cyberattack Tools

**Figure 5. Information passed from the cyber threat intelligence building block**

## 5.3 Processes and Actions

CTI is produced by nonprofits, government agencies, and for-profit enterprises that specialize in monitoring and analyzing the ever-changing cyber threat landscape. CTI is consumed by many types of organizations (including utilities); however, before an organization begins monitoring CTI sources, they should create a thorough inventory of their assets—the systems, devices, applications, and software they use. These assets should be prioritized by criticality. This prioritized asset list enables the organization to focus on alerts and notifications that are most relevant. If an alert or notification addresses a threat to a type of device that the organization does not have, it can be ignored. Alternately, if the organization has the device but is using it in a setting with low or middle criticality, there is less urgency to respond to the alert or notification. The inventory of assets, prioritized by criticality, enables prioritization of response.

Next, the organization needs to decide which sources of CTI it will monitor. There are many; organizations should research CTI sources to find those that match their needs and budget.

Some CTI sources are specific to industrial control systems or the electric sector, while others are more general in nature. Some charge for the information they provide, and others are free of charge. Security consultants have assembled lists of CTI sources, along with guidance for evaluating them (Metivier 2016). The list below provides example CTI sources from governments, nonprofits, and commercial entities. Note: The list provides examples and is not meant to be an endorsement of any particular CTI source.

- **Spamhaus Project** (www.spamhaus.org)
    - International nonprofit, Switzerland-based
    - General CTI
    - Free public service (with some restrictions).
- **SANS Internet Storm Center** (isc.sans.edu)
    - Private company (SANS Institute)
    - General CTI
    - Free public service.
- **ICS-CERT** (www.us-cert.gov/ics)
    - U.S. government program
    - CTI specific to ICS
    - Free public service.
- **RSA** (www.rsa.com)
    - Private company
    - Sector-specific with automated segmentation
    - Paid subscription.
- **National Council of ISACS** (www.nationalisacs.org)
    - Coordinator for 20 individual ISACS
    - Each ISAC is sector-specific (e.g., Electricity ISAC)
    - Some ISACS are free, others membership-based.

Threats to the most critical systems and data should get the most attention; therefore, a prioritization of these critical assets will help inform the selection of CTI sources.

Organizations then need to decide who will monitor the CTI sources and what actions will be taken in response. There is no point in gathering CTI if no one has been assigned responsibility for following up on alerts or notifications. Budget must be set aside for both the time required to monitor and respond to CTI alerts and notifications. Upper management must instruct staff in all departments to be ready to cooperate with efforts to respond to alerts and notifications (e.g., mitigate a newly discovered vulnerability).

At that point, the organization can begin monitoring CTI sources. Individual alerts and notifications may need to be acted on (e.g., mitigation of a newly discovered vulnerability), while longer-term trends in CTI become input for the **risk management** building block.

## 5.4 Essential Data

Organizations that plan to monitor CTI should research the sources that best fit their needs. Gathering the following information will help them select from the many sources available:

- An inventory of the organization's assets, prioritized by criticality
- A list of CTI sources, prioritized by applicability to the organization's critical assets
- Processes and plans for responding to CTI.

***References and more resources for this building block appear in the appendix under "Cyber Threat Intelligence."***

# 6 Laws, Regulations, and Standards

Laws and regulations are enacted by governments to specify certain standards of behavior for individuals, corporations, or other entities. Laws are enacted by a legislative body (or other authorized bodies). Regulations are enacted by government agencies to specify the implementation of a law. Laws and regulations that apply to electric utilities are meant to advance grid reliability, safety, affordability, and security ("Cyber Evaluative Framework for Black Sea Regulators" 2017, 5).

Regulations sometimes incorporate standards—best practices that have been assembled and vetted by a trusted organization. For instance, the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) have jointly published the ISO/IEC 27000 series of standards, which address information security. When standards are incorporated into regulations, regulatory compliance naturally includes compliance with the standards. Organizations (including utilities) may choose to comply with certain standards, even if they are not compelled to do so by regulations. This can provide assurance to internal stakeholders (e.g., executive management) that the organization is implementing prudent security measures.

**Box 4: Three Types of Standards**

The word "standards" actually has multiple meanings in the cybersecurity domain.

- *Best practice standards* such as ISO/IEC 27000 (described at left).
- *Technical standards* that define how technologies work and interact such as the Institute of Electrical and Electronics Engineers standard 802.11, which defines wireless protocols used on Wi-Fi networks ("IEEE 802.11" 2020).
- *Standards* that are rules an organization develops and enforces internally such as how often employees need to change their passwords.

All meanings are correct, and the intended meaning is usually apparent from the context (Harris and Maymi 2016).

Government agencies in different nations take different approaches to cybersecurity laws and regulations. The laws of different nations may be structured to result in very dissimilar styles of regulation. In addition, the agency tasked with developing and enforcing regulations for the energy sector also varies, and this can have an impact on how regulations are enforced. In the United States, the North American Energy Reliability Corporation establishes reliability standards that include cybersecurity. In Great Britain, the Office of Gas and Electricity Markets establishes regulations that include cybersecurity. In India, the Central Electricity Regulatory Commission performs this function. How best to regulate cybersecurity is a challenge, and varying priorities lead to country-specific implementations.

## 6.1 Importance

Laws and regulations provide incentives for utilities to adopt effective cybersecurity measures (Ragazzi et al. 2020). This motivation may include incentives for strengthening cybersecurity or repercussions for failing to do so. A well-structured regulation will balance the cybersecurity benefit of compliance against the cost to the utility. However, creating a "well-structured" regulation can be tricky, and the consequence of getting it wrong can be dire. A poorly structured regulation could force utilities to expend their resources on compliance with little actual cybersecurity benefit. This could result in an electric grid that is even less secure than if no regulation had been implemented. In other words, the organization might have achieved more effective cybersecurity if it had invested its resources as it saw fit, rather than spending to comply with poorly structured regulations.

Internationally recognized standards are valuable because the best practices they embody go through an extensive vetting process. They also provide a “common language” for security professionals.

## 6.2 Intersections with Other Building Blocks

Laws and regulations are implemented by governments to define required behaviors. Standards may be implemented by many types of organizations (including international standards bodies) and define recommended behaviors. The compliance effort within the utility strives to interpret and enact those behaviors, as well as document the utility’s adherence to the regulations and standards.

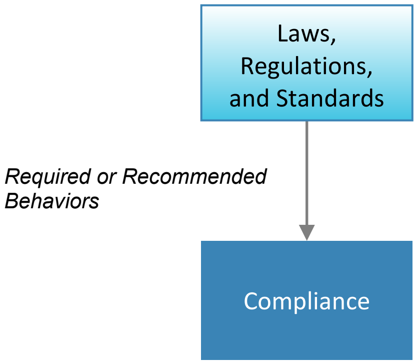

Laws, Regulations, and Standards
Required or Recommended Behaviors
Compliance

**Figure 6. Information passed from the laws, regulations, and standards building block**

## 6.3 Processes and Actions

The items below are adapted and abridged from *Evaluating the Prudency of Cybersecurity Investments: Guidelines for Energy Regulators* (Ragazzi et al. 2020), which expands on each of the items presented.

Government agencies seeking to implement or revise a cybersecurity regulation framework should first consider which type of regulatory framework will be most effective for their purposes.

### *Performance-Based Regulation Framework*

In performance-based regulation, regulators define security objectives and the indicators (metrics) to be used for validating compliance (through audits or inspections). The utility determines how to meet these objectives.

The process for establishing a performance-based regulation framework begins with defining a cybersecurity strategy. This is followed by defining objectives that fit within the strategy. Then, indicators of the objectives are defined along with economic incentives for achieving the objectives. The regulator conducts audits or inspections to determine compliance. Over time, the regulator should update the framework based on feedback from the utilities or their own observations about the effectiveness of the framework.

