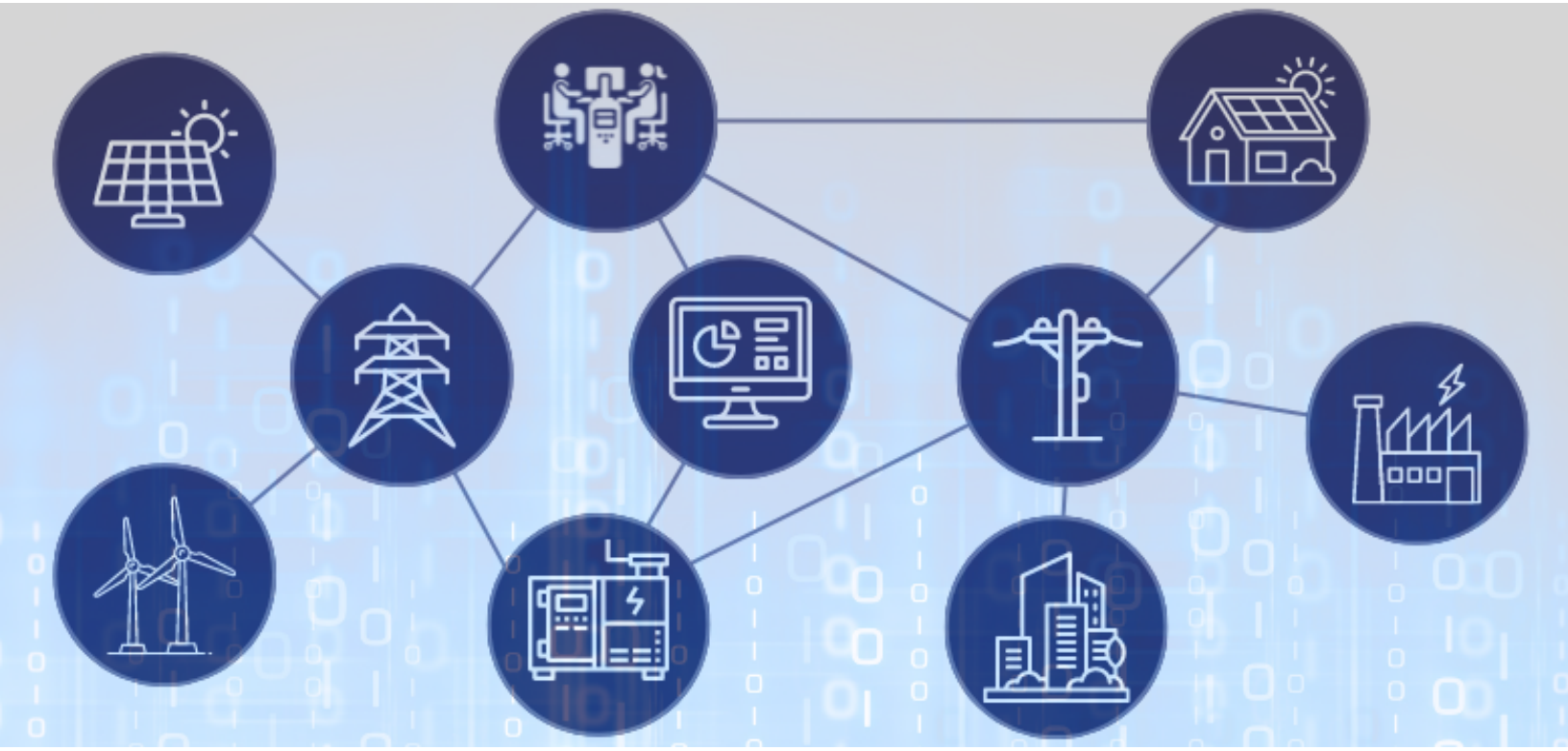


PHOTO CREDIT: EnerNex

CYBERSECURITY AND DIGITALIZATION: HANDBOOK ON ELECTRIC SECTOR SUPPLY CHAIN CYBERSECURITY

December 2024

Disclaimer

This Handbook is made possible by the generous support of the American people through the United States Agency for International Development (USAID). The contents are the responsibility of USEA and EnerNex and do not necessarily reflect the views of USAID or the United States Government.

Executive Summary

The global electric sector depends on increasingly complex supply chains, which have become a source of cybersecurity risk that utilities and other organizations in the sector must manage, especially as they continue toward digitalization to realize efficiency and control in their operations. Cybersecurity Supply Chain Risk Management (C-SCRM) requires organizations to understand not only their own infrastructure and processes, but also their dependencies on vendors, their vendors' cybersecurity risk management capabilities, and the cybersecurity capabilities of the vendors' products. This handbook considers C-SCRM through the lenses of risk management, asset management, policies and planning, and procurement. Each section captures the information presented during a live webinar (recordings are available on the United States Energy Association's website for Cybersecurity and Digitalization) and provides links to additional resources to help utilities learn about and implement C-SCRM. Links to the individual webinars can also be found at the beginning of each section and in Appendix C.

Risk Management

Risk management begins with understanding risk. In the supply chain context, measures to assess and mitigate risk depend heavily on what the utility can control and what their vendors must control. Standards like International Standards Organization/International Electrotechnical Commission (ISO/IEC) 27001 and International Society of Automation (ISA)/IEC 62443 can be useful to utilities and vendors to provide assurance about practices and expectations on both sides. Utilities must understand how they can work with vendors and hold them accountable, while vendors need a clear understanding of expectations and requirements. Building trust through relationships becomes essential, but at the same time, utilities must take ownership of the final implementation and verify that their own needs are met.

Asset Management

Bringing vendor assets into the utility network requires careful consideration of the relative benefits and risks. Mitigations that reduce risks include deploying defensible architectures and secure remote access, including secure cloud services. A defensible architecture should align with and support the utility's incident response plan. That is, the network architecture, including strong demarcation between enterprise information technology (IT) networks and operational technology (OT) networks, should help the utility maintain operations throughout an incident from detection to response and through recovery. As organizations grow, their network architecture will have to evolve to maintain appropriate cybersecurity capabilities while procuring and deploying new systems. As organizations rely more on remote access and cloud services, careful consideration of the relative benefits and risks is needed. In both cases, best practices in defensible architecture can help mitigate identified risks.

Policies and Planning / Governance

One of the most important cybersecurity controls any organization can implement is an Incident Response Plan. Two examples of incident response plans, with focus on response to supply chain incidents, demonstrate common concerns that utilities must address.

A durable cyber risk management program requires executive buy-in. As supply chain cybersecurity risks grow, procurement policies and processes take on greater importance. Governance drives strategy and management will be the final determinant of risk tolerance.

Finally, several tools have been developed to help organizations manage cybersecurity risks, especially C-SCRM. Cyber informed engineering (CIE) presents a systematic process to incorporate cybersecurity

into the development of new projects and maintenance of existing infrastructure. The Distributed Energy Resources Cybersecurity Framework (DERCF) is a tool to manage risks associated with DER, a rapidly growing generation source that will be essential to many countries to meet climate change goals.

Procurement

The procurement process is the moment where the organization interacts directly with the supply chain and has the greatest opportunity to shape the relationship. Utilities must know their own requirements going into the procurement process and should not shy away from holding vendors to account in order to get products that match the utility's needs. Resources like the North American Transmission Forum's (NATF's) Energy Sector Supply Chain Risk Questionnaire provide a widely used resource to evaluate vendors during procurement. An Implementation Plan can be a good place to capture details, including cybersecurity considerations, throughout the deployment process.

Acknowledgements

This *Handbook on Electric Sector Supply Chain Cybersecurity* and the ten-part webinar series on Supply Chain Cybersecurity was developed by the United States Energy Association (USEA) and EnerNex LLC with funding and guidance from the U.S. Agency for International Development (USAID). The writing team would like to thank Marina Barnett, Marjorie Jean-Pierre, and Tricia Williams at USEA as well as Jamila Amodeo and Kristen Madler at USAID for coordinating and managing the webinar series and for their contributions to this handbook.

The writing team at EnerNex, including Scott Morgan, Hannah Mendel, and Mark Szewczuk, extend their gratitude to the many speakers and presenters who provided their cybersecurity expertise in individual webinars.

Webinar Speakers and Presenters

Jamila Amodeo
USAID

Tony Assan
GRIDCo Ghana

Frances Cleveland
Xanthus Consulting International

Mikhail Falkovich
Consolidated Edison (ConEd)

Camilo Gomez
Yokogawa

Frank Harrill
Schweitzer Engineering Laboratories (SEL, Inc.)

Frank Honkus
Electricity Information Sharing and Analysis Center (E-ISAC)

Claudia Iannazzo
Catalisto

Terri Khalil
Ampyx Cyber (formerly Ampere Industrial Security)

Michael Martin
Chelan County Public Utility District (PUD)

Mark Menezes
USEA

Roland Miller, III
Cyber Florida

Markus Mueller
Dragos, Inc.

Sokol Mukaj
KESH (Albanian Power Corporation)

Jacob Phillips
Midcontinent Independent System Operator (MISO)

Gigi Pugni
START 4.0 Competence Center (Italy)

Anuj Sanghvi
National Renewable Energy Laboratory (NREL)

Justin Searle
InGuardians

Jason Shea
Southern California Edison (SCE)

Ginger Wright
Idaho National Laboratory (INL)

Contents

Figures

Acronyms

AD	Active Directory
ADKAR	Awareness, Desire, Knowledge, Ability, and Reinforcement
ADMS	Advanced Distribution Management System
AMI	Advanced Metering Infrastructure
AmpUp	Advancing Modern Power through Utility Partnerships
AMR	Automatic Meter Reading
APN	Access Point Name
APT	Advanced Persistent Threat
BESS	Battery Energy Storage System
C2M2	Cybersecurity Capability Maturity Model
CIE	Cyber Informed Engineering
CIP	Critical Infrastructure Protection
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
CMF	Collection Management Framework
CRM	Customer Relationship Management
C-SCRM	Cybersecurity – Supply Chain Risk Management
CSIRT	Cybersecurity Incident Response Team
CSO	Chief Security Officer
CVE	Common Vulnerabilities and Exposures
DER	Distributed Energy Resources
DERCF	Distributed Energy Resources Cybersecurity Framework
DERMS	Distributed Energy Resources Management System
DMS	Distribution Management System
DMZ	Demilitarized Zone
DSO	Distribution System Operator
EDR	Endpoint Detection and Response
EEI	Edison Electric Institute
E-ISAC	Electricity Information Sharing and Analysis Center
FAN	Field Area Network
FAT	Factory Acceptance Testing
FEPs	Front-End Processors
GDP	Gross Domestic Product
GDPR	Global Data Protection Regulations
GIS	Geographic Information System
HMI	Human-Machine Interface
IACS	Industrial Automation and Control System
ICS	Industrial Control System
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IMP	Incident Management Plan
INL	Idaho National Laboratory
IP	Internet Protocol
IPS	Intrusion Prevention System
IR	Incident Response
IRP	Incident Response Plan
ISA	International Society of Automation
ISMS	Information Security Management System
ISO	International Standards Organization

IT	Information Technology
KESH	Albanian Energy Corporation
KPI	Key Performance Indicator
MFA	Multi-Factor Authentication
MISO	Midcontinent Independent System Operator
MPLS	Multiprotocol label switching
MSSP	Managed Security Service Provider
NAS	Network Attached Storage
NATF	North American Transmission Forum
NVD	National Vulnerabilities Database
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
NREL	National Renewable Energy Laboratory
OCM	Organizational Change Management
OMS	Outage Management System
OT	Operational Technology
OT/OPS	Operational Technology / Operations
OT-CERT	Operational Technology - Cyber Emergency Readiness Team
PAM	Privileged Access Management
PCI	Payment Card Industry
PKI	Public Key Infrastructure
PLC	Programmable Logic Controller
PUD	Public Utility District
RaaS	Ransomware as a Service
RBAC	Role Based Access Control
RFP	Request for Proposal
RTU	Remote Terminal Unit
SAT	Site Acceptance Testing
SCADA	Supervisory Control and Data Acquisition
SCE	Southern California Edison
SDN	Software-Defined Networking
SD-WAN	Software-Defined Wide Area Network
SEL	Schweitzer Engineering Laboratories
SIEM	Security Incident and Event Management
SLA	Service Level Agreement
SOC	Security Operations Center
SOC2	Service Organization Control 2
TSO	Transmission System Operator
TLS	Transport Layer Security
TSA	Transportation Security Administration
USAID	United States Agency for International Development
USEA	United States Energy Association
VPN	Virtual Private Network
XDR	Extended Detection and Response
YoY	Year-over-Year
ZTA	Zero Trust Architecture

Introduction

The global electric power sector depends on increasingly complex supply chains that have become a source of cybersecurity risk, which utilities and other organizations in the sector must manage, especially as they continue toward digitalization to realize efficiency and control in their operations. Cybersecurity Supply Chain Risk Management (C-SCRM) requires organizations to understand not only their own infrastructure and processes, but also their dependencies on vendors, their vendors' cybersecurity risk management capabilities, and the cybersecurity capabilities of the vendors' products. This handbook considers C-SCRM through the lenses of risk management, asset management, policies and planning, and procurement.

Organization of this Handbook

The contents of this handbook were developed based on a ten-part webinar series on supply chain cybersecurity issues in the electric power sector. These webinars were recorded and links to each are included at the beginning of each section and in Appendix B. The webinar series was organized through the US Energy Association's (USEA's) Advancing Modern Power Through Utility Partnerships (AmpUp) program. The AmpUp program is funded by the United States Agency for International Development (USAID). The ten webinars were grouped into four overarching categories:

- **Risk Management**: The webinars in this section examined the current landscape of supply chain cybersecurity risks, the standards that exist to help organizations address that risk, and the methods that utilities can apply for risk assessment and mitigation.
- **Asset Management**: The webinars in this section looked at how organizations can adapt to supply chain risks through sound asset management. Defensible architecture is foundational to mitigating many cybersecurity risks, including supply chain risks. Defensible architecture also enables utilities to rely on vendors who require remote access, including cloud services, which act a bit like remote users with uninterrupted remote access.
- **Governance, Policies, And Planning:** The webinars in this section covered some of the strategic, executive thinking needed to build a culture of security, including supply chain cybersecurity. All utilities should develop incident response plans that capture how personnel would respond to an incident, especially a supply chain related incident. This plan drives requirements for additional controls and capabilities. Governance policies and procedures are essential to create a unified security posture across the organization and to identify and address gaps. Strategic planning and risk management can be informed by popular frameworks and tools such as the Cyber Informed Engineering (CIE) and the Distributed Energy Resources Cybersecurity Framework (DERCF) discussed here.
- **Procurement:** The webinars in this section explored the procurement process and lifecycle of relationships with vendors. Utilities must begin with cybersecurity in mind when procuring new products and systems, from gathering requirements prior to the request for proposal, to evaluating vendors and their products, to deploying selected products and services, and even through off-boarding vendors at the end of a relationship with a supplier.

Appendix A contains hyperlinks to additional resources noted in each section. The list of webinars, presenters, and links to recordings are captured in Appendix B.

This webinar series and handbook are a follow-up to the 2020 webinar series and the "Electricity Sector Cybersecurity and Digitalization Handbook" from USAID and USEA.

Photo Credit: USAID Energy/Flickr

Risk Management

The Emerging Cyber Threats to Industrial Control Systems (ICS) – Supply Chain Cybersecurity

Presenter:

- **Camilo Gomez**, Global Cybersecurity Strategist, Yokogawa

In a world of increasing global cybersecurity threats, organizations need to understand the nature of the threats, as well as to recognize the role that organizations play in end-to-end supply chain cybersecurity in responding to them. Critical infrastructure like energy utilities often lack a workforce with specialized skills needed to address cyber security. Webinar Recording

Standards on Third-Party Risk Management and Cyber Risk Assessment Methodologies

Presenters:

- **Frances Cleveland**, President and Principal Consultant, Xanthus Consulting International
- **Gigi Pugni**, START 4.0 Competence Center

Internationally accepted standards and guidelines support identifying and managing cybersecurity risks associated with the supply chain risk from third parties/suppliers. A survey of these resources (e.g., the U.S. National Institute of Standards and Technology [NIST] Cybersecurity Framework, NIST SP 800-161, ISO/IEC 27036-1:2021, NISTIR 8276) is presented. Webinar Recording

Conducting Cyber Risk Assessments for Supply Chain Risk Management

Presenters:

- **Frank Honkus,** Associate Director of Intelligence Programs / Director of the Cybersecurity Risk Information Sharing Program (CRISP), E-ISAC
- **Mikhail Falkovich,** Chief Information Security Officer, Con Edison

This section examines risk management practices for supply chain related cybersecurity risks, including considerations for supply chain vulnerability management and equipment country-of-origin. Risk management implies understanding threats, vulnerabilities, and potential impacts. Effective risk management also addresses prioritization, developing projects to mitigate risks, and evaluating the effectiveness of mitigations. Webinar Recording

The Emerging Cyber Threats to Industrial Control Systems (ICS) – Supply Chain Cybersecurity

Presenter
Camilo Gomez Yokogawa Webinar Recording Presentation Slides

In a time defined by rapid technology advancements, the increasing digitalization of critical infrastructure brings new opportunities to modernize and improve the electric sector worldwide. These new opportunities also bring new cybersecurity risks. As organizations embrace digital controls, the supply chain for the electric sector—from new systems within utilities, to cloud services, to integrating third-party operations like distributed energy resource (DER) aggregators—has become an essential consideration in any digitalization project. Electric utilities must recognize indicators of threat, identify potential vulnerabilities, and respond to threats before serious consequences arise. The supply chain is one key place to analyze these risks.

Threat Categorization

There are several recent high-profile cyberattacks that all utilities should learn from and analyze from their own perspective: the 2016 Ukrainian electric grid attack, the 2020 SolarWinds hack, and the 2021 Colonial Pipeline ransomware event that led to a gas and diesel fuel panic in the United States are quintessential examples of the potential impact that cyberattacks can have. The attackers in each case had unique motivations, but they engineered each attack in ways that best suited their intended target. The 2020 SolarWinds hack stands out because of the attackers' abuse of legitimate supply chain channels.

In December 2016, a substation in the Ukrainian electric transmission grid was the target of a cyberattack, resulting in an approximately one-hour blackout in Kyiv, a smaller impact than it could have been. Hackers attacked operational technology (OT) systems and used a malware framework called CRASHOVERRIDE (also known as Industroyer) to target and physically disrupt operations by opening relays to interrupt power flow and digitally wiping equipment to make it unusable among other functions. CRASHOVERRIDE is a modular framework that utilized an initial backdoor to provide attackers with access to the system and then deployed a loader module and payload modules. The modular framework made this malware adaptable to maximize damage and potentially target a wide array of utilities.[1]

The Colonial Pipeline attack resulted in a six-day halt of the company's operations in 2021, causing a loss of 100 million gallons of fuel per day to consumers. This led to a gasoline, diesel fuel, and jet fuel shortage panic on the eastern seaboard of the United States. Unlike the Ukrainian grid attack that targeted OT systems, Colonial Pipeline faced a ransomware attack that infected their IT network. The attackers used ransomware-as-a-service (RaaS) after accessing the Colonial Pipeline network through a compromised password for a virtual private network (VPN) account of an end-user at the company. Colonial Pipeline chose to shut down operations out of an abundance of caution to ensure the ransomware would not directly impact OT systems.[2]

In 2020, SolarWinds faced a similar attack on their information technology (IT) systems; however, rather than directly impacting SolarWinds, the attackers inserted malicious code into the Orion framework, SolarWinds' platform for IT performance monitoring and management, which is used by thousands of

[1] See ESET: Win32/Industroyer: a new threat for industrial control systems and Dragos, Inc.: CRASHOVERRIDE Analysis of the Threat to Electric Grid Operations for two descriptions of the attack.

[2] Colonial Pipeline Company, Media Statement Update: Colonial Pipeline System Disruption

organizations. The attackers used a cutting-edge attack method and distributed hidden malware to Orion users through a legitimate, routine software update of Orion that was pushed to client organizations. Unbeknownst to Orion users, upon accepting the compromised software update, the victim organizations inadvertently granted the hackers access to their systems, confidential data, and classified files. In addition to data breaches for multinational companies and government agencies around the world, SolarWinds suffered hundreds of millions of dollars in reputational impact.

Cybercrimes can be analyzed in terms of "who" commits the crimes, "what" is the (potential) impact to the organization, "why" the criminals targeted the victim, and "how" the attack was possible. Five different threat actors who carry out these attacks include: insiders, hacktivists, cyber criminals, nation-states, and terrorists. Although important to be aware of who the attackers are, the "what," "why," and "how" behind cybercrime are more important.

Organizations play a crucial role in end-to-end supply chain cybersecurity by taking appropriate actions to respond to and mitigate threats. Whether the attackers exploit people or technology vulnerabilities, ultimately, attackers are only successful if they can gain access to the system, which is something that can be controlled by enacting cybersecurity controls—measures that can reduce the risk of a cybersecurity attack. However, even the most secure organizations are at risk as attack methods are evolving. Supply chain attacks have become more common but remain difficult to detect and protect against.

End-to-End Supply Chain Cybersecurity

Supply chain cybersecurity is only as strong as its weakest link. To adequately defend against cybercrime, end-to-end supply chain cybersecurity must be prioritized by organizations. End-to-end supply chain cybersecurity places responsibility on all roles—from fabrication to consumption—to tackle threats and reduce vulnerabilities.

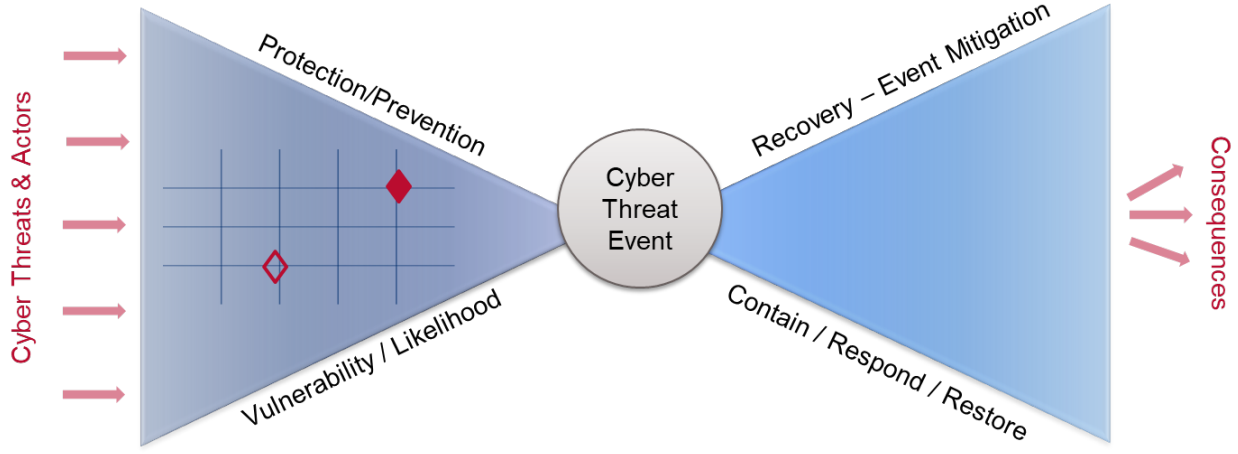


Figure 1. Risk Management Bow Tie

The Risk Management Bow Tie (Figure 1) is a visual, scenario-based method for risk identification, analysis, and management. It provides a framework for analyzing potential malicious cyber threats and actors and possible mitigating actions to minimize any consequences or negative outcomes. The left side of the bow tie represents protective/preventative measures that impede incoming cyber threats and bad

TSA Pipeline Regulation

One recent example of cybersecurity regulations is the Transportation Security Administration (TSA) Pipeline Security Directive, *Pipeline-2021-02 series: Pipeline Cybersecurity Mitigation Actions, Contingency Planning, and Testing*. This directive was issued by the United States TSA in response to the Colonial Pipeline attack in 2021. Following the attack, TSA mandated that owners and operators of critical liquid and natural gas pipelines establish and implement a *Cybersecurity Implementation Plan*, develop and maintain a *Cybersecurity Incident Response Plan*, and establish a *Cybersecurity Assessment Program* to proactively and continually test implemented cybersecurity measures and identify and correct any vulnerabilities. The scope of the directive is for any IT and OT system or data that, if compromised or exploited, could result in operation disruption, including business services that, if compromised or exploited, could result in operational disruptions (e.g., billing systems).

The requirements in the TSA Pipeline Security Directive align with the Risk Management Bowtie. The *Cybersecurity Implementation Plan* covers the full bowtie from end to end. The right side constitutes the *Cybersecurity Incident Response Plan*, and the left side lists the prevention plans and programs that are to be routinely tested for effectiveness in the *Cybersecurity Assessment Program*.

actors depicted by inbound red arrows on the left. The right side corresponds to recovery actions in place to reduce consequences. Prevention is based on both the vulnerability and the likelihood of that vulnerability being exploited. Recovery efforts deal with containing the event, responding to the event, and restoring operations to minimize negative outcomes.

On the left side, examples of barriers to cyber threats include security programs, security policies and procedures, infrastructure defense, products with built-in defenses, and threat detection mechanisms. When these mechanisms are not sufficient, recovery measures are enacted to contain and respond to the attack, and to restore the system(s) while mitigating negative consequences. These measures can include triage procedures and alerting, response and communication procedures, drill exercises, organizational impact management, and even forensics to identify lessons learned and fortify the system moving forward.[3]

IT vs. OT Supply Chains

IT and OT have unique supply chains and unique risks, as shown in Table 1, below. For example, IT systems and devices tend to be refreshed every 2-5 years. OT systems, on the other hand, are not replaced or significantly updated as frequently as IT devices. OT sees technology refreshes typically every 10-15 years, oftentimes even longer, rendering their security and communication protocols obsolete and leaving the systems exposed compared to their more frequently refreshed IT counterparts. These long operational lives place greater importance on quality incident response plans, secure network architecture, and risk-based vulnerability management programs.

Table 1. Unique Challenges in IT and OT Supply Chain Risk Management

Challenges		
	IT	**OT**
Technology Refresh	2-5 years	5+ years
Typical size of capital projects	Millions	Multi-millions to billions
Weight of Budget	Capital project: High	Operations: Low
Built-in Capability of Legacy	Somewhat capable	Incapable/less capable

[3] See the webinar, "Cybersecurity Incident Response Plan Development," summarized below for more information.

IT and OT supply chains have unique strengths as well, as shown in Table 2, below. Both have their own series of standards that define methods and procedures to protect their assets. IT often follows the ISO/IEC 27000 series that applies to information security management systems (ISMS), and OT follows the ISA/IEC 62443 series that applies to industrial automation and control systems (IACS), with the latter helping bridge the gap between IT and OT. Unlike IT devices, it is common for OT devices to come with cybersecurity, safety, and interoperability certifications due to their long lifecycle and long replacement timeline.

Table 2. Unique Strengths in IT and OT Supply Chain Risk Management

Strengths		
	IT	**OT**
Standards	ISO/IEC 27000	ISA/IEC 62443
Product Certification	Unpopular	Prevalent
Standards Supply Chain Assurance	Product	Both Product and Product Supplier Organization

OT supply chains further enhance product certifications as it is common for the supplier to also have their own assurances with respect to production standards. Not only are OT products certified, but the companies building and providing the products are certified to have processes in place that align with appropriate standards. As it is less common to provide certifications for IT products, naturally, it is less common to provide assurances that IT product suppliers align with applicable standards.