### *Cost-of-Service Framework*

In cost-of-service regulation, regulators define the objectives and how to meet those objectives. The regulator also identifies and benchmarks the costs of the security efforts. This regulatory framework is also called "cost plus."

The process for establishing a cost-of-service framework begins with defining a cybersecurity strategy—similar to the performance-based regulation framework. However, the second step jumps to defining the actual countermeasures to be used within the strategy. The regulator then determines the expenses associated with those countermeasures. Accountability procedures are developed by the regulator, who then verifies that the utility has complied with the prescribed countermeasures. Over time, the regulator should update the framework based on feedback from the utilities or their own observations about the effectiveness of the framework.

### *Cost-Effectiveness*

Key to any framework is the ability to compare the cost of a particular security control (also called a countermeasure) with the benefit provided by that countermeasure. In this regard, it is helpful to consider alternate scenarios where a utility is regulated versus not regulated, and then calculate a variety of costs under both normal operating conditions and cyberattack. The costs of implementing the regulation requirements and the avoided costs of a cyberattack are then weighed for each of these conditions. This exercise is discussed in detail in *Evaluating the Prudency of Cybersecurity Investments: Guidelines for Energy Regulators* (Ragazzi et al. 2020).

To be truly cost-effective, the regulation should be developed jointly by the regulatory agency and those being regulated—the utilities. Regulation should not be unilateral or adversarial. Rather, it should proceed from the assumption that all parties have the same objective—improved security—and unique, valuable insights into how best to achieve that objective.

Regardless of the type of framework used, government agencies may choose to incorporate one or more international standards for best practices into their regulations. This provides a starting point for both regulators and utilities, because for any widely recognized standard there will be guidance for effective implementation.

## 6.4 Essential Data

Agencies that wish to create or amend a regulatory framework should collect the following:

- A list of the current applicable regulatory frameworks (cyber and otherwise)
- Information about the utilities that will be subject to the new or revised regulations. This information should include details about the system itself (generation size and type, loads, and so on), economic information about the utility's current cost recovery framework, and the cyber preparedness of the utility's equipment and personnel.
- Points of contact within the utility or utilities that will be subject to regulation
- Threats likely to affect utility operations (both cyber and otherwise) and the likely economic impact of such threats.

***References and more resources for this building block appear in the appendix under "Laws, Regulations, and Standards."***

# 7 Compliance

*Compliance* refers to the responsibility and effort within a utility to adhere to laws, regulations, and standards that may be imposed on a national or regional level. Compliance may require deploying technical controls (such as firewalls), administrative controls (such as staff training), or physical controls (such as locks and fencing).

## 7.1 Importance

Directives from government and regulatory authorities define certain cybersecurity behaviors. Often, these behaviors are enforced through audits or inspections by the regulatory agency or through self-documentation on the part of the utility. While audits may seem burdensome, they are also an opportunity to get feedback from an outside party—the auditor—regarding security controls and accountability mechanisms. This feedback can serve as a fresh perspective that helps the utility achieve a stronger security posture.

Lack of compliance may be penalized. The regulatory agency may impose a fine, and depending on how these fines are determined and the severity of the violation, the financial impact may be severe (Workentin 2019). But the impact may be more than financial—lack of compliance can also impact reputation and customer trust (West 2019).

Regulations can motivate utility decision makers to make resources available for cybersecurity that might not otherwise be forthcoming. Some information technology managers have observed that without regulations, they might not get any funding from their bosses for cybersecurity. If laws and regulations are well structured, they can kick-start a utility's cybersecurity program, which can then mature over time. (See the **laws, regulations, and standards** building block for a discussion of "well structured" versus "poorly structured" regulations.)

## 7.2 Intersections with Other Building Blocks

The **compliance** building block within the utility must identify all applicable laws, regulations, and standards and interpret how the recommended or required behaviors apply to the utility. The **compliance** building block then supplies high-level information regarding regulatory requirements to the **governance** building block. This enables utility leaders to make informed decisions regarding allocation of security resources. More detailed regulatory requirements are provided to the **organizational security policy** building block, so that the (externally driven) compliance efforts and the utility's (internally driven) risk management efforts can be harmonized across the organization.

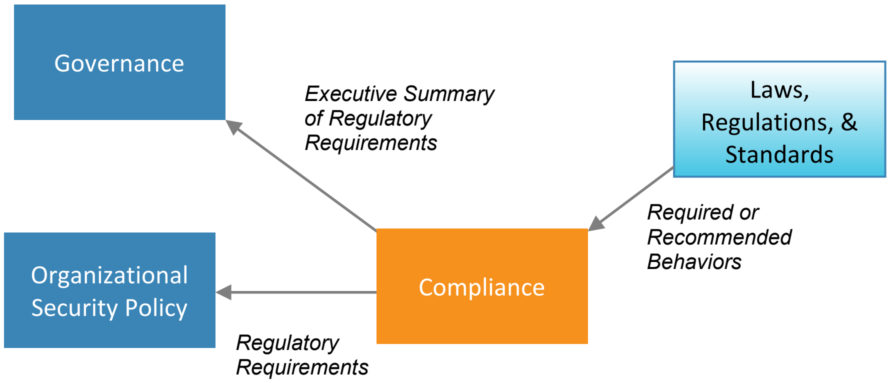

Governance
Executive Summary of Regulatory Requirements
Laws, Regulations, & Standards
Required or Recommended Behaviors
Organizational Security Policy
Compliance
Regulatory Requirements

**Figure 7. Information passed to and from the compliance building block**

## 7.3 Process and Actions

Forming organizational policies that adhere to the cybersecurity behaviors and standards defined in regulations requires careful consideration. A solid first step is to identify someone who has experience with (or at least interest in) regulations and compliance, and who can take on the responsibility of leading the utility's compliance effort. This person becomes the *compliance officer* for the utility.

The compliance officer leads groups of other employees (and possibly outside consultants) through the following processes:

- Research laws, regulations, and standards that apply to the utility and relate to cybersecurity, privacy, disclosure of cyber incidents, and related topics
- If regulations are structured with different levels of compliance—for instance, if larger generation facilities have a heavier regulator burden—determine which level of compliance applies to the utility and what compliance tasks need to be performed.
- Research any resources that assist in developing policies and procedures to help with compliance
- Interface with authorities and translate requirements within the organization
- Develop a process of gathering information about the compliance procedures and document incidents that are and are not in accordance with the enforced rules
- Develop compliance audit and review mechanisms internal to the organization
- Develop a reporting mechanism to submit periodic summaries of the compliance status.

## 7.4 Essential Data

When undertaking compliance, a utility should collect the following information:

- Government executive orders
- Standards and directives mandated by regulatory authorities
- Standards that the utility has elected to apply
- Regional/national/local laws and requirements

- A list of critical systems within the utility and the devices and applications running within those systems. The compliance officer will need this list if regulations specify specific controls for specific types of systems.

***References and more resources for this building block appear in the appendix under "Compliance."***

# 8 Procurement

*Procurement* is the process by which a utility acquires devices, applications, or services that will be incorporated into its systems. Although sometimes thought of as simply purchasing, procurement is actually a multistage process that includes defining requirements, evaluating options for purchase, negotiating contracts, purchasing, and receiving the devices or applications (Harris and Maymi 2016) or activating the service.

## 8.1 Importance

The overall security of a utility depends to a large extent on the security of the individual devices, applications, or services within that utility. Technical controls can somewhat compensate for security gaps in these products, but the resulting system will never be as secure as one built from the ground up with secure components. Devices, applications, or services may be insecure due to mistakes made in designing or implementing security features, or they may have been made insecure deliberately to allow attackers access to systems after they are installed.

Therefore, procurement has a critical role to play in cybersecurity. At the very least, a thorough procurement process offers an opportunity for utilities to learn about the state of security of various products. In the best-case scenario, the utility can use procurement to select secure products while simultaneously communicating to vendors that cybersecurity is a product differentiator. If vendors hear that cybersecurity is a consideration in utility purchasing decisions, they are likely to invest more resources to make future products more secure.