OT product security certifications frequently follow the ISA/IEC 62443 series of standards. This series addresses end-to-end supply chain cybersecurity by defining standards for each role in the supply chain: product suppliers, service providers, system integrators, and asset owners. Certifications based on the 62443 series holistically assess products and systems to ensure that they are secure by design with built-in security capabilities and free of known vulnerabilities. Other certifications are also available, such as those that ensure support throughout the entire lifecycle of the product, including patches for new vulnerabilities and end-of-life product support.

Vulnerability Intelligence & Management

Vulnerabilities are key to understanding risks. Two vulnerability intelligence and management websites for IT and OT, respectively are CVE.org and CISA.gov. These sites provide vulnerability reporting, vulnerability alerts, and other technical intel for their respective jurisdictions.

The MITRE ATT&CK framework (https://attack.mitre.org/) is another valuable vulnerability repository and framework for attack classification where users are able to familiarize themselves with known attack techniques and tactics and learn how to best defend against adversaries

Additional Resources

- National Renewable Energy Laboratories (NREL), Resilient Energy Platform
- TSA Pipeline Security Directive 2021-01B (see also the full list of Security Directives)
- ISA Standards
- IEC Standards
- ISASecure Certification: ISASecure - IEC 62443 Conformance Certification
- IECEE CMC Certification
- Common Vulnerabilities and Exposures website (CVE.org)
- U.S. Cybersecurity and Infrastructure Security Agency (CISA)

- MITRE ATT&CK
- USEA Webinar on Standards and Best Practices
- USEA Webinar on ISO 27001

Standards on Third-Party Risk Management and Cyber Risk Assessment Methodologies

Presenters

Frances Cleveland
Xanthus Consulting International

Gigi Pugni
START 4.0 Competence Center

Webinar Recording

Presentation Slides

There are several internationally accepted standards and guidelines that can help address third-party risk management and cyber risk assessment methodologies and mature their risk-management practices.

Cybersecurity is not only a technology issue; it is also an organizational concern that requires appropriate policies and procedures in addition to security technologies. Risk is inherent in operations, so a risk assessment is essential to determine the appropriate mix of policies, procedures, and technologies. One critical aspect of any cybersecurity risk assessment is supply chain cybersecurity.

Unique Qualities of Supply Chain Cybersecurity Standards

Most cybersecurity standards focus on the actions a single organization should take to secure their own people, systems, and operations. Typically, an organization can implement top-down control over their own internal cyber risk management to achieve desired results. Supply chain security risks, on the other hand, involve multiple organizations, which makes these issues complex in relation to other security issues.

The supply chain is often thought of as the procurement of products from other organizations, but it also includes services like access to information such as markets and cloud services, which therefore relies on external communication networks. As DERs become more common, utilities must incorporate equipment from other organizations into their operations as well. These interactions with third party entities add to the complexity.

Supply Chain Risks and Vulnerabilities

Supply chain cybersecurity risks are unique compared to many of the usual cybersecurity considerations. Some examples of supply chain risks can include but are not limited to:

- Utility interfaces to third-party products, which contain malicious code
- Supplier provides lower quality or counterfeit products due to their supply chain problems
- Utility develops software using code from compromised sources
- Utility purchases energy management products from vendors who have deliberately or accidentally incorporated malicious code into their systems

Due to the complexity of the supply chain, there could be numerous points of failure. In many cases, the vulnerability may stem from the utility's failure to do something, such as not having a comprehensive security policy for OT systems, not having a procurement policy that considers cybersecurity, not checking the vendors' supply chain policies, not testing products from vendors, not having multiple vendors for essential products and services, and not enforcing supply chain security requirements on vendors. For example, when utilities bring on DER resources through a third-party aggregator, a contractual agreement should specify requirements, including roles and responsibilities, for both the utility and the third party.

Key Actions to Address Supply Chain Vulnerabilities

Risk Assessments—These assessments are essential to understand the threats, vulnerabilities, and potential impacts. Formal assessment processes systematically consider each area while accounting for the scope of the assessment: the product, system, or organization under assessment.

Power System Monitoring—OT security is sometimes referred to as cybersecurity plus physics. The underlying physical processes of delivering electricity can be an important source of information for identifying anomalies in digital controls, not just within your own organization, but also the interconnecting systems.

Contractual Agreements—Contracts specify requirements for suppliers to hold them accountable for their own cybersecurity risk management and may set minimum expectations around the suppliers' capabilities for protection, detection, response, and recovery, as well as specifics for roles and responsibilities during and after an incident.

Role-Based Access Control (RBAC)—External suppliers frequently need some access to the utility's systems. RBAC is a best practice for implementing strong access control and limiting permissions.

Use of Gateways—Placing gateways in front of and/or between critical systems (e.g., between a utility's supervisory control and data acquisition [SCADA] and an aggregator's DER management system [DERMS]) enables several beneficial controls like access control, data validation, protocol security and agreements.

Standards on Third-Party Risk Management

NIST Cybersecurity Framework 2.0

The NIST Cybersecurity Framework 2.0 is the latest version of one of the most popular international frameworks used to guide organizations building a cybersecurity program. The NIST Framework is an excellent starting point for considering enterprise C-SCRM, which is included as a "Category" in the "Govern" function of the Framework. The Govern function is new in version 2.0 of the Framework, but it matches the lived experience of many organizations: starting with Governance issues, and developing strategies for addressing cybersecurity, including C-SCRM, is an essential step for both large and small companies.

The new version of the NIST Framework includes new subcategories within the C-SCRM category. Previous subcategories promoting a C-SCRM risk management plan, integration of C-SCRM into enterprise risk management, understanding and management of risks associated with suppliers, and including suppliers in incident management plans remain in the new version. In addition, organizations are now encouraged to know their suppliers and prioritize them in terms of their criticality, to perform due diligence before entering formal relationships, to integrate C-SCRM practices in overall risk management programs, and to extend risk management plans through and beyond the conclusion of the relationship with the supplier. Integrating C-SCRM practices into overall risk management programs means not only that organizations must be collecting appropriate information from their suppliers,[4] but also that organizations must set clear expectations on what suppliers must do to support the organization's cybersecurity.

NIST Special Publication 800-161r1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations

The NIST Special Publication 800-161r1, "Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations", provides a comprehensive look at C-SCRM issues. This document

[4] See sections in the "Procurement" chapter below for further guidance.

highlights the reduced visibility, understanding, and control with each step along a supply chain from the acquiring enterprise to their first-tier suppliers, to the second tier, and so on. NIST SP 800-161r1 highlights the activities needed to manage the cybersecurity risk associated with external parties into five categories, which enable an organization to:

- Determine cybersecurity requirements for suppliers
- Implement requirements through formal agreements
- Communicate to suppliers how these requirements will be verified and validated
- Verify that cybersecurity requirements are met through a variety of assessment methodologies
- Continuously maintain and improve the entire process proactively

Translating Requirements Standards to Technical Implementation

Requirement standards like the NIST Cybersecurity Framework, ISA/IEC 62443, and ISO/IEC 27001 are broader than just C-SCRM and provide a good starting point for developing a security program. Technical standards like IEC 62351 on security for communications protocols and guidance standards like ISO 31000 on risk assessments also provide supporting details for a cybersecurity program. These standards and the NIST SP 800-161r1 standard on C-SCRM provide requirements that an organization can translate into policies and guidelines that reflect the unique reality within the organization, for example, by defining roles and responsibilities that align with the personnel and capabilities within the organization (see Figure 2, below). These "global policies" establish the rules of the game for the organization to follow and apply to its unique risks and the underlying assets.

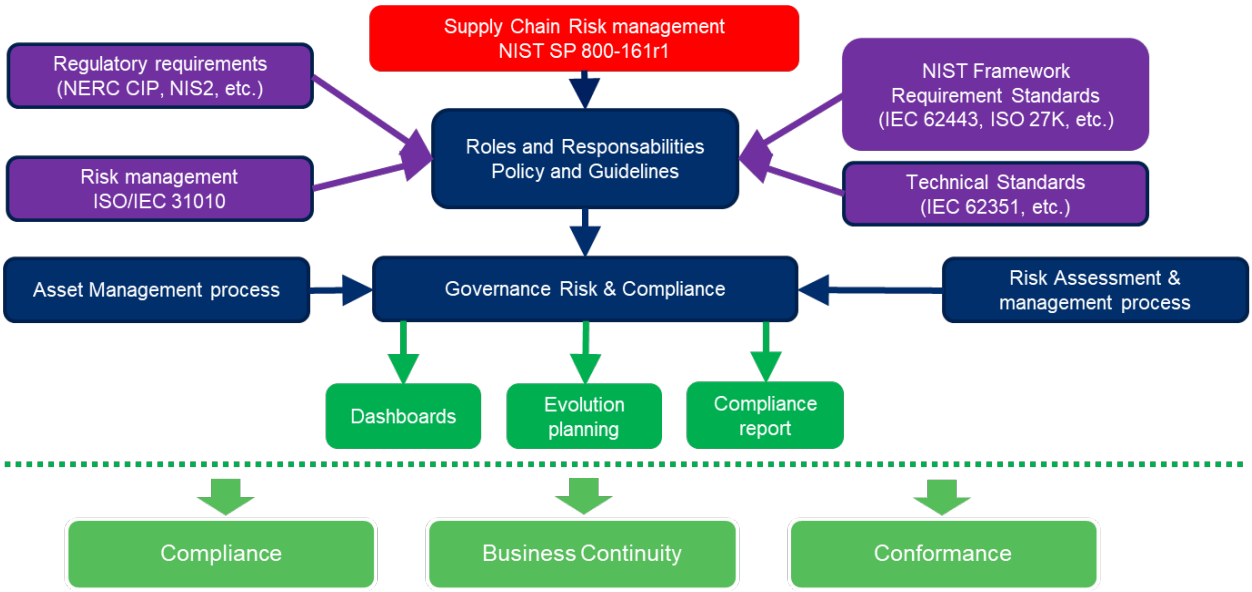


Figure 2. Relationship of various standards to support organizational cybersecurity risk management.

The global policies should be understood and supported by top management and address both internal and external parties. Policies, however, do not specify implementation details and must be translated into the specific requirements for implementation in each context. For example, to carry out a policy that requires RBAC, the organization may need to develop a Public Key Infrastructure (PKI) system. Deploying a technical system like PKI may require another level of specificity supported by standards, e.g., one of the communication protocols security profiles in the IEC 62351 family of standards.

The details of the global policies, the contextual requirements, and the technical specifications will be important not only for the internal controls, but also for external parties to deliver solutions that fit the

organization. Moreover, requirements from international standards like ISA/IEC 62443 and IEC 62351 will be easier for suppliers to understand and implement than an idiosyncratic internal standard would be. Responsibility for each requirement or control should be clearly assigned to specific actors of the supply chain (e.g., client, integrator, manufacturer, service provider).

C-SCRM Lifecycle

The C-SCRM lifecycle is a 5-step process involving each stage of the supply chain, as shown in Figure 3. The first stage begins with understanding and assuring that manufacturers and providers have the right qualifications, including appropriate cybersecurity certifications and competencies. Suppliers must understand that they should be compliant to expected standards such as ISA/IEC 62443 and the ISO 27000 series.

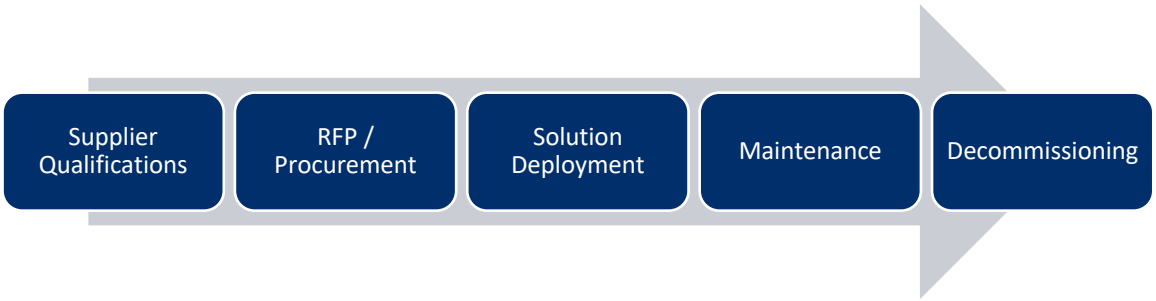


Figure 3. C-SCRM Lifecycle.

The second stage is developing the request for proposal (RFP). A risk assessment should be conducted on the product or service's intended use cases. A utility should consider adding a clause to all contracts with a supplier allowing for periodic audits of technical standard compliance. The utility should ensure that there are significant event notifications and vulnerability alerts when adding new products to the system. Additionally, utilities should ensure that there are lifecycle clauses in contracts, so that suppliers can patch, maintain, and decommission devices and products when necessary.

Following the purchase of a product or service, the enterprise can develop and deploy the solution. The enterprise should design these solutions with security in mind from the beginning and throughout the entire development cycle. The security of these solutions should be standards based (IEC 62531, etc.).

As the solution is deployed into systems and actively in use, a maintenance plan must be developed. Business continuity processes and regular testing can occur on the system to ensure proper functionality. Patching and maintenance plans can be developed to ensure that there are no known vulnerabilities in the solution. Regular audits can be scheduled to ensure that proper maintenance is followed. The utility can develop a Cybersecurity Incident Response Team (CSIRT) to address any identified issues.[5]

The decommissioning phase falls at the end of the lifecycle, where the solution or product is phased out of use. Company sensitive data must be secured and disposed of properly according to regulatory and compliance requirements.

[5] See, for example, discussion of "Implementation Phase" and "Post Implementation Phase & Offboarding" in the section Coordinating Cybersecurity Risk Management with Hardware/Software Vendors, below.

ISO 31000 – Risk Management Applied to Supply Chains

The ISO 31000 standard on Risk Management starts with identifying the scope, context, and criteria for the risk management activities, similar to other standards discussed above. Without these high-level considerations captured in policies, it would be impossible to manage the vendor relationships. As the organization's business processes and risks change, the scope, context, and criteria should be re-evaluated to ensure continuous improvement.

The second step in the ISO 31000 risk management process is the risk assessment. There are many methods to follow, particularly NIST SP 800-161r1 discussed above. Organizations must adapt whatever method they follow to their own operations. Questionnaires and interviews are solid sources of performing a risk assessment, but it is also important to gather statistical information on the success of supplier quality.

This standard also highlights communications, not only with internal stakeholders, but also with vendors, customers, and authorities. Finally, the steps above feed into the risk treatment, which accounts for all the previous considerations.

Tailoring Standards to the Organization

Starting with governance is essential because it defines the rules of the game in a way that makes sense for your organization. For example, organizations in the electric sector may face regulatory requirements that make certain supply chain related actions difficult, such as notification timelines for vulnerabilities. A long and intricate supply chain will make the notification process difficult, increasing the chance of falling out of compliance with a regulation with strict notification timing requirements. A second example is the OT assets that electric utilities rely on. OT assets have much longer lifecycles than IT assets, and they tend to be more distributed, which may mean solutions meant for IT will not be supported by OT assets, so policies should be tailored with these considerations in mind.

Additional Resources

- NIST SP 800-161r1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations
- NIST Cybersecurity Framework v2.0
- European Energy Information Sharing & Analysis Centre (EE-ISAC)
- ISO/IEC 27001 – Information Security Management System
- ISA/IEC 62443 Standards – Security of Industrial Automation and Control Systems
- IEC 62531 – Cyber Security Series for the Smart Grid
- ISO 31000 Risk management

Conducting Cyber Risk Assessments for Supply Chain Risk Management

Presenters
Frank Honkus E-ISAC
Mikhail Falkovich ConEd
Webinar Recording
Presentation Slides

As supply chain operations become increasingly interconnected and digitalized, organizations must conduct cyber risk assessments on procured products and services and their suppliers. Supply chain risk management is a dynamic and ongoing process that requires an understanding of existing threats and vulnerabilities in all areas of the supply chain. Successful supply chain risk management tactics address prioritization, employ continual assessments, and involve collaboration with others up and down the supply chain and across the whole industry. Due to the breadth of supply chains, it is paramount that organizations stay vigilant in their own self-assessments and vendor evaluations.

Understanding vulnerabilities is a key component of understanding risk. Vulnerabilities exist in both the IT and OT space and can be found in hardware and software alike. Vulnerabilities in products introduce risk wherever they are deployed, both in terms of where on the network they are deployed or where, physically within the organization they are deployed. Vulnerabilities are not limited to products but may also exist in services as well, which can also introduce risk.

Country-of-origin risks represent one class of risks to consider. The country where products or services originate may not align with your organization's security posture. That country's standards of hardware and software development may not be sufficient. They may lack regulations to encourage secure development practices, or they may have regulations or local laws that actively require capabilities that could be concerning, like prioritizing the ability to monitor devices over privacy. There may also be concerns about using real-time support, which could result in connections from the country into your organization (e.g., for troubleshooting) or a phone call, which may be recorded and monitored.

As a hypothetical example, an electric utility may have a requirement in their procurement contracts that technology products should be manufactured within their own country, "Country X." A product the utility procures may be assembled in Country X, but some of the internal hardware components were manufactured in "Country Y." After deployment, the utility's security team detects outbound communication between the product and the infrastructure of that foreign country, Country Y.

In industry, it is common for manufacturers to source components from foreign countries and then assemble and resell the device in their home country. In this example, unbeknownst to the utility, the technology product used internal hardware components that were produced in Country Y. Supply chains can easily and unintentionally obfuscate some of these country-of-origin concerns.

Risk Mitigation Strategies

To address cybersecurity supply chain risks, organizations must manage these third-party risks. C-SCRM risks should be considered within the broader risk context, which could include potential financial, geopolitical, and cybersecurity risks introduced by any specific vendor. Organizations may choose to conduct a risk assessment of a vendor and their product internally or the organization may choose a separate vendor or aggregator to conduct the assessment. Regardless of choice of assessor, it is up to the purchasing organization to accept the risk. If the risk is deemed too high to accept, the purchasing organization will have to identify alternatives. Although there are standards and frameworks to help

organizations assess risk, such as ISO 27001 and Service Organization Control 2 (SOC2), nothing is foolproof. Even the most well-functioning and well-protected third parties face the risks of cyberattacks and data breaches, so it is crucial that organizations take additional steps to mitigate and manage risk.

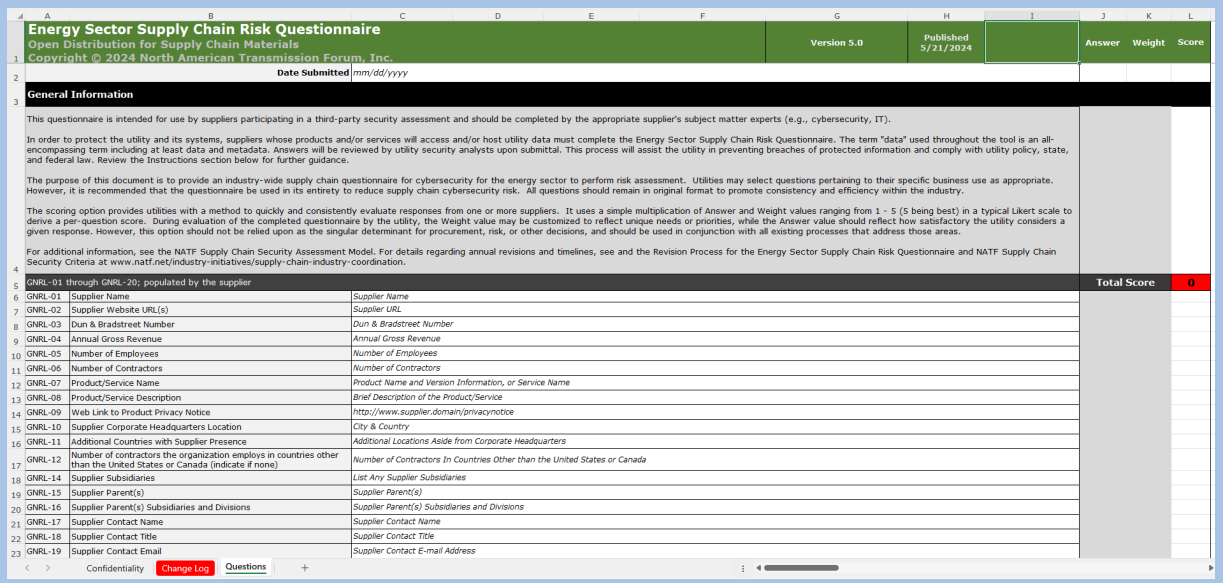
Another type of risk management strategy is the application of cybersecurity controls. Cybersecurity controls encompass a wide range of activities whose aim is to reduce risk. Risk assessments can help to prioritize and evaluate controls based on risk tier. The first step in a vendor product/service risk assessment is understanding the impact if that product fails or that service goes away. How much damage would that cause to business operations? The answer enables the organizations to assign that risk a tier, which they can use to identify the level of protection an asset requires. Not all failures are created equal; different levels of data sensitivity and operational significance require different levels of security. For example, a service that relies on the organization's public data is much less risky in terms of data protection than a service that relies on proprietary company data.

The severity and impact of a risk can be unique to different organizations, so the organization must set thresholds and determine what is risky and what is less risky; nothing is risk-free. However, depending on the region and the industry, regulatory bodies may mandate compliance requirements for how to manage risk and validate controls (for example, North American Electric Reliability [NERC] Critical Infrastructure Protection [CIP] in North America). Organizations must ensure that their risk management strategies align with both their own internal needs and local regulatory requirements, if

NATF Vendor Cybersecurity Questionnaire

Many utilities and organizations require vendors to respond to cybersecurity questionnaires and evaluations. Vendors may receive thousands of distinct questionnaires if every organization had its own evaluation process.

The North American Transmission Forum (NATF) managed a collaborative industry process to develop a Supply Chain Criteria and Risk Questionnaire, that is freely available, to manage this dilemma. The Risk Questionnaire was endorsed by NERC and has been implemented globally. Many vendors, in turn, have already completed this questionnaire, and maintain their responses to quickly provide this information to purchasing utilities.



1	**Energy Sector Supply Chain Risk Questionnaire** Open Distribution for Supply Chain Materials Copyright © 2024 North American Transmission Forum, Inc.					Version 5.0	Published 5/21/2024		Answer	Weight	Score
2		**Date Submitted**	*mm/dd/yyyy*								
3	**General Information**										
4	This questionnaire is intended for use by suppliers participating in a third-party security assessment and should be completed by the appropriate supplier's subject matter experts (e.g., cybersecurity, IT). In order to protect the utility and its systems, suppliers whose products and/or services will access and/or host utility data must complete the Energy Sector Supply Chain Risk Questionnaire. The term "data" used throughout the tool is an all-encompassing term including at least data and metadata. Answers will be reviewed by utility security analysts upon submittal. This process will assist the utility in preventing breaches of protected information and comply with utility policy, state, and federal law. Review the Instructions section below for further guidance. The purpose of this document is to provide an industry-wide supply chain questionnaire for cybersecurity for the energy sector to perform risk assessment. Utilities may select questions pertaining to their specific business use as appropriate. However, it is recommended that the questionnaire be used in its entirety to reduce supply chain cybersecurity risk. All questions should remain in original format to promote consistency and efficiency within the industry. The scoring option provides utilities with a method to quickly and consistently evaluate responses from one or more suppliers. It uses a simple multiplication of Answer and Weight values ranging from 1 - 5 (5 being best) in a typical Likert scale to derive a per-question score. During evaluation of the completed questionnaire by the utility, the Weight value may be customized to reflect unique needs or priorities, while the Answer value should reflect how satisfactory the utility considers a given response. However, this option should not be relied upon as the singular determinant for procurement, risk, or other decisions, and should be used in conjunction with all existing processes that address those areas. For additional information, see the NATF Supply Chain Security Assessment Model. For details regarding annual revisions and timelines, see and the Revision Process for the Energy Sector Supply Chain Risk Questionnaire and NATF Supply Chain Security Criteria at www.natf.net/industry-initiatives/supply-chain-industry-coordination.										
5	GNRL-01 through GNRL-20; populated by the supplier								Total Score		0
6	GNRL-01	Supplier Name	*Supplier Name*								
7	GNRL-02	Supplier Website URL(s)	*Supplier URL*								
8	GNRL-03	Dun & Bradstreet Number	*Dun & Bradstreet Number*								
9	GNRL-04	Annual Gross Revenue	*Annual Gross Revenue*								
10	GNRL-05	Number of Employees	*Number of Employees*								
11	GNRL-06	Number of Contractors	*Number of Contractors*								
12	GNRL-07	Product/Service Name	*Product Name and Version Information, or Service Name*								
13	GNRL-08	Product/Service Description	*Brief Description of the Product/Service*								
14	GNRL-09	Web Link to Product Privacy Notice	*http://www.supplier.domain/privacynotice*								
15	GNRL-10	Supplier Corporate Headquarters Location	*City & Country*								
16	GNRL-11	Additional Countries with Supplier Presence	*Additional Locations Aside from Corporate Headquarters*								
17	GNRL-12	Number of contractors the organization employs in countries other than the United States or Canada (indicate if none)	*Number of Contractors In Countries Other than the United States or Canada*								
18	GNRL-14	Supplier Subsidiaries	*List Any Supplier Subsidiaries*								
19	GNRL-15	Supplier Parent(s)	*Supplier Parent(s)*								
20	GNRL-16	Supplier Parent(s) Subsidiaries and Divisions	*Supplier Parent(s) Subsidiaries and Divisions*								
21	GNRL-17	Supplier Contact Name	*Supplier Contact Name*								
22	GNRL-18	Supplier Contact Title	*Supplier Contact Title*								
23	GNRL-19	Supplier Contact Email	*Supplier Contact E-mail Address*								

Confidentiality | Change Log | Questions

applicable. Assessing and ranking the cybersecurity risk of a third-party product or service drives both the application of security controls and the evaluation of vendors.

Organizations can align the criteria for vendor risk assessments to the risk tier associated with the potential use case. For vendors processing or accessing less sensitive data for relatively trivial tasks, self-certification (e.g., a signed document) attesting that the vendor has the requested cybersecurity controls in place, may suffice. That said, the purchasing organizations should reserve the right to audit. In cases where a vendor is accessing more confidential data or performing larger, more important tasks, the purchasing organization may find it more appropriate to delineate a set of functional criteria or have a third-party assessor evaluate the vendor to determine if the level of control is appropriate for the risk tier. Vendors accessing critical and proprietary data such as intellectual property face the highest level of scrutiny in evaluations such as full sets of detailed questionnaires and validating specifications and features with vendor architects and engineers.

The final risk management strategy prior to deployment is in the contractual terms and conditions.[6] The terms and conditions set the expectations for the business relationship. An example of this is defining the process and timeline of security notifications if the vendor has a security breach. Delays in notification from the vendor increase exposure and delay any internal processes to manage such security breaches.

Risk Mitigations in Practice

Supply chain cybersecurity risk management is not only an external process to ensure that vendors implement and provide appropriate cyber risk mitigation tactics, but also an internal process as well. Mitigating risk is a company-wide effort requiring solution validation from all corners of an organization. From an architectural perspective, it is important to make sure that the appropriate architectures exist within the organization so that the product or service works as intended and is secured appropriately. From a privacy perspective, it is important to make sure that the correct datasets are included and protected. From a cybersecurity perspective, it is important to make sure that the required controls are both present in the product during procurement and fully functional and operational during deployment.