Utilities should make cybersecurity a key consideration in every phase of procurement.

## 8.2 Intersections with Other Building Blocks

*Organizational security policy* should include directives to incorporate cybersecurity into the procurement process. These may include regulatory requirements for procurement that originate with the **compliance** building block. These directives should be followed by those utility workers doing requirements analysis for new device and application purchases, those issuing requests for proposals, those reviewing vendor proposals, those issuing purchase orders, and those in charge of receiving.

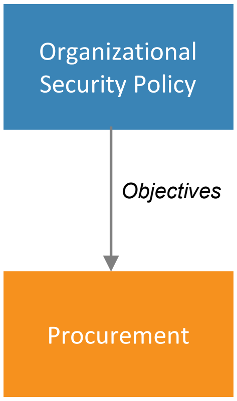


**Figure 8. Information passed to the procurement building block**

## 8.3 Processes and Actions

Security issues around procurement and supply chains have received a great deal of attention in recent years. A number of countries—including Russia, India, China, and the United States—have efforts underway to better address supply chain cybersecurity. Approaches vary widely, with some countries even restricting the use of foreign-made components or systems. However, electrical utilities in many countries may not have the option to buy locally if the devices and applications they need are only made overseas. In those cases, the utility must find a pragmatic approach to procurement and supply chain risk.

One source of actionable guidance on supply chain risk comes from the United Telecom Council's *Cyber Supply Chain Risk Management for Utilities—Roadmap for Implementation* (Bartol 2015). The following are highlights from that document (more details and in-depth explanations can be found there):

- **Identify suppliers, assess their risk, and prioritize them.** This will require some effort, as a single utility may depend on hundreds of different suppliers. Also, each supplier may incorporate parts and equipment from many sub-suppliers. But once the utility has identified its major suppliers and sub-suppliers, it can identify those that are the most critical for cybersecurity, either because of the nature of their products or the amount of access they will have to the utility's system during the business relationship. The most critical suppliers and sub-suppliers have the greatest potential for impact and must receive more attention during procurement.
- **Determine security requirements and how to monitor compliance with those requirements.** There are numerous policies and standards that can be used as the basis of security requirements (for instance, those from North American Electric Reliability Corporation Critical Infrastructure Protection or NIST). Utilities can ask suppliers to self-attest to adhere to these policies and standards, or they can take a more rigorous approach and conduct site visits or tests of the suppliers' products. The most rigorous approach involves third-party testing or certification.
- **Prepare for the end-of-the-supplier relationship.** At some point, the utility may decide to switch suppliers for any number of reasons. The utility should have a plan in place to terminate the supplier's access to utility systems when that access is no longer needed. The longer the supplier relationship lasts, the more careful and thorough the utility must be when disengaging.

Another valuable resource from the Energy Sector Control Systems Working Group, *Cybersecurity Procurement Language for Energy Delivery Systems* (Goff, Glantz, and Massello 2014), provides procurement language that addresses cybersecurity. The procurement language covers topics such as access control, logging and auditing, malware detection, and the supplier's secure development practices. Utilities can take this language and customize it for contracts issued to suppliers, ensuring that they have covered all aspects of security relevant to the product being procured.

The American Public Power Association and the National Rural Electric Cooperative Association recommend sending standard cybersecurity questionnaires to vendors as a way of vetting them—possibly during the request for proposals stage ("Managing Cyber Supply Chain Risk-Best Practices for Small Entities" 2018). They provide topics for these questions (e.g., nature of access controls and information management security) but do not provide sample questions. However, such sample questions can be obtained from consultant websites (Keller 2020) or adopted from other industries (Ehrlund n.d.).

## 8.4 Essential Data

Utilities seeking to improve their procurement processes should collect the following information:

- A list of critical systems within the utility, and the devices, applications, and services operating within
- A list of vendors associated with those products and the period of time that vendor relationship is expected to continue
- Alternates for critical products in case the supplier goes out of business or no longer makes or supports a critical product
- An inventory of all suppliers or vendors that have access to the utility's systems, the reason for that access, and how that access could be suspended if need be
- A list of sources for information on new or existing product vulnerabilities and recommended remediation actions.

***References and more resources for this building block appear in the appendix under "Procurement."***

# 9 Technical Controls

*Technical controls* are the hardware and software components that protect a system against cyberattacks. Firewalls, intrusion detection systems (IDS), encryption, and identification and authentication mechanisms are examples of technical controls (Harris and Maymi 2016).

## 9.1 Importance

Technical controls perform many critical functions, such as keeping unauthorized individuals from gaining access to a system and detecting when a security violation has occurred. Because they are so critical, some people think of technical controls as being the entirety of cybersecurity, ignoring other essential elements (those captured in the other building blocks).

Technical controls must be organized in such a way that they provide protection for both data at rest (e.g., data stored on a hard drive) and data in motion (e.g., data moving across a network). A common approach for deploying controls is *defense-in-depth*, where controls are layered. In such an arrangement, if an attacker breaches one control, controls at the next layer continue to provide protection.

## 9.2 Intersections with Other Building Blocks

The **organizational security policy** building block defines objectives for the **technical controls** building block. Decisions regarding which controls to deploy and how the system of controls will work together (the security architecture) are made by the staff in charge of technical controls. Because of the complexity involved in deploying technical controls, it is not uncommon in small and under-resourced utilities to see security controls overbuilt in some areas and underbuilt in others (Ingram and Martin 2017). This problem is avoided by having the organizational security policy set technical control objectives based on risk management needs, compliance needs, and governance strategy (see the building blocks for **risk management**, **compliance**, and **governance**). This provides a more balanced, organization-wide perspective on security, which can then be addressed by selectively deploying security technical controls.

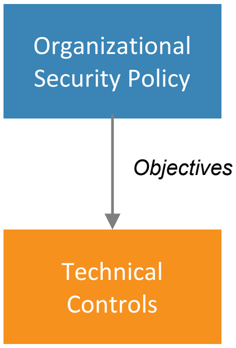


**Figure 9. Information passed to the technical controls building block**

## 9.3 Process and Actions

Deploying technical controls involves many types of technology and skills, making it difficult to point to any one action as the definitive "first step." Nonetheless, network security is often at the forefront of many efforts to improve security. In 2020, when India issued new security mandates for the power sector, it called out firewalls as an example of the type of protective devices that would be required (T&D World 2020). This was in part a response to a malware infection at India’s atomic power producer (Singh 2019).

A modern utility is likely operating multiple networks simultaneously, including an enterprise network—supporting business and office functions (e.g., accounting and email)—and a supervisory control and data acquisition (SCADA) network—which controls and monitors grid equipment (e.g., remote terminal units). As advanced metering infrastructure, smart meters, and distributed energy resources (such as customer-owned solar) are deployed in greater numbers, utilities will need to extend wide area networks further into the field to gather data and monitor the state of the grid.

Network security involves many different functions (more than can be covered in these building blocks). However, two are particularly worth mentioning: access control and network monitoring. *Access controls* are those technologies that determine who can connect to a network or system and what they can do once they are connected. A password is an example of access control; specifically, passwords address *authentication*, which verify that person, device, or application that wishes to connect to the network is indeed who they claim to be. Only you are supposed to know your password, so anyone who knows your password is assumed to be you. Access control is taken for granted on enterprise networks (you log in with your password every day for work). But as SCADA and wide area networks push outward and closer to the grid edge, access control becomes an issue there as well.