Organizations typically employ Service Level Agreements (SLAs) in the procurement process; however, organizations must have their own internal mitigation measures in place in case a vendor does not meet the expectations defined in the SLA. Internal mitigation methods include architectural and process controls that mitigate risk and secure data, network segmentation to isolate and protect critical infrastructure, and active anomaly detection and monitoring to detect an incident before receiving a vendor security breach notification.

Furthermore, no vendor is perfect, and security events are always a concern. If the terms and conditions of an SLA have no consequences, the organization has no power or influence over the vendor, and the vendor has no impetus to improve performance. That said, building a trusted relationship with vendors can deliver benefits beyond following the minimum terms of the SLA. When organizations have a healthy relationship with vendors, there is a higher chance that the vendor is willing to collaborate and make requested changes to meet needs that lie outside of the SLA.

Supply chain cybersecurity risk management is a continuous process. Vendor assessments and evaluations must be continually performed and documented, such as evaluating their performance and

[6] See for example, Edison Electric Institute (EEI) Model Procurement Contract Language Addressing Cybersecurity Supply Chain Risk. Version 3.0 (October 2022)

level of support offered, among others. If a vendor or solution does not meet an organization's needs, the organization needs to be able to pivot and identify alternatives.

Additional Resources

- NATF Documents
- NATF Energy Sector Supply Chain Risk Questionnaire (xlsx)
- NATF Supply Chain Risk Management Guidance (pdf)
- NATF Supply Chain Security Criteria (xlsx)
- EEI, Model Procurement Contract Language Addressing Cybersecurity Supply Chain Risk, Version 3.0, October 2022

Photo Credit: USAID Energy/Flickr

Asset Management

Best Practices for Secure Remote Access and Cloud Security in the Electricity Sector

Presenter:

- **Justin Searle**, Director of ICS Security, InGuardians

Remote access has become a requirement for many organizations, including electric utilities. In addition, cloud services have been used more and more for certain applications. This webinar presented best practices for secure remote access (e.g., by equipment suppliers for monitoring and maintenance) as well as the considerations needed to implement cloud services. This webinar delved into how utilities are using remote access and cloud services, what are the risks, what is the software lifecycle (e.g., challenges of onboarding and offboarding cloud-based services), how to do it securely now and in the future, and how to deal with changes on the supplier side. Webinar Recording

Defensible Architecture and Asset Management for Electric Utility Cybersecurity

Presenters:

- **Markus Mueller**, Principal Industrial Consultant, Dragos
- **Jason Shea**, Senior Cybersecurity Manager, Southern California Edison

Shifting to a defensible architecture model allows utilities to use an intelligence-based approach to protect their assets from the risks that cyber threats present today. A defensible architecture is not a static design but a process of deploying people, processes, and technology that any utility can follow for more effective asset protection. This practice includes asset management efforts to understand what needs to be protected and what capabilities exist within the environment. The webinar covered best practices for utilities when developing defensible architecture and conducting asset management,

addressed the difference between planning for security during new deployment versus reviewing and improving existing ICT networks, network and access control, network configuration, onboarding, and offboarding third-party suppliers for on-premises software/hardware. Webinar Recording

Best Practices for Secure Remote Access and Cloud Security in the Electricity Sector

Presenter
Justin Searle InGuardians Webinar Recording Presentation Slides

Remote access—being able to access critical control systems from outside the physical facility, from an external network—has become an essential business requirement for many organizations. But remote access brings significant cybersecurity risks just as it makes operations more flexible. A popular, recent resource from the SANS Institute, "The Five ICS Cybersecurity Critical Controls," identifies "Secure Remote Access" and "Defensible Architecture" as two of the five critical controls. Moreover, a "Defensible Architecture" is a prerequisite for the "Secure Remote Access" control, as shown in Figure 4 below. These two critical controls stand out as paramount to provide secure remote access and cloud security, which are necessary capabilities to mitigate supply chain cybersecurity risks.

A Defensible Architecture

Network security organization is enhanced by structuring networks into defined security zones. The Purdue Model[7] is a linguistic tool commonly used to talk about the delineation between security zones, rather than to guide which security checks and balances to put in place. Each level in the Purdue model has different components, services, and functions, and a single level can contain multiple subnets. Security zones typically represent a grouping of networked assets that serve a single service or function. These security zones become the defensible areas, where security administrators can apply monitoring and controls to track and/or limit traffic or users.

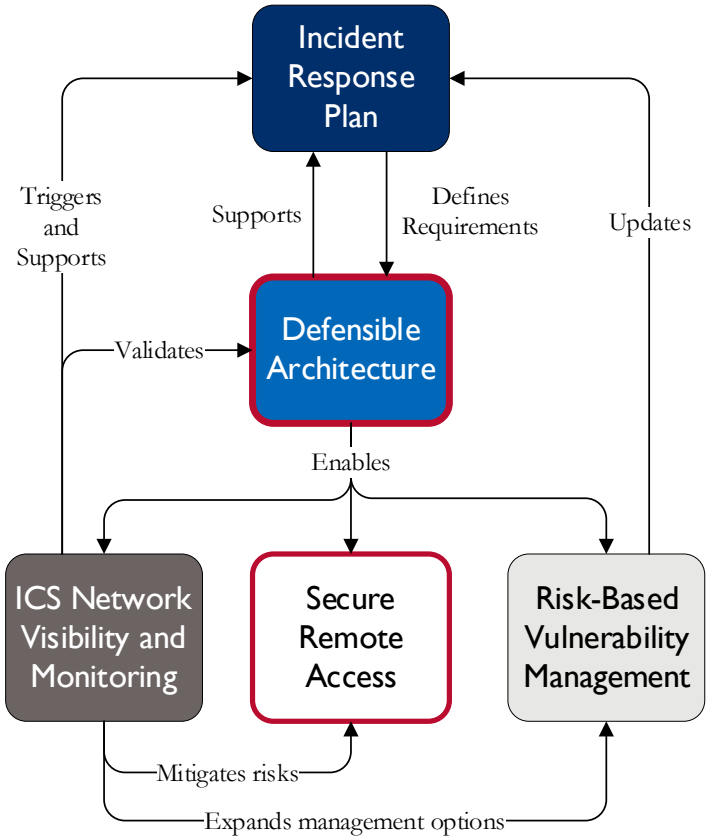


Figure 4. Adapted from "The Five ICS Cybersecurity Critical Controls"

An enforcement boundary naturally fits not only between Purdue levels but also between components, services, and functions in separate zones within a Purdue level, enabled by this segmentation into security zones. Firewalls, intrusion detection systems, and other network monitoring solutions are typical technology controls placed in the boundary, depending on budgets, risk levels, and other considerations.

One of the most important aspects of a defensible architecture is defining the demarcation between IT and OT systems (typically, between Purdue levels 4 and 3). This demarcation acts as the primary line of defense (i.e., the primary enforcement boundary) for the OT space. OT systems are heavily dependent on network

[7] Officially, the Purdue Enterprise Reference Architecture (PERA), but frequently referred to as the Purdue Model.

defenses, external to what can be installed onto an OT device. Assets should be placed in either the IT or the OT environment, but not both nor on a dividing line. The placement is determined by considering whether the asset could have an impact on the OT processes. If there could be any potential disturbance in the OT process by an asset, it should be placed in the OT side of that demarcation.

Once the IT/OT boundary has been created and established, the next step is limiting what is allowed to come into the OT area. Using the Purdue model, as shown above, levels 4 and 5 are the business and enterprise networks, respectively. These are considered part of the IT environment and distinct from the OT environment, which comprises levels 0 – 3.

General cybersecurity guidelines dictate that no assets in level 3 or lower should have direct internet access. That is, internet and email should not go deeper than Level 4. In the OT environment, Active Directory (AD) may be useful for managing accounts and access to OT components, but this AD should be separate and distinct from the Enterprise AD used in the IT environment. Shared credentials between an Enterprise AD and an OT environment AD creates substantial risk that compromised credentials could be used to target operations.

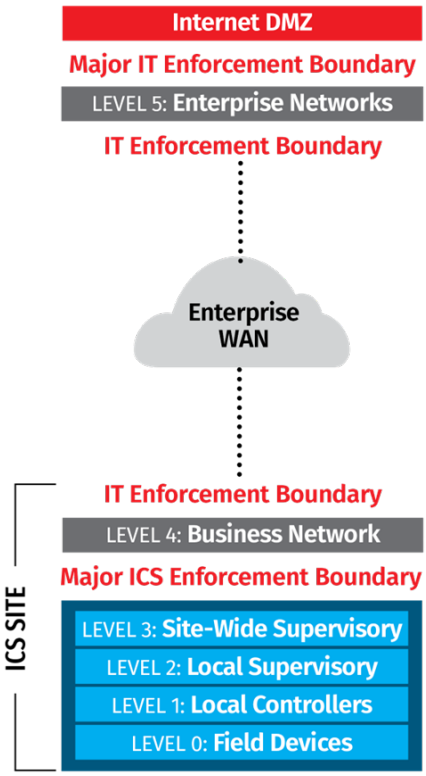


Figure 5. Focus on enforcement boundaries between Levels 5 and 4. (Justin Searle)

Another important aspect of this demarcation point is the inclusion of a demilitarized zone (DMZ) as part of a strong perimeter for the OT environment. The DMZ will include assets like servers that can facilitate the exchange of information between the IT and OT environments. This allows organizations to ensure the traffic between IT and OT environments can be inspected before transfer.

Small sites may use a single ICS DMZ, but larger sites with a complex amount of IT/OT traffic may scale or expand the number of DMZs to separate traffic and mitigate risk. Each of these DMZs can be segmented at this level such that if one of the servers or data transferring assets is compromised, the ability for the attacker to move laterally is harshly limited. Security services and patch managers should not be at this DMZ level, but rather in Purdue level 3.

One common example of multiple DMZ occurs with separate DMZs for the "northbound" and "southbound" network traffic. That is, assets in level 4/5 push data and information to the "southbound" DMZ and assets in Level 3 pull from it. Similarly, assets in Level 3 push data and information into the "northbound" DMZ and assets in Level 4/5 pull from there. In addition to IT/OT ICS traffic DMZs, there may also be DMZs for cloud access and remote access, further separating traffic and mitigating risk.

A common security mistake is sharing management solutions across both IT and OT across the boundary. For example, shared AD exposes OT credentials to attacks on Enterprise AD. Compromised Enterprise AD would then allow an attacker to completely bypass the IT/OT boundary. Shared network and virtualization management leads to IT/OT perimeter bypasses as well. Organizations should separate all management solutions between IT/OT, such as separate AD with no trust relationships and managing OT networks, virtualization, backups, patching, and endpoint detection and response (EDR) from within

the OT environment, keeping all IT and OT tools separate entirely. It is possible to use the same solution within both IT and OT; however, different management servers should be used. This setup allows for bulk licensing and shared knowledge between the IT and OT teams. Moreover, it reduces the number of communication streams between the IT and OT environments that must be managed.

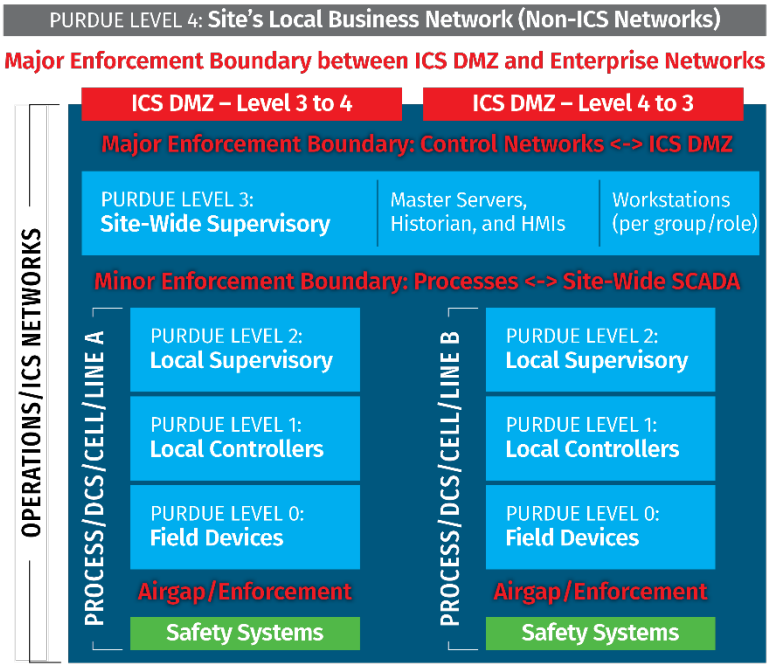


Figure 6. Focus on enforcement boundaries between Levels 4 and 3 and Levels 3 and 2. (Justin Searle)

Software Defined Networking (SDN) is becoming more common and is frequently found on wide area networks (WANs) to manage the network communication pathways. Different SDN solutions will have different capabilities, so care should be taken to understand the fit for purpose. For example, some SDN solutions may look like a management solution, in which case the earlier discussion on separating management solutions for IT and OT environments applies. If a single SDN solution has capabilities to manage assets within IT and OT at once, this could be a tool to upend protections that separate the IT and OT networks and offer a path for an attacker to reach operations.

The biggest limitation to modern end-point security or EDR solutions is where they can be installed in the OT environment. Assets that can run EDR solutions are typically in Purdue Level 3, because many of them are Windows and Linux servers. It is less common that devices in lower levels, closer to the operations, can support EDR. But in the context of security with a defensible architecture, an attacker will have to gain access to Level 3 devices first making them an ideal place for EDR. Many modern EDR solutions are cloud-backed to conduct deeper investigation of data, so organizations will likely have to determine whether the trade-off for more capabilities for a little bit more risk is worthwhile.

Enforcement boundaries should also exist between Purdue Level 3 and the subprocesses in levels 2, 1 and 0, as shown in Figure 6. Internal enforcement boundaries within the OT environment are critical to reduce the attack surface and prevent pivoting from one process to another, or even to the supervisory level. Safety systems and communication should be isolated from the rest of the ICS network.

Secure Remote Access

Remote access into the OT environment will come from Level 4/5 or direct from the internet. It is recommended to have two separate steps for including remote access into an OT environment because having a single step remote access solution would create a single point of failure. The first step in the two-step remote access solution is reaching the ICS DMZ. This connection should leverage a VPN or a Zero Trust Architecture (ZTA) remote access solution. There should be mandatory two-factor authentication. This first step of remote access can use either a separate, standalone authentication specifically for remote access or in some cases using Enterprise AD. Using a combination of separate, standalone authentication for contractors or consultants and Enterprise AD for internal users is also

possible, but this is dependent on the organization. Many ZTA solutions allow the user to connect to AD, but it is up to the organization whether to do so. If you do make this connection, use the Enterprise AD rather than an OT AD.

> "Defensible architectures and remote access have to go together"
>
> – Justin Searle, InGuardians

The second step to remote access is then from the ICS DMZ to individual assets or a jump host in Level 3. This step acts as a second level of authentication to add security. This jump host should use the OT AD authentication method that is separate from the Enterprise AD, as discussed above. This step allows two separate sets of credentials and two layers of control. It also allows for fine control over access to specific assets. The first step lets the user access the perimeter of the ICS environment, but the second step can limit access to specific assets within the ICS environment.

Additional controls can bolster this 2-step process to support detection and response and recover capabilities. For example, organizations should record the remote access session in either step 1 or step 2 so that the security team can identify what the remote access user is doing. Creating a record of the session can be done in either step 1 or in step 2, but generally not in both. Organizations should also prevent remote access users from bringing in data unless they absolutely need to. There are exceptions, such as vendors bringing in a patch, but these exceptions depend on a case-by-case basis, so it must be explicitly stated who can bring in what. If a remote access user is bringing in any type of file or data, it is strongly recommended that these files or data are uploaded to a separate file server in an ICS DMZ or ZTA that can scan the file for vulnerabilities, as well as store the file, store the hash of the file, and keep a record of who brought it into the environment. After the checks are done on the file or data, it can then be facilitated through the DMZ to the appropriate location.

Cloud Connectivity

Cloud connectivity should be considered very carefully. While it can add huge business and operational benefits, it also adds risk. Cloud connectivity should be treated like traditional vendor remote access, but with 24/7 access. The risks are quite similar between vendor remote access and cloud services, and in both cases, the security risk team should carefully consider them to determine if the benefits outweigh the risks and what appropriate measures should be taken to mitigate risks.

One example of a risk that utilities should consider is geopolitics. Organizations should ensure the cloud provider's servers are not located in an "adversarial" country, which could come with additional risks. Another consideration for cloud solutions is the robustness of the solution. Solutions hosted by the three big vendors (Google, Amazon, and Microsoft) tend to be secure and robust, while other vendors may require additional scrutiny.

There are several best practices for risk mitigations in these scenarios. Organizations should use cloud services that support transport layer security (TLS) protected protocols or VPNs to protect data in transit so that all the data going to and from the cloud service will be encrypted. In general, firewalls on the perimeter of the ICS environment should have rules that are as specific as possible, specifying which machines from the cloud and which assets in the ICS environment are allowed to communicate via the DMZ; firewall rules should use internet protocol (IP) addresses, if possible, hostnames if not. Similarly, firewall rules should be highly specific in both directions—to and from the cloud.

Finally, all traffic should move through a DMZ specifically for this cloud connectivity. This traffic could flow through either a server that brokers traffic between cloud and ICS assets (some cloud services may

supply just such an asset to install in the DMZ) or a web proxy with allowlists between specific systems and services. In either case, the solutions should support logging.

There may be cases where devices or agents internally need to communicate directly with the cloud. This case carries a little more risk, which may be mitigated by further limiting what locations those assets can communicate with (e.g., limit by IP address if possible, or hostnames if not). Organizations may also choose to build security perimeters around these internal assets as well to block pivoting and to address the scenario that the cloud service has been compromised.

One emerging use case for cloud services supporting the OT environment is to manage back-up for the OT environment. Like with other shared services, administrators for the OT environment should ensure that IT and OT environments use separate instances of that management solution. Cloud backup could be an acceptable solution if the organization has done their due diligence that it will be feasible. One consideration that may be pertinent to electric utilities is to ensure that the backup does not saturate network traffic such that SCADA communications could be affected.

Conclusion

For electric utilities, many innovations—including DER, microgrids, smart cities, electric vehicles, and others—rely more heavily on communications between systems than legacy systems and could look more like remote access or cloud systems in terms of communication requirements. Electric sector organizations that have shied away from remote access may be forced into it through these new technologies. Moreover, the vendors of these new technologies may be requiring remote access more and more, so organizations should build perimeters around those assets.

Creating a defensible perimeter between IT and OT is paramount to enable remote access and cloud connectivity to ICS systems. Without this defensible perimeter, an attacker could leverage remote access to pivot from the IT network to the OT network and would therefore immediately be one step closer to potential impacts on operations. Enforcement boundaries within the OT environment between assets or systems bolster defense, especially for critical assets. Without these enforcement boundaries, an attacker could leverage remote access to a low value asset in the OT environment to pivot to a critical asset.

Similarly, if cloud connectivity is being utilized in one asset or process, this asset or process needs to be isolated from other assets and processes to limit and block pivoting, thus reducing attack surfaces. The key to remote access and cloud connectivity is having a defensible and secure network architecture.

Actions Toward Defensible Architecture and Secure Remote Access

Defensible architecture

- ✓ Segmentation between IT and OT (Purdue Levels 5 and 4)
- ✓ One or more DMZs as appropriate to separate traffic between IT and OT (within Level 4)
- ✓ Separate all processes (in Level 2) from the site-wide supervisory (Level 3)
- ✓ Segmentation between processes within OT environments
- ✓ Separate management services (e.g., AD) for IT and OT

Secure Remote Access / Cloud Access

- ✓ Separate DMZs for remote access and cloud access as appropriate
- ✓ 2-step authentication for humans

Additional Resources

- ➢ SANS, The Five ICS Cybersecurity Critical Controls (November 2022)

- ISA/IEC 62443 Standards – Security of Industrial Automation and Control Systems
- Williams, T. J. "The Purdue Enterprise Reference Architecture." IFAC Proceedings Volumes, 12th Triennial World Congress of the International Federation of Automatic control. Volume 4 Applications II, Sydney, Australia, 18-23 July, 26, no. 2, Part 4 (July 1, 1993): 559–64. https://doi.org/10.1016/S1474-6670(17)48532-6.

Defensible Architecture and Asset Management for Electric Utility Cybersecurity

Presenters

Markus Mueller
Dragos

Jason Shea
Southern California Edison

Webinar Recording

Presentation Slides

Utilities frequently rely on reference architectures when attempting to build a defensible network as part of a robust cybersecurity program. Some examples of the best practices that typically follow from these references include:

- Define and segment the layers
- Defense at each layer
- Traffic inspection and filtering between layers
- Encrypt critical data
- Deploy security solution on the network and endpoints
- Zero Trust

While utilities can be quite successful with these reference architectures and best practices, an intelligence driven approach—figuring out the problems you have, and then addressing those problems—can guide utilities to maintain a strong cybersecurity program even as the business grows and changes. It can also help guide utilities to make smarter investments that yield real risk reduction.

In the context of OT systems, intelligence-driven defensible architecture is based on five considerations:

1. **Process understanding:** Process understanding involves identifying and understanding the critical systems, learning how they operate, and what happens when they fail. The Crown Jewel Analysis is an approach to help organizations with this process of figuring out which assets are the most critical and their possible attack vectors.
2. **Threat scenarios**: Organizations need to determine what threats exist and the threat scenarios that are likely to impact their environment; threats and threat scenarios can vary based on size, location, and purpose of the organization.
3. **Operational constraints:** Operational constraints help determine what defensive actions and architecture can be designed and implemented to maintain operations without hindrance.
4. **Business constraints:** Like operational constraints, business constraints help determine the policies and processes that are available to build a robust cybersecurity program.
5. **Capabilities:** For a deployed strategy to be effective, the organization must have the capabilities available to digest and respond to the data provided by the defense mechanism.

The remainder of this section looks at a fictitious water utility, ACME Co, to help illustrate the above process in practice at varying operational scales.

Small Utility

ACME is a relatively small water utility serving 6,000 customers. They have seven wells, two large water tanks, four small water tanks, one treatment plant, and two lift stations. For business systems, they use cloud-based software (e.g., Microsoft 365 or a cloud-based customer information system), and for OT systems, they use Rockwell programmable logic controllers (PLCs), Ignition, and a Badger Meter system.

In this fabricated example, an ACME employee fell prey to a phishing email, resulting in downloaded malware. The malware infected a handful of computers and two OT systems: the metering system and the employee workstation. ACME lost revenue due to being unable to bill customers, and the company

lost programming and files due to poorly maintained backups. This incident acted as a catalyst for ACME to implement intelligence-driven defense.

ACME started by reexamining their processes. A Crown Jewel Analysis identified that Well 1, Tank 1, and the singular water treatment plant were most critical to operations and meeting demand. As ACME is not a large target, nor one of exceptional importance, they determined that the most likely threat scenario to defend against is opportunistic ransomware. However, limited staff, a limited budget, and infrequent production outages constrained their response. With these considerations in mind, ACME implemented several new defense measures.

Resource constraints meant ACME could not implement a separate domain network for their OT infrastructure, so they used a shared infrastructure model. Using only the one firewall, ACME segmented the network with different firewall rules and different zones on the firewall for the IT and OT networks. They also established an OT DMZ to monitor and control data movement between the IT and OT systems and focused on making sure data moved through the DMZ. Figure 7 below models this hypothetical segmentation scenario.

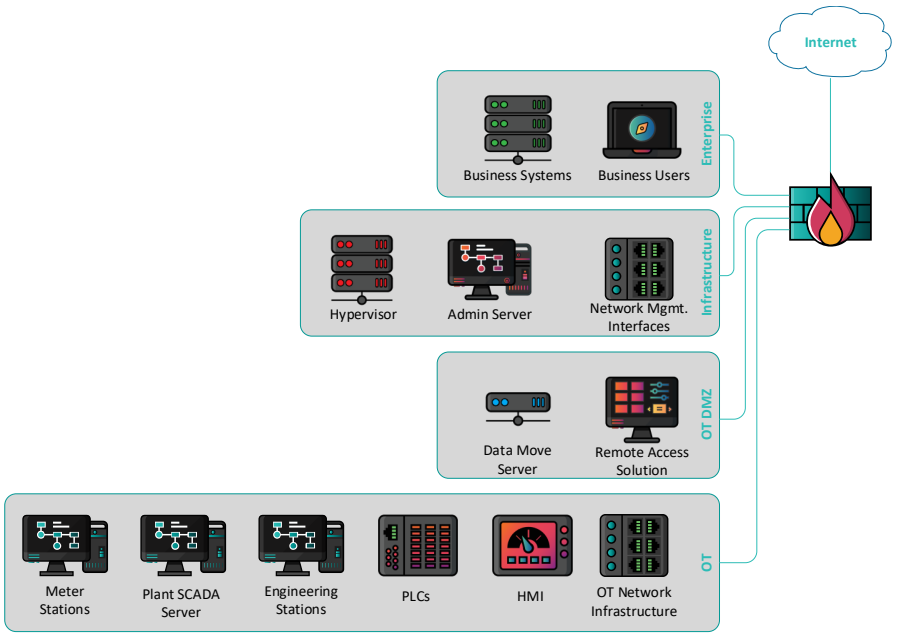


Figure 7. ACME Network Segmentation

In addition to network segmentation, ACME rolled out new security controls, including partnering with engineers and operators to create and maintain an asset inventory and hardening system security with a password vault and role-based user access with a few defined roles (Admin, Operator, and Read Only). With the ransomware threat in mind, they focused on backups and deployed a system to manage PLCs and maintain their backups, and they expanded backup solutions for OT with a local network attached storage (NAS) and offline removeable disks. With shared infrastructure, ACME recognized the potential for an attacker to pivot from IT to OT too easily, so they required multi-factor authentication (MFA) on remote and admin accounts. Although these defense mechanisms enhance overall security at ACME, they do not inherently enable a defensible architecture.

To be defensible, ACME developed policies and processes to complement these technology defense measures. As such, they created security use cases and began centralized logging of events on a security

incident and event management (SIEM) system. Rather than creating alerts for every possible concerning event in the logs, they focused on events to which they knew they could and would respond. They built playbooks to define the actions they would take in a ransomware incident such as IT/OT disconnection and OT restoration during an event. They joined intelligence networks like the WaterISAC and cross-trained their IT and OT employees to better equip and prepare them for future events. Incident response tabletop exercises and restoration tests highlighted some gaps, which ACME addressed to validate their newly implemented intelligence-driven defense architecture.

Medium Utility

ACME has acquired an electric utility that serves a similar customer base and scaled up to a medium utility. As a medium-sized water and electric utility, ACME's infrastructure and technology stack has grown to include additional infrastructure and new IT and OT systems, namely a new water SCADA system and an electric distribution management system (DMS). ACME repeated the Crown Jewel Analysis and found that the SCADA system and DMS were their most critical systems. Having expanded in size as a utility, ACME may now be a larger target, thus increasing their threat scenarios to not only opportunistic ransomware but also targeted ransomware and hacktivism. Their constraints remain the same: limited budget, limited staff, and infrequent production outages.