*Network monitoring* tools detect suspicious activity or traffic on a network. These tools generally operate through either signature detection or anomaly detection. *Signature detection* looks for data that is known to be associated with a particular piece of malware, while anomaly detection looks for anything out of the ordinary that “looks suspicious.” While there are many commercial network monitoring tools on the market, there are also high-quality open source alternatives (Drolet 2018). Below are three examples:

- **Snort** is highly configurable. Users can tell it what to look for on the network and what actions to take when a threat is detected.
- **Zeke** analyzes network traffic. Its sophisticated scripting capabilities can automate the work of responding to threats, but it has a steep learning curve.
- **Kismet** detects intrusions on wireless networks, including Wi-Fi and Bluetooth. It can be used to track down unauthorized access points, which helps with access control.

SCADA networks have security needs that are somewhat different from enterprise networks. Because they control devices and processes in the physical world, special care must be taken when responding to suspected cyber intrusions so that the cyber response actions do not cause unintended consequences in the physical systems being controlled. (For instance, before disconnecting a generation station that might be affected by malware, consider whether doing so might cause a cascading outage.) Utilities should study the special requirements associated with SCADA security.

The items below are selected and adapted from *21 Steps to Improve Cybersecurity of SCADA Networks* (PCIP and DOE 2002). More details are provided in that document, and many of the

21 steps not included here are covered in other building blocks. Many items on the list also apply to enterprise networks.

- **Isolate the SCADA network as much as possible.** Find all touchpoints between the SCADA network and the utility's own local area networks, the internet, or networks operated by other entities. These might include wireless routers, satellite links, or dial-up modems. Shut down as many of these touchpoints as possible. For instance, if a touchpoint is used infrequently and exists only to make it convenient for certain employees to connect, consider eliminating it. The remaining touchpoints should be strengthened with firewalls, IDS, or other similar protections.
- **Remove unnecessary devices and services from the SCADA network.** More devices mean more points for a cyberattacker to target. Shutting down or removing unneeded services and devices is a low-cost way of protecting the network.
- **Use whatever security features exist on devices or systems.** Some devices and systems may have built-in security features (such as encryption or authentication), but these are not always used because doing so may require more staff effort. Reviewing technical documentation of these devices and—if feasible—activating them is another low-cost way to improve security.
- **Deploy IDS.** IDS scan for known malware or monitor network traffic for anomalies. Snort, Bro, and Kismet are all examples of open-source network IDS, while OSSEC is an example of an open-source "host-based" IDS (Drolet 2018).
- **Have "red teams" identify possible SCADA attack scenarios.** "Red team" refers to a group tasked with finding vulnerabilities in a system. Red teams may be contractors (such as those hired to do a penetration test) or employees from another department within the organization. Ideally, red teams should not include anyone responsible for the security of the system—the idea is to get a fresh perspective on the security posture of the system.
- **Review the physical security of remote sites connected to the SCADA network.** Physical access to a device or a site can provide opportunities for cyber compromise. If a would-be attacker has unsupervised physical access to a device, they have a good chance of eventually bypassing its cyber defenses.

## 9.4 Essential Data

Utilities seeking to improve the technical controls for their SCADA networks should collect the following information:

- Details of touchpoints between the SCADA network and other networks, including the utility enterprise network and the internet
- Physical security details of remote sites with SCADA access
- Asset management data regarding devices on the system and the services they run
- Information about the security features built into devices connected to the SCADA network
- Repositories of valuable data on both enterprise and SCADA networks and the technical controls used to protect them.

***References and more resources for this building block appear in the appendix under "Technical Controls."***

# 10 Incident Response

Even the most sophisticated defenses can be breached by attackers with sufficient skills and resources. When that happens, the incident will be much worse if the defenders have not planned and rehearsed a strategy for responding. The actions taken by an organization to prepare for and respond to a cyberattack constitute *incident response.*

## 10.1 Importance

Responding to a cyber incident is a complicated, sensitive process. Even in the best circumstances, the time following an attack will be chaotic as staff struggle to understand what has happened, why it happened, the impact on the business, and the best way to restore business functions. Utilities should prepare their responses in advance; otherwise, the cyberattack will likely last longer and do more damage as utility staff scramble to formulate an *ad hoc* response. Proactively preparing for an attack through planning, training, and rehearsal will reduce the chaos and the impact of the attack.

Although this **incident response** building block is written with a utility focus, it applies equally to government agencies, private businesses, nonprofits, and others. Every type of organization can benefit from incident response planning when the inevitable attack materializes.

## 10.2 Intersections with Other Building Blocks

The **organizational security policy** building block defines some key objectives for the incident response effort and answer some key questions. What are the roles and responsibilities associated with incident response? Which department is responsible for planning the organization's incident response? Who has the authority to initiate an incident response? What resources are available for incident response? With whom does the organization share data about the attack? The answers to these questions will inform the organization's incident response plan.

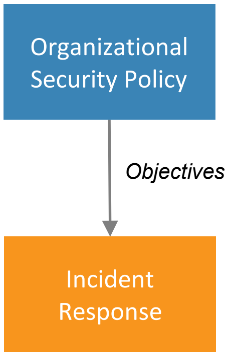


**Figure 10. Information passed to the incident response building block**

Depending on the organization, it may make sense to include only the highest-level details regarding incident response in the organizational security policy and capture lower-level details in a separate *incident response policy*, which can then be updated more frequently. At the very least, the organizational security policy should include a statement of commitment from management and a description of the organizational structure that will support incident response.

## 10.3 Processes and Actions

The items below are adapted and abridged from *The Computer Security Incident Handling Guide* (Cichonski et al. 2012), which expands on each of the elements presented. The Guide recommends creating incident response policy, plan, and procedures documents and lists the elements that should go into each. The policy is the most strategic of the three, while the procedures document is the most tactical. Small utilities or those just beginning to address incident response may combine these into a single document, with sections focusing on policy, planning, and procedures.

In preparation for creating these documents, the utility will need to gather or create the following information:

- A list of all applicable laws, regulations, and standards related to incident response and applicable to the utility. Whatever actions are indicated by these laws, regulations, and standards must be included in incident response documents. This will vary between countries. Utilities must include not only laws, regulations, and standards specific to the utility sector but also laws, regulations, and standards that address privacy, consumer protection, and related topics. The regulatory agencies themselves should provide useful information on these topics.
- Definition of terms related to incident response, as they will be used in the incident response documents. For instance, a utility may choose to define a cybersecurity "incident" according to its own particular criteria.
- A mapping of the utility's departments and offices to the roles, responsibilities, and levels of authority they will have in incident response. For instance, who within the utility has the authority to disconnect equipment if it is suspected of being compromised?
- Prioritization of incidents by potential impact on the utility
- A communication plan for incident response that covers communication both internal to the utility and to other organizations (e.g., the media, customers, software vendors, law enforcement, and organizations that track CTI).
- Specific checklists, forms, and processes that will be used during incident response (for instance, the procedure for preserving infected hard drives for later forensic analysis).

The utility must identify the tools that it will use to identify cyber incidents, such as IDS, antivirus software, and log analyzers. These will be covered in the **technical controls** building block.

The incident response documents should cover four phases:

- **Preparation.** Creating the incident response policy, plan, and procedures document(s); rehearsing the plan and improving it based on lessons learned; collecting all hardware and software (backup drives, forensic tools, printers, etc.) needed to execute the incident response; and determining the best location where incident responders can work.
- **Detection and Analysis.** Monitoring IDS, system logs, and/or antivirus software for indicators of compromise; once a suspected incident is detected, verifying the incident and triggering the response process; correlating the indicators of compromise with other observations about the network, devices, and systems in operation; investigating the cause and potential impacts of the cyber incident to formulate the best response.

- **Containment, Eradication, and Recovery.** Selecting and executing strategies for containment (activities that stop the cyberattack from spreading to other devices or systems), eradication (the process of removing malware from the system), and recovery (the process of returning the system to normal functioning).
- **Post-Incident Activity.** Gathering lessons learned from the incident, improving the process of incident response, and reviewing data about incidents that help to identify weaknesses in security defenses that may need to be addressed.

Details can be found in *Computer Security Incident Handling Guide* (Cichonski et al. 2012).