In response to growing threats, ACME bolstered their network segmentation with dedicated OT infrastructure and internal segmentation by function/process, grouping together components that supported the same process. This strategy also helps address vulnerabilities in legacy systems that may not have modern security capabilities by putting defenses close to the systems. Similarly, it helps to

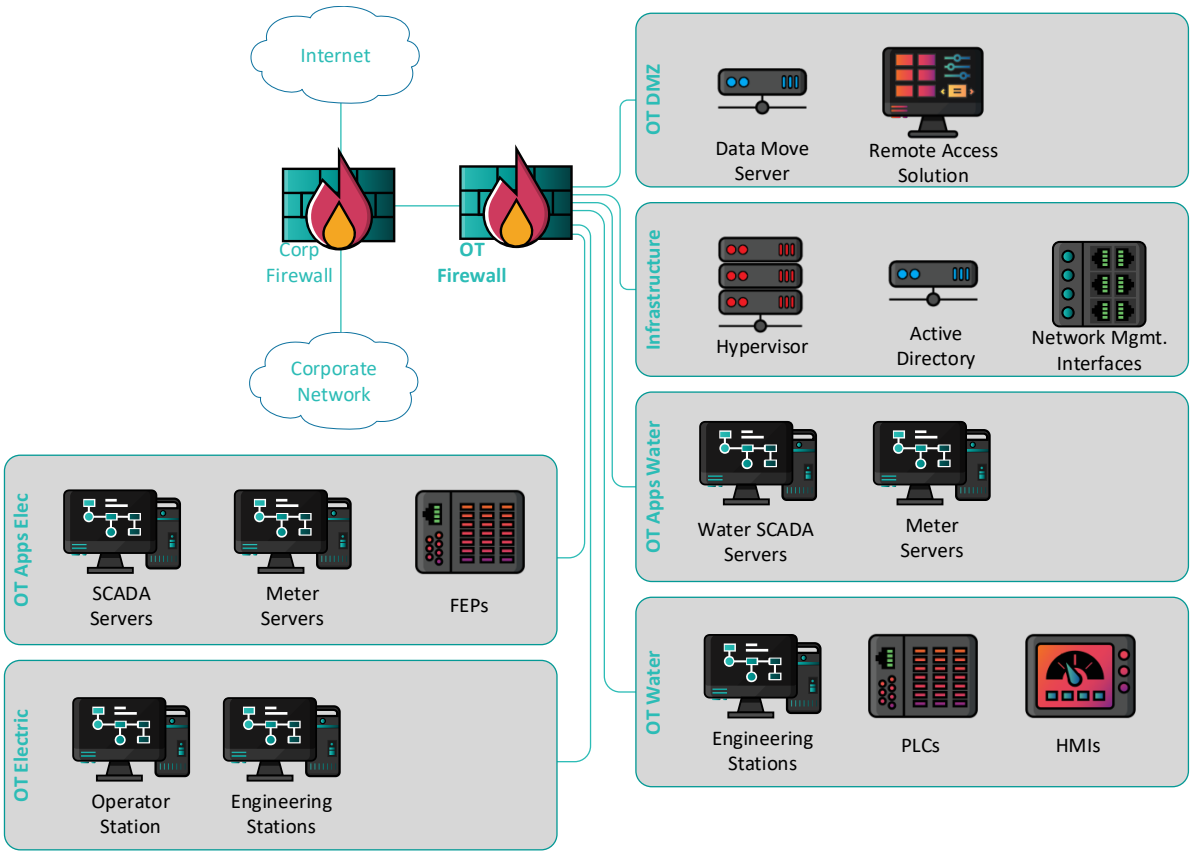


Figure 8. Increased ACME Network Segmentation (Water and Electric)

isolate vendor devices that may not be trusted by enabling the utility to segment that device and the traffic to and from it. In general, ACME restricted data flow to the one up/one down model—data flows that traverse security zones only flow one zone higher or one zone lower. Figure 8 depicts this level of segmentation.

ACME also reviewed their field area network (FAN) and made plans to address identified threats. As a small utility, ACME was able to use public communication infrastructure without worry. However, intel indicated that hacktivists in the geopolitical space were targeting publicly available IP addresses. They moved to private communication paths like private cellular, deployed some of their own network, and stopped using public infrastructure (i.e., with public IP addresses) as shown in Figure 9.

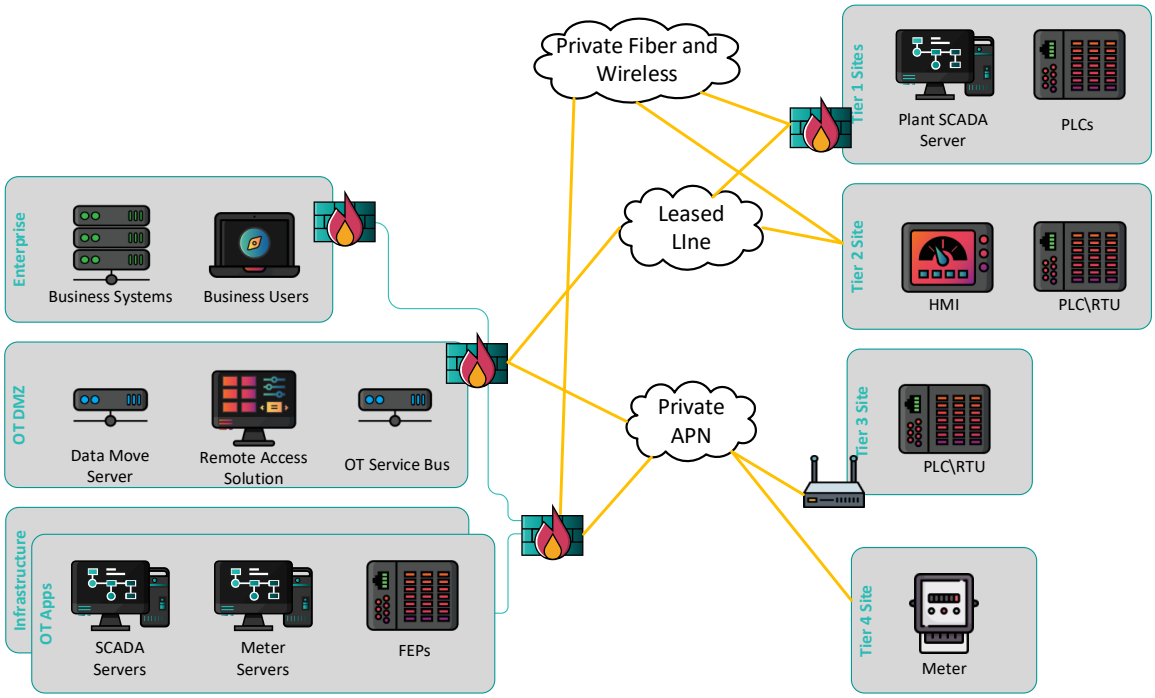


Figure 9. ACME Field Area Network

ACME also strengthened their identity management practices while trying to limit the number of passwords each user must use. They maintained segmentation between IT and OT, so users typically had an identity for the enterprise networks (managed with Azure AD), a method for remote access, and access credentials to assets in the production environment. They further hardened the system by implementing application whitelisting/allowlisting, EDR, and a privileged access management (PAM) solution. They continued to focus on recovery and augmented their backup strategy with local/site-to-site replication and offline-to-tape solutions to ensure that if there was an attack, they could recover quickly and completely.

With changes in defense mechanisms also came changes in actions and capabilities to maintain defensibility. ACME increased ICS network visibility with an industrial visibility platform in their Control Center. They conducted hunts into their own environment to actively look for signs of malicious activity based on industry intel, and they developed more use cases and playbooks, such as how to respond to compromised credentials or a compromised system and how to perform forensic triage. ACME expanded its intelligence network by joining the Electricity Information Security and Analysis Center (E-ISAC) and elevated their security operations center (SOC) by hiring a managed security service provider

(MSSP). ACME continued to run tabletop exercises and site recovery drills. They even made site recovery a part of the commissioning process for new equipment. Engineering and security would collaborate to ensure that recovery processes were functioning.

Large Utility

In a final example, ACME expanded operation by adding utility scale solar and wind generation, a large battery energy storage system (BESS), and allowing customers to install solar and BESS behind the meter, particularly solar and wind. To manage these new systems and requirements, ACME deployed an advanced distribution management system (ADMS), AMI metering, and their own cellular network in some locations. The Crown Jewel Analysis identified the ADMS and water SCADA system as most indispensable. Ransomware remained a threat, but they also worried about advanced persistent threats (APTs) that might be targeting electric utilities. Given ACME's larger size, they now face heightened levels of scrutiny and oversight from regulators, further constraining operations.

To adapt to their changing environment, ACME maximized network segmentation. They thought about site and path resilience and deploying technologies like software defined networking (SDN) in an SD-WAN (software-defined wide area network) to enable multipath communication to primary and backup sites. They implemented micro segmentation and containers to expand asset protection. Figure 10 below depicts their new level of network segmentation.

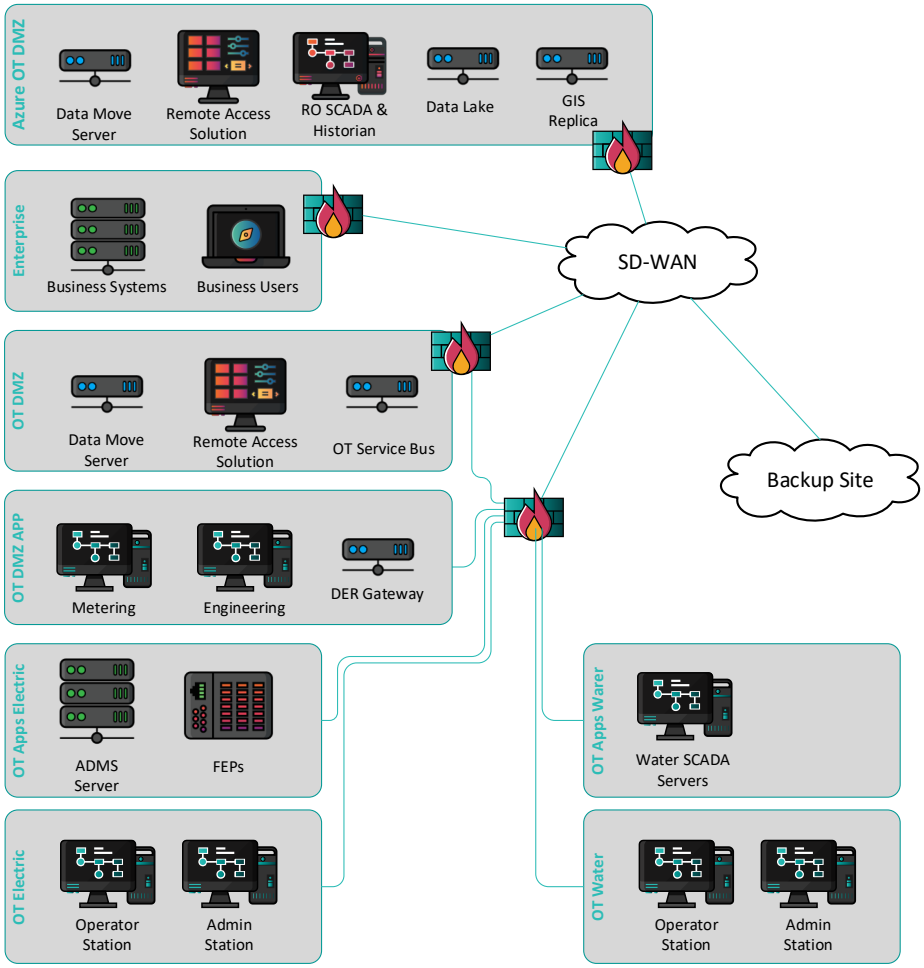


Figure 10. ACME Network Segmentation (Water, Electric, and Generation)

With distributed energy systems and behind-the-meter generation like customer-sited solar, ACME knew they were not going to be able to control both sides of the connection for grid-connected devices. This required security enhancements to their FAN and shifting to an SD-WAN model where all endpoints had access rules, and traffic was controlled across their network. Figure 11 models this new field area network.

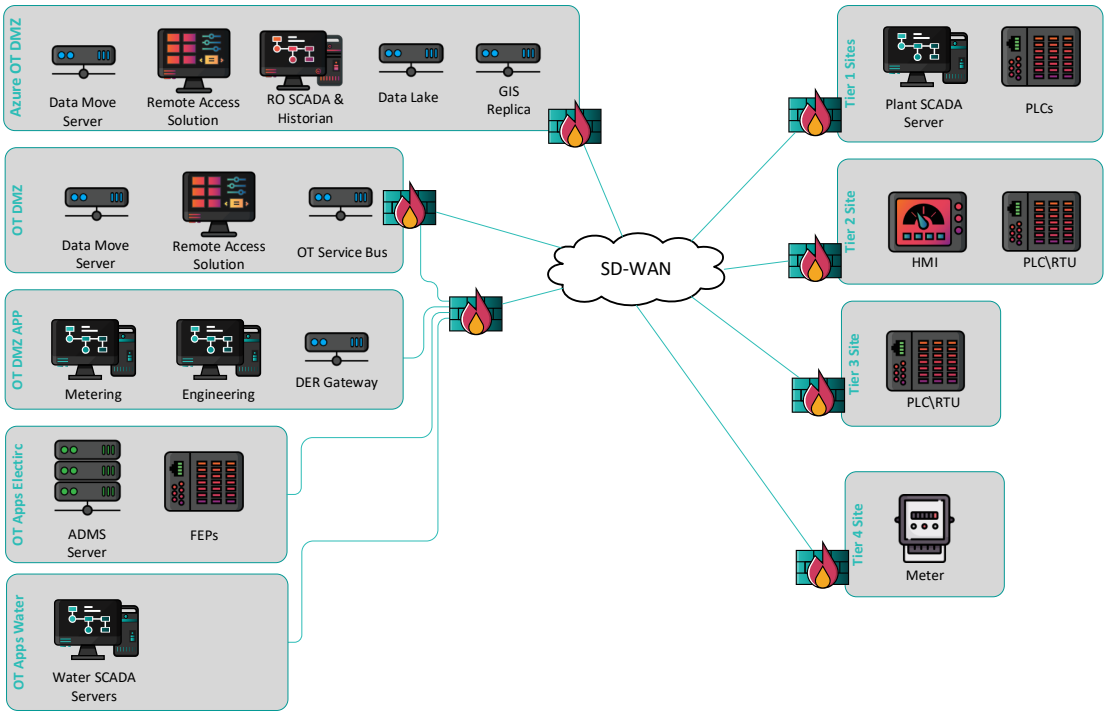


Figure 11. ACME Field Area Network (Water, Electric, and Generation)

ACME further enhanced their identity management capabilities to increase usability given the additional personnel. They sought to make access to read-only accounts in the OT DMZ a little easier by implementing an Azure AD for the OT DMZ which connected to the distinct Enterprise Azure AD via Azure's B2B settings. They kept the separate credentials for OT assets but made the management more flexible so they could more tightly control who had access to what equipment.