## 10.4 Essential Data

Utilities seeking to create or amend an incident response plan should collect the following information:

- A list of all applicable laws, regulations, and standards related to incident response
- The phone tree/contract tree that utility employees will use to alert each other when an incident has been declared
- A list of outside parties with which the utility will want to communicate during an incident response. These may include media, customers, software vendors, law enforcement agencies, and internet service providers.
- Records of software licenses
- Locations of backup data and systems and procedures for restoring from backup
- Location of equipment and tools that will be used during incident response.

**Box 5:**
**Incident Response Terminology**

An *incident* or *computer security incident* is "a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices" (Cichonski et al. 2012).

The term *event* is sometimes used interchangeably with *incident*. However, *event* is a broader term that encompasses anything that can be observed on the system (e.g., a user sending an email). Events may or may not have a negative impact. Incidents have negative impact (Harris and Maymi 2016).

***References and more resources for this building block appear in the appendix under "Incident Response."***

# 11 Cybersecurity Awareness Training

To thwart cyberattacks, all utility employees must understand the basic good habits that support cybersecurity—what security professionals call *cyber hygiene*. For this reason, utilities need to educate their employees about potential threats and their roles in preventing them. This education is often called *cybersecurity awareness training*.

## 11.1 Importance

Cyberattacks often depend on human mistakes to be successful. Many companies and even governments have fallen victim to malware because an unaware employee clicked on an infected email attachment or inserted an infected USB drive into a computer, as was likely the case when Stuxnet entered Iran's nuclear enrichment facility (Zetter 2014). Cybersecurity awareness training teaches employees to avoid these mistakes. The development of good, safe computer habits (cyber hygiene) can often save an organization time, money, frustration, and reputational damage. Though simple, these habits are extremely effective in closing off vulnerabilities that can give attackers access to utility systems. Research has shown a significant number (19%–36%) of data breaches can be traced to human error ("2017 Cost of Data Breach Study" 2017).

## 11.2 Intersections with Other Building Blocks

The **organizational security policy** building block defines objectives for the **cybersecurity awareness training** building block. Cybersecurity awareness training, which focuses on teaching cyber hygiene to all employees, benefits from workforce development, which provides advanced skills development for technical staff. Those technical professionals can help monitor and coach nontechnical staff, making cybersecurity awareness training more effective.

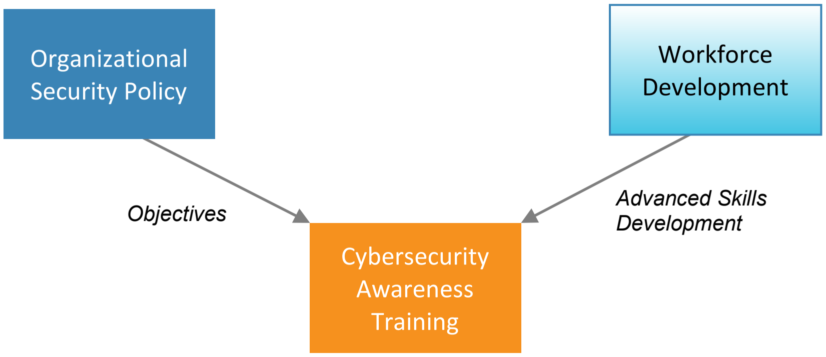

Organizational Security Policy
Workforce Development
Objectives
Advanced Skills Development
Cybersecurity Awareness Training

**Figure 11. Information passed to the cybersecurity awareness training building block**

## 11.3 Process and Actions

Utility staff may believe that responsibility for cybersecurity rests only with the IT department. Staff may not be aware that their actions can impact cybersecurity, or that they have a crucial role to play in keeping cyberattackers off utility computers and networks.

Management must impress on all employees that cybersecurity is an organizational priority and everyone's responsibility. They must create a corporate culture that emphasizes cybersecurity as a key element of the organization's success. The utility leadership must commit to building a culture of cybersecurity (Drolet 2019). Staff will be more open to change if they understand that the entire hierarchy values cybersecurity and is making the effort together ("The Truth About Cybersecurity Training" 2020).

Cybersecurity awareness training works best when some initial training (e.g., a day-long class on cyber hygiene) is reinforced regularly (Harris and Maymi 2016, 159). Reinforcement may be through follow-up classes or online webinars, quizzes, or social engineering exercises. *Social engineering* refers to attempts by a cyberattacker to trick employees into cyber-unsafe behavior. One example of this is *phishing*, in which people are tricked into clicking a malicious link in an email by making that link appear to be legitimate.

The same social engineering tricks used by attackers can also be used within a utility to train staff to resist these tricks (e.g., the utility security staff can phish their fellow employees). The aim of these exercises should be to provide a useful learning exercise for employees to increase their awareness of attempted attacks in the future. Punitive action should be reserved for situations where an employee willfully refuses to follow cyber hygiene guidance or continually proves to be a potential cyber risk ("The Truth About Cybersecurity Training" 2020, 20).

Management should incentivize good cybersecurity awareness. Employee cybersecurity errors can usually be addressed through additional education and training; sometimes, just the awareness of internal social engineering exercises is enough to motivate better behavior. Where possible, cybersecurity awareness training should be entertaining, humorous, and easy to understand (Harris and Maymi 2016, 157). The goal is to keep employees engaged long enough that the good cyber habits become a kind of muscle memory (Osterman Research 2020).

Finally, employees' cybersecurity awareness should be tracked to show awareness of and compliance with expected behaviors over time.

## 11.4 Essential Data

All employees need training at a basic level of cybersecurity awareness. This includes avoidance of phishing, responsible use of removable media (e.g., USB storage devices), and avoidance of unsecured Wi-Fi networks. In addition, some employees need additional training if they regularly handle sensitive information. Sensitive information includes:

- Data about operations and security of the utility
- Personally identifiable information about customers and staff
- Financial information
- Trade secrets
- Any information deemed sensitive by local laws or regulations
- Software licenses
- Details about computer network configurations and other data that would be useful to cyberattackers
- Information that is covered by a nondisclosure agreement signed by the utility.

It is therefore important to know who within the utility has access to sensitive databases and files to determine the type of security training needed. Useful questions to ask when gathering data include:

- For each category of sensitive information, who has access to it?
- How do we track who has access to sensitive information?
- Is there a process for revoking access to sensitive information when the employee no longer needs it or when the employee leaves the organization?
- How sensitive is this information? (What negative impact would arise if it were lost, stolen, or altered by an attacker?)
- What do staff need to know about security for each type of sensitive information and the system that stores it?

Assembling these data will enable utility management to identify the training needs of different members of the staff.

***References and more resources for this building block appear in the appendix under "Cybersecurity Awareness Training."***

# 12 Workforce Development

Utilities need their IT staff, security staff, and engineers to have specialized technical knowledge regarding cybersecurity. Government agencies can help meet this need through *workforce development* programs that provide cybersecurity training.

## 12.1 Importance

Securing the electrical grid against cyberattacks is necessary for the safe, reliable operation of this critical infrastructure. However, there is a gap between the number of qualified cybersecurity professionals in the workforce and the number needed. The International Information System Security Certification Consortium estimates the workforce shortfall of skilled cybersecurity professionals to be more than 4 million worldwide ("(ISC)$^2$ 2019). Furthermore, utilities everywhere must compete against other industries—finance, retail, manufacturing, etc.—when hiring for cybersecurity positions.

Workforce development efforts make cybersecurity educational resources available to all who wish to learn these skills. Workforce development programs may be implemented by national governments, not-for-profit organizations, utilities, or any entity with an interest in ensuring an adequate supply of cybersecurity professionals.

## 12.2 Intersections with Other Building Blocks

The **workforce development** building block augments utilities' efforts in the **cybersecurity awareness training** building block. Whereas cybersecurity awareness training addresses the basic, safe cybersecurity habits that all employees should have, workforce development cultivates those specialized, in-depth cybersecurity skills needed by IT professionals, security professionals, and engineers. Those technical professionals can help monitor and coach nontechnical staff, making cybersecurity awareness training more effective.

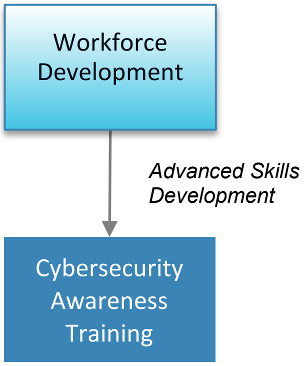


**Figure 12. Information passed from the workforce development training building block**

## 12.3 Processes and Actions

Government agencies may consider incentives to encourage organizations to create workforce development programs as a way of ensuring an adequate supply of cybersecurity professionals for all industries, including critical infrastructure. Governments may even consider organizing such programs themselves.

Whoever establishes a workforce development program should engage entities that operate critical infrastructure related to their cybersecurity needs and the gaps in skills they see among job candidates. Because grid security is an issue of national security, defense or military agencies might also contribute by identifying workforce training objectives. The responsible government agency can then review educational resources internal to the nation (universities, trade schools, etc.) that may be able to establish in-person or online learning opportunities. If defense or military agencies have sufficient resources, they may also provide cyber training to civilians (including utility staff).

Workforce development opportunities may also be available through for-profit institutions or even foreign government agencies. A plan for cybersecurity workforce development should be written and reviewed by all stakeholders (being sure to take into account skill gaps and budget). Government agencies might consider incentives that would encourage individuals already working in critical infrastructure to increase their skills in cybersecurity. These incentives could be provided directly to the individuals or their utility/critical infrastructure employers, or to the organizations that provide the training programs.

## 12.4 Essential Data

Whether it is a government agency, not-for-profit organization, university, or other institution, anyone setting up a workforce development program should find out if critical infrastructure entities (such as utilities) currently have access to the following skills (either through staff or contractors). Assembling this data will better focus the workforce development program on the needs of critical infrastructure.

- Access control and account management
- Network security and network segmentation
- Applicable laws, regulations, and standards
- Physical security
- Security needs specific to the systems and networks needed for delivery of services (for instance, in an electric utility, this might include security for SCADA systems).

***References for this building block appear in the appendix under "Workforce Development."***

# Appendix A. References and Resources

The references and resources below are arranged according to their relevant building blocks.

Some of the references and resources below were published or sponsored by commercial cybersecurity awareness training companies. Inclusion in this list does not imply endorsement of the publisher or sponsor.

## Governance

### *References*

Bew, Robyn. “Five Principles for Stronger Board Oversight of Cybersecurity.” BRINK – News and Insights on Global Risk. Accessed January 5, 2021. https://www.brinknews.com/five-principles-for-stronger-board-oversight-of-cybersecurity/.

National Association of Corporate Directors. 2020. *NACD Director’s Handbook on Cyber-Risk Oversight.* https://www.nacdonline.org/insights/publications.cfm?ItemNumber=67298.

NIST. 2018. *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1.* https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

NREL. “Distributed Energy Resource Cybersecurity Framework.” Accessed January 5, 2021. https://dercf.nrel.gov/.

Rothrock, Ray A., James Kaplan, and Friso Van der Oord. “The Board’s Role in Managing Cybersecurity Risks.” *MIT Sloan Management Review*. November 16, 2017. https://sloanreview.mit.edu/article/the-boards-role-in-managing-cybersecurity-risks/.

Tyler Cybersecurity. “Cybersecurity Training for Executives and Boards of Directors.” Accessed January 5, 2021. https://www.tylercybersecurity.com/services/executive-cybersecurity-readiness-program.

### *More Resources*

ANSI Webstore. “ISO/IEC 38500:2015 - Information Technology - Governance of IT for the Organization.” Accessed January 4, 2021. https://webstore.ansi.org/Standards/ISO/ISOIEC385002015?gclid=EAIaIQobChMImNnrn6SD7gIVBK-GCh38NQ8jEAAYASAAEgLCe_D_BwE.

Atkinson, Sean. “Breaking the Divide Between Governance and Operational Cybersecurity.” Center for Internet Security. April 10, 2018. https://www.cisecurity.org/blog/breaking-the-divide-between-governance-and-operational-cybersecurity/.

Bodeau, Deb, Steve Boyle, Jenn Fabius-Greene, and Rich Graubart. 2010. *Cyber Security Governance: A Component of MITRE’s Cyber Prep Methodology.* MITRE Corporation. https://www.mitre.org/sites/default/files/pdf/10_3710.pdf.

Box. “Simplify Your IT Governance Strategy.” Accessed January 4, 2021. https://www.box.com/resources/dm/5-steps-to-good-governance/it-governance.

Burke, Brandon. “Governance vs Compliance.” April 3, 2019. http://community.aiim.org/blogs/brandon-burke/2019/04/03/governance-vs-compliance.

Cybersecurity & Infrastructure Security Agency. “Cybersecurity Governance | CISA.” October 27, 2020. https://www.cisa.gov/cybersecurity-governance.

Educause. “Information Security Governance.” Accessed January 4, 2021. https://library.educause.edu/topics/cybersecurity/information-security-governance.

Fontaine, David, and John Stark. “Cybersecurity: The SEC’s Wake-up Call to Corporate Directors.” The Harvard Law School Forum on Corporate Governance (blog). March 31, 2018. https://corpgov.law.harvard.edu/2018/03/31/cybersecurity-the-secs-wake-up-call-to-corporate-directors/.

Swinton, Seth, and Stephanie Hedges. “Cybersecurity Governance, Part 1: 5 Fundamental Challenges.” Insider Threat Blog (blog). July 25, 2019. https://insights.sei.cmu.edu/insider-threat/2019/07/cybersecurity-governance-part-1-5-fundamental-challenges.html.

Veltsos, Christophe. “Board Directors Need to Get Involved With Cyber Risk Governance.” Security Intelligence. August 24, 2017. https://securityintelligence.com/board-directors-need-to-get-involved-with-cyber-risk-governance/.

## Organizational Security Policy

### *References*

Harris, Shon, and Fernando Maymi. 2016. *CISSP All-in-One Exam Guide 7th ed.* New York: McGraw Hill Education.

Kee, Chaiw. 2001. *Security Policy Roadmap - Process for Creating Security Policies.* SANS Institute. https://www.sans.org/reading-room/whitepapers/policyissues/security-policy-roadmap-process-creating-security-policies-494.

SANS. “Security Policy Templates.” Accessed December 30, 2020. https://www.sans.org/information-security-policy/.

### *More Resources*

Duigan, Adrian. “10 Steps to a Successful Security Policy.” *Computerworld*. October 8, 2003. https://www.computerworld.com/article/2572970/10-steps-to-a-successful-security-policy.html.

IBM Knowledge Center. “Developing a Security Policy.” October 24, 2014. www.ibm.com/support/knowledgecenter/ssw_ibm_i_74/rzamv/rzamvdevelopsecpol.htm.

National Center for Education Statistics. 2020. “Chapter 3 - Security Policy: Development and Implementation.” In *Safeguarding Your Technology: Practical Guidelines for Electronic Education Information Security*. https://nces.ed.gov/pubs98/safetech/chapter3.asp.

Irwin, Luke. "How to Write an Information Security Policy – with Template Example." IT Governance Blog En. June 4, 2020. https://www.itgovernance.eu/blog/en/how-to-write-an-information-security-policy-with-template-example.

Ng, Cindy. "How to Create a Good Security Policy." Inside Out Security (blog). March 29, 2020. https://www.varonis.com/blog/how-to-create-a-good-security-policy/.

Wood, Charles Cresson. 2002. *Information Security Policies Made Easy 9th ed.* PentaSafe Security Technologies.

## Risk Management

### *Reference*

U.S. Department of Energy. 2012. *Electricity Subsector Cybersecurity Risk Management Process*. DOE/OE-0003. https://www.energy.gov/ceser/downloads/cybersecurity-risk-management-process-rmp-guideline-final-may-2012.

### *More Resources*

Paté-Cornell, M.-Elisabeth, Marshall Kuypers, Matthew Smith, and Philip Keller. "Cyber Risk Management for Critical Infrastructure: A Risk Analysis Model and Three Case Studies." *Risk Analysis* 38, no. 2 (2018): 226–41. https://doi.org/10.1111/risa.12844.

Resilient Energy Platform. "Calculate Risks." Accessed January 5, 2021. https://resilient-energy.org/guidebook/calculate-risks.

Westby, Jody, and Leslie Lamb. "Rethinking Risk in a Post-Pandemic World – Risk Management." *Risk Management.* December 1, 2020. http://www.rmmagazine.com/2020/12/01/rethinking-risk-in-a-post-pandemic-world/.

## Cyber Threat Intelligence

### *References*

ENISA. 2013. *Smart Grid Threat Landscape and Good Practice Guide*. https://www.enisa.europa.eu/publications/smart-grid-threat-landscape-and-good-practice-guide.

Metivier, Becky. 2016. "A Guide to Cyber Threat Intelligence Sources." Tyler Cybersecurity. July 12, 2016. https://www.tylercybersecurity.com/blog/guide-to-cyber-threat-intelligence-sources.

Threat Analysis Group. "Threat, Vulnerability, Risk - Commonly Mixed up Terms." Threat Analysis Group (blog). May 3, 2010. https://www.threatanalysis.com/2010/05/03/threat-vulnerability-risk-commonly-mixed-up-terms/.

### More Resources

Anderson, Chad. 2020. “5 Simple Steps to Bring Cyber Threat Intelligence Sharing to Your Organization.” Help Net Security (blog). September 21, 2020. https://www.helpnetsecurity.com/2020/09/21/5-simple-steps-to-bring-cyber-threat-intelligence-sharing-to-your-organization/.

Crowdstrike. 2020. *Threat Intelligence, Cybersecurity’s Best Kept Secret.* https://go.crowdstrike.com/rs/281-OBQ-266/images/WhitepaperThreatIntelligence.pdf.

ENISA. “ENISA Threat Landscape - 2020.” Topic. Accessed December 15, 2020. https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends.

Guercio, Kyle. “Top Threat Intelligence Platforms for 2021 | ESecurity Planet.” Accessed December 18, 2020. https://www.esecurityplanet.com/products/threat-intelligence-platforms/.

Harris, Kevin. “The Changing Threat Landscape in Today’s Cybersecurity.” *Security*. September 16, 2020. https://www.securitymagazine.com/articles/93367-the-changing-threat-landscape-in-todays-cybersecurity?v=preview.

Jones, Sherry. “Threat, Vulnerability, and Risk: What’s the Difference?” Reciprocity. March 31, 2020. https://reciprocitylabs.com/threat-vulnerability-and-risk-whats-the-difference/.

U.S. Department of Homeland Security. “Understanding the Threat Landscape.” Accessed December 15, 2020. https://us-cert.cisa.gov/sites/default/files/c3vp/smb/Understanding_the_Threat_Landscape.pdf.

## Laws, Regulations, and Standards

### References

“IEEE 802.11.” 2020. Standard. Institute of Electrical and Electronics Engineers. https://standards.ieee.org/standard/802_11-2020.html.

Keogh, Miles, and Paul Stack. 2017. *Cyber Evaluative Framework for Black Sea Regulators*. National Association of Regulatory Utility Commissioners. https://pubs.naruc.org/pub.cfm?id=E3CE75B5-155D-0A36-31FD-1B268F7BD125.

Ragazzi, Elena, Alberto Stefanini, Daniele Benintendi, Ugo Finardi, and Dennis K. Holstein. 2020. *Evaluating the Prudency of Cybersecurity Investments: Guidelines for Energy Regulators*. National Association of Regulatory Utility Commissioners. https://pubs.naruc.org/pub.cfm?id=9865ECB8-155D-0A36-311A-9FEFE6DBD077.

### More Resources

Findlaw. “What’s the Difference Between Laws and Regulations?” Accessed December 18, 2020. https://blogs.findlaw.com/law_and_life/2015/10/whats-the-difference-between-laws-and-regulations.html.

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

Massachusetts Mental Health Counselors Association Inc. "Laws vs. Regulations: What's the Difference?" Accessed December 18, 2020. http://www.mamhca.org/assets/1/7/Laws_vs_regulations.pdf.

NARUC. "The Regulatory Cybersecurity Strategy: A Key Building Block for an Energy Sector's Cybersecurity Policy Framework." Accessed May 13, 2020. https://www.naruc.org/international/news/the-regulatory-cybersecurity-strategy-a-key-building-block-for-an-energy-sector-s-cybersecurity-policy-framework/.

Singh, Rajesh Kumar. "India Plans to Mandate Cyber Security Measures for Power Grids." *The Economic Times*. January 21, 2020. https://economictimes.indiatimes.com/industry/energy/power/india-plans-to-mandate-cyber-security-measures-for-power-grids/articleshow/73479609.cms?from=mdr.

Walstrom, Michael. "India's Electrical Smart Grid: Institutional and Regulatory Cybersecurity Challenges." The Henry M. Jackson School of International Studies (blog). November 16, 2016. https://jsis.washington.edu/news/indias-electrical-smart-grid-institutional-regulatory-cybersecurity-challenges/.

## Compliance

### References

West, Kurt. "5 Best Practices for Utility Compliance: How to Avoid Regulatory Violations." Utility Cloud. October 20, 2019. https://www.utilitycloud.us/blog/best-practices-utility-compliance-avoid-regulatory-violations.

Workentin, Brandon. "Largest NERC CIP Fine to Date: What You Need to Know." Forescout (blog). February 2, 2019. https://www.forescout.com/company/blog/largest-nerc-cip-fine-to-date/.

### More Resources

Burke, Brandon. "Governance vs Compliance." April 3, 2019. http://community.aiim.org/blogs/brandon-burke/2019/04/03/governance-vs-compliance.

## Procurement

### References

American Public Power Association & National Rural Electric Cooperative Association. 2018. *Managing Cyber Supply Chain Risk-Best Practices for Small Entities*. https://www.cooperative.com/programs-services/government-relations/regulatory-issues/Documents/Supply%20Chain%20White%20Paper%204-25%20Final.pdf.

Bartol, Nadya. 2015. *Cyber Supply Chain Risk Management for Utilities--Roadmap for Implementation.* Utilities Telecom Council. https://utc.org/wp-content/uploads/2018/02/SupplyChain2015-2.pdf.

Ehrlund, Andreas. "Cybersecurity Starts with the RFP: 7 Tips to Keep Data Safe." Radiology Business. Accessed July 16, 2020. https://www.radiologybusiness.com/sponsored/1068/topics/privacy-security/cybersecurity-starts-rfp-7-tips-keep-data-safe.

Goff, Ed, Cliff Glantz, and Rebecca Massello. 2014. "Cybersecurity Procurement Language for Energy Delivery Systems." In *Proceedings of the 9th Annual Cyber and Information Security Research Conference on - CISR* 14, 77–79. Oak Ridge, Tennessee: ACM Press. https://doi.org/10.1145/2602087.2602097.

Harris, Shon, and Fernando Maymi. 2016. *CISSP All-in-One Exam Guide 7th ed*. New York: McGraw Hill Education.

Keller, Joel. "Top 10 Questions in Vendor Cybersecurity Questionnaires." Venminder. January 22, 2020. https://www.venminder.com/blog/top-10-questions-vendor-cybersecurity-questionnaires.

### *More Resources*

Bartol, Nadya. "Cyber Supply Chain Security Practices DNA – Filling in the Puzzle Using a Diverse Set of Disciplines." *Technovation* 34, no. 7 (2014): 354–61. https://doi.org/10.1016/j.technovation.2014.01.005.

Boyens, Jon M., Celia Paulsen, Rama Moorthy, and Nadya Bartol. 2015. *Supply Chain Risk Management Practices for Federal Information Systems and Organizations.* NIST SP 800-161. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-161.

Haas, Jeremy, and Ryan Bergquist. "Five Questions to Ask About Third-Party Vendors and Cybersecurity." SupplyChainBrain. November 19, 2019. https://www.supplychainbrain.com/blogs/1-think-tank/post/30489-the-company-you-keep-five-questions-to-ask-about-third-party-vendors-and-cybersecurity.

Whistic. "RFPs: Introducing Information Security & Cybersecurity Standards in RFPs." *Medium*. January 16, 2019. https://blog.whistic.com/rfps-introducing-information-security-cybersecurity-standards-in-rfps-abeddb80ced9.

## Technical Controls

### *References*

Drolet, Michelle. "5 Open Source Intrusion Detection Tools That Are Too Good to Ignore." Towerwall (blog). October 19, 2018. https://towerwall.com/5-open-source-intrusion-detection-tools-that-are-too-good-to-ignore/.

Harris, Shon, and Fernando Maymi. 2016. *CISSP All-in-One Exam Guide 7th ed*. New York: McGraw Hill Education.

Ingram, Michael, and Maurice Martin. 2017. *Guide to Cybersecurity, Resilience, and Reliability for Small and Under-Resourced Utilities.* NREL/TP-5D00-67669. National Renewable Energy Laboratory. https://energy.gov/sites/prod/files/2017/01/f34/Guide%20to%20Cybersecurity%2C%20Resilience%2C%20and%20Reliability%20for%20Small%20and%20Under-Resourced%20Utilities.pdf.

PCIPB, DOE. 2002. "21 Steps to Improve Cyber Security of SCADA Networks." President's Critical Infrastructure Protection Board and U.S. Department of Energy, Office of Energy Assurance. https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/21_Steps_-_SCADA.pdf.

Singh, Rajesh Kumar. "India Says Nuclear Plant Was Affected by Computer Malware." Bloomberg. October 31, 2019. https://www.bloomberg.com/news/articles/2019-10-31/india-says-nuclear-power-plant-was-affected-by-computer-malware.

T&D World. "India Plans to Mandate Cybersecurity Measures for Power Grids." January 22, 2020. https://www.tdworld.com/smart-utility/grid-security/article/21121025/india-plans-to-mandate-cybersecurity-measures-for-power-grids.

### More Resources

Gaither, Andy, Scott King, Darren Bennet, Joshua Carlson, Shane Markley, Patrick Norton, SANS Institute ICS Curriculum Team, Ted Gary, and Cody Dumont. n.d. *Implementation Guide for Industrial Control Systems Version 7.* Center for Internet Security. https://www.cisecurity.org/white-papers/cis-controls-implementation-guide-for-industrial-control-systems/.

Obregon, Luciana. 2015. *Secure Architecture for Industrial Control Systems.* SANS Institute. https://www.sans.org/reading-room/whitepapers/ICS/secure-architecture-industrial-control-systems-36327.

Stouffer, Keith, Victoria Pillitteri, Suzanne Lightman, Marshall Abrams, and Adam Hahn. 2015. *Guide to Industrial Control Systems (ICS) Security*. NIST Special Publication 800-82. National Institute of Standards and Technology. http://dx.doi.org/10.6028/NIST.SP.800-82r2.

## Incident Response

### References

Cichonski, Paul, Thomas Millar, Tim Grance, and Karen Scarfone. 2012. *Computer Security Incident Handling Guide*. NIST Special Publication (SP) 800-61 Rev. 2. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r2.

Harris, Shon, and Fernando Maymi. 2016. *CISSP All-in-One Exam Guide 7th ed.* New York: McGraw Hill Education.

### *More Resources*

Crowdstrike. “Incident Response.” Accessed November 18, 2020. https://www.crowdstrike.com/services/am-i-breached/incident-response/.

Security Intelligence. “Incident Response.” Accessed April 17, 2019. securityintelligence.com/category/incident-response.

## Cybersecurity Awareness Training

### *References*

Drolet, Michelle. “Seven Tips For A Successful Security Awareness Training Program.” *Forbes*. August 16, 2019. https://www.forbes.com/sites/forbestechcouncil/2019/08/16/seven-tips-for-a-successful-security-awareness-training-program/.

Harris, Shon, and Fernando Maymi. 2016. *CISSP All-in-One Exam Guide 7th ed*. New York: McGraw Hill Education.

Osterman Research. “The Truth About Cybersecurity Training.” 2020. Accessed December 10, 2020. https://www.mimecast.com/globalassets/documents/whitepapers/wp_thetruth_cybersecuritytraining_osterman.pdf.

Ponemon Institute. 2017. *2017 Cost of Data Breach Study*. https://www.ibm.com/downloads/cas/ZYKLN2E3.

Zetter, Kim. 2014. *Countdown to Zero Day*. New York: Crown Publishers.

### *More Resources*

Bedell, Crystal. “First Line of Defense: Are Humans Doing a Good Enough Job?” InfoSecurity Professional. May 14, 2020. https://blog.isc2.org/isc2_blog/2020/05/the-first-line-of-defense-are-humans-doing-a-good-enough-job.html.

Livingsecurity. “Immersive Cybersecurity Training Content to Engage Employees...and Keep Them Learning.” Accessed December 11, 2020. https://www.livingsecurity.com/products/cybersecurity-training-content.

Morgan, Steve. “Twitter Sends Its Employees Back To School For Cybersecurity Training.” *Cybercrime Magazine* (blog). July 18, 2020. https://cybersecurityventures.com/twitter-sends-its-employees-back-to-school-for-cybersecurity-training/.

Osterman Research. 2018. *Best Practices for Protecting Against Phishing, Ransomware, and Email Fraud.* https://www.knowbe4.com/hubfs/Best_Practices_for_Protecting_Against_Phishing_Ransomware_and_Email_Fraud.pdf?hsCtaTracking=67a14d06-dd12-49c7-8070-93fa017a2729%7C082896ec-48d5-4248-b50b-a38e0076ee1a

Rose, Ashley. “Security Awareness Training: Don’t Blame Your Employees.” *Cybercrime Magazine* (blog). October 12, 2020. https://cybersecurityventures.com/security-awareness-training-dont-blame-your-employees/.

## Workforce

### *References*

ISC$^2$. “(ISC)2 Finds the Cybersecurity Workforce Needs to Grow 145% to Close Skills Gap and Better Defend Organizations Worldwide.” November 6, 2019. https://www.isc2.org:443/News-and-Events/Press-Room/Posts/2019/11/06/ISC2-Finds-the-Cybersecurity-Workforce-Needs-to-Grow--145.

**www.resilient-energy.org | www.nrel.gov/usaid-partnership**

**Jeremy Foster**
U.S. Agency for International Development
Email: jfoster@usaid.gov

**Sarah Lawson**
U.S. Agency for International Development
Email: slawson@usaid.gov

**Sadie Cox**
National Renewable Energy Laboratory
Email: sadie.cox@nrel.gov

The Resilient Energy Platform provides expertly curated resources, training, tools, and technical assistance to enhance power sector resilience. The Resilient Energy Platform is supported by the U.S. Agency for International Development.

The USAID-NREL Partnership addresses critical challenges to scaling up advanced energy systems through global tools and technical assistance, including the Renewable Energy Data Explorer, Greening the Grid, the International Jobs and Economic Development Impacts tool, and the Resilient Energy Platform. More information can be found at: **www.nrel.gov/usaid-partnership**.

NREL/TP-5R00-79396 | March 2021