ACME reviewed and enhanced most of their security controls as part of scaling up their defensible architecture. They codified an asset management and a change management program, started baseline tracking, and implemented a risk-based vulnerability management program to prioritize and optimize security actions. ACME did not let these enhancements detract from their continued focus on maintaining backup solutions that enable them to withstand a security event, including local/cloud replication, immutable cloud storage, and standby systems.

Just as before, ACME's architecture defensibility is enabled by their monitoring and response capabilities. As such, ACME expanded visibility within the ICS network and added more logging—both OT system logging and ICS device logging—and created more specific and niche playbooks, like insider threats and defensible cyber stance to instruct operation during an attack. Having more experience and knowledge under their belt, ACME began contributing to information sharing groups rather than solely receiving intel. Their workforce advanced and was able to create an in-house L2+ SOC and dedicate responders to security events. Lastly, to prepare for a catastrophic event, ACME rounded out their tabletop

exercises and recovery drills by running tabletop exercises that included the executives and leadership and developing and practicing a system-wide recovery drill.

Lessons Learned

As seen in each of the three scenarios above, ACME followed the same steps each time. They looked at and understood their industrial processes, identified threats faced and constraints imposed, and developed capabilities that enabled a defensible architecture. Intelligence-driven defensible architecture is a deceivingly complex process. It requires intimate knowledge of how operations and the business function to design an intelligence-driven strategy that fits the environment. However, a strategy is only as successful as its weakest link.

Deployed technologies and processes must support event detection and response, in addition to being robust, to protect critical assets from a spectrum of threats. Although working towards a zero-breach architecture might be ideal, it is not realistic, and utilities need to focus on establishing procedures that define how to maintain operations during an attack and how to recover quickly and fully following an attack. Playbooks can be particularly helpful for utilities to document exactly how they will respond (i.e., what actions they will take) to a specific type of event. Some organizations may even decide that preparing redundant equipment (e.g., a pallet of the required assets) to be delivered in response to an event is necessary to stand up a new, clean network to restore operations. Collaboration and community within industry is imperative to help investor-owned utilities, cooperatives, and municipalities alike adapt to the ever-increasing level of grid interconnectedness and vulnerability.

While broad intel to understand likely threats and scenarios (e.g., opportunistic ransomware vs. an APT), is instrumental to strategic decisions around building a defensible architecture, bringing the latest intelligence streams into the cybersecurity program is typical of a mature program and less essential early on. Utilities may see some benefit from spending a small amount of time (e.g., one person-hour per week) reviewing streams to be aware of trends and drive conversations with OT staff to understand potential exposure. For example, the CyberAvengers attacks in the fall of 2023 targeted PLCs made by a specific manufacturer. Companies around the world had these PLCs installed and available on the public internet. Following intel feeds would have alerted a company to double check with their engineering whether they have these PLCs in production environments.

Many organizations have opportunities to target what is coming in the door rather than having to be reactive to what is available for procurement. Organizations can hold vendors accountable for the security of their products by pushing for secure-by-design practices. Additionally, organizations can ask themselves how they will operate without that product or service. Playbooks can document the actions the utility would take if the product or service becomes unavailable.

Additional Resources

- Scott Fitch and Michael Muckin, *Defendable Architectures: Achieving Cybersecurity by Designing for Intelligence Driven Defense* (2019)
- SANS, The Five ICS Cybersecurity Critical Controls (November 2022)
- Dragos, Operational Technology - Cyber Emergency Readiness Team (OT-CERT)
- E-ISAC
- WaterISAC

Photo Credit: USAID Energy/Flickr

Governance, Policies, and Planning

Cybersecurity Incident Response Plan Development

Presenters:

- **Michael Martin**, Control Systems Engineer, Chelan County PUD
- **Tony Assan**, Head of IT, GRIDCo (Ghana)

An incident response plan (IRP) is an essential tool for utilities to prepare for an event and can help drive the utility's overall cybersecurity activities. This webinar discussed how utilities should incorporate supply chain cybersecurity considerations into an IRP. Important steps include identifying scenarios, identifying critical utility systems/assets, identifying supporting systems/assets, calculating business impacts, using existing risk analysis, and developing and testing playbooks. This webinar also discussed key strategies to testing and improving the incident response plan and highlighted several useful resources to developing the IRP. Webinar Recording

Governance Policies and Procedures for Third-Party Cybersecurity Risk Management

Presenters:

- **Terri Khalil**, Senior Consultant, Ampyx Cyber (formerly Ampere Industrial Security)
- **Roland Miller III**, Ambassador for Cyber Florida, The Florida Center for Cybersecurity

This webinar focused on developing and maintaining organizational cybersecurity governance and the best practices on policies and procedures to address supply chain risk management. The webinar highlighted typical models for managing cybersecurity (e.g., the role of a Chief Information Security Officer [CISO] or Chief Security Officer [CSO]) and level of visibility into cybersecurity risks from the senior management to technical staff. The presenters also discussed strategies and approaches to

communicating not only within an organization about cyber risks, but also with regulatory authorities, especially in support of review and approval of capital expenditures (CAPEX) and operating expenses expenditures (OPEX) cyber investments. Webinar Recording

Managing Cybersecurity Risks in a Rapidly Expanding Electric Grid

Presenters:

- **Anuj Sanghvi**, Researcher III-Cyber Security & Resilience, National Renewable Energy Laboratory (NREL)
- **Ginger Wright**, Cyber-Informed Engineering Program Manager, Idaho National Laboratory (INL)

As utilities rapidly expand electric grids and prepare for transitions from centralized to distributed grids and create new interconnections, consideration of cybersecurity requirements is paramount. Transmission system operators, distribution system operators, and market operators must incorporate distributed energy resources into the electric grid and accommodate independent power producers, generally, but this creates new communication and control requirements which must be secure. This webinar addressed considerations for security of integrations between transmission, distribution, and market operations systems through Cyber Informed Engineering (CIE) and applying the Distributed Energy Resources Cybersecurity Frameworks (DERCF). Webinar Recording

Cybersecurity Incident Response Plan Development

Presenters
Michael Martin Chelan County PUD
Tony Assan GRIDCo (Ghana)
Webinar Recording
Presentation Slides

Incident response planning is an essential control for electric utilities given the digitalization of OT systems. Developing an incident response plan is the first control in the SANS Institute's "The Five ICS Cybersecurity Critical Controls," in part because it can help utilities determine what additional controls can deliver the highest value. That is, additional cybersecurity controls should support the capabilities the utility needs to have an effective incident response.

Two case studies below discuss two utilities' approaches to developing incident response plans: Chelan County Public Utility District (Chelan PUD), a generation/transmission/distribution utility in the United States and GRIDCo, the electric transmission grid operator in Ghana.

Case Study: Chelan County Public Utility District

Chelan PUD operates in the northwest United States, managing three hydroelectric dams. These facilities produce a significant amount of electricity (totaling roughly 7.5 million MWh in 2023), and they sell surplus electricity to neighboring utilities. Chelan PUD also provides transmission and distribution services with more than 3,000 km of distribution lines. This backdrop underscores the critical need for a robust cybersecurity posture to protect the utility's OT, as an operational impact could affect many customers and businesses.

Adopting the NIST Cybersecurity Framework

Chelan County PUD began overhauling their incident response plan in 2016 to comply with NERC CIP regulations. This effort was informed by key documents like the NIST Special Publication 800-61 Revision 2, "Computer Security Incident Handling Guide" and the Department of Homeland Security's guide on "Developing an Industrial Control Systems Cyber Security Incident Response Capability." The adoption of the NIST Model was pivotal in this strategic redirection. The NIST Model highlights four interconnected phases: Preparation; Detection and Analysis; Containment, Eradication, & Recovery; and Post-incident Activity, as shown in Figure 12.

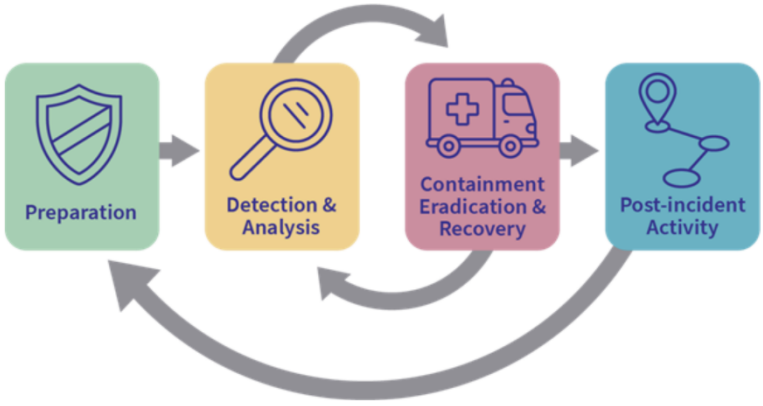


Figure 12. Four-step process to developing incident response capabilities.

Preparation: Identifying Critical Utility Assets

The preparation phase involved applying NERC CIP classification criteria to identify critical assets and applying physical and cybersecurity controls based on their impact assessment. NERC CIP regulations require identifying and classifying critical cyber assets and their supporting systems with either high,

medium, low, or no impact to the greater interconnected power grid. Based on these impact ratings, these systems are then protected by appropriate physical and cybersecurity controls to mitigate their associated risks. Chelan PUD conducts business impact risk assessments to identify additional mitigations like insurance, support agreements, and preventative maintenance to enhance resilience.

Writing Your Incident Response Plan

When developing an incident response plan, the best approach is to get something put on paper. The first draft does not have to be perfect, and a "Crawl, Walk, Run" approach to maturing the plan is effective. That is, utilities should create a basic plan first and improve it over time to the point where it becomes fully fleshed out and functional for all parties involved. Once you have a plan, implementing lessons learned from incident response plan exercises is the most effective method to improve your plan. Chelan PUD's IT department used the American Public Power Association's Public Power Cyber Incident Response Playbook (2019) as a guide to developing their cyber incident response plan.

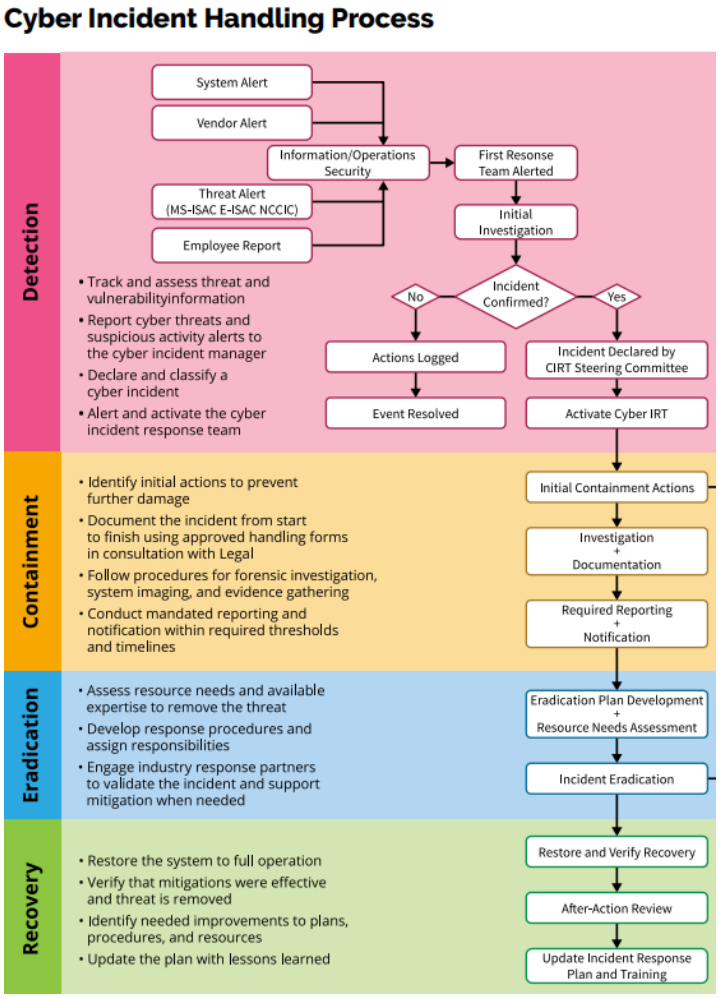


Figure 13. Example cyber incident handling process flowchart (Source: APPA 2019 via Michael Martin)

Cybersecurity Incident Response Plan: Key Elements

A successful Cybersecurity Incident Response Plan should include the following key elements:

- **Roles and Responsibilities**: Clearly defining the roles of all participants in the response process
- **Detection**: Distinguishing incidents from normal events
- **Containment**: Actions to take to prevent further damage
- **Eradication**: Removing the threat
- **Recovery**: Steps to restore the system to full operation
- **Communication Plans:** Documenting communication methods and how communication occurs between departments and to external groups

NERC defines a cybersecurity incident as: "A malicious act or suspicious event that … disrupts or attempts to disrupt the operation of a utility cyber system." To detect a cybersecurity incident, it is important to train system operators and system administrators on what to look for. The NERC "Cyber Intrusion Guide for System Operators" and the NIST SP 800-82 Revision 3, "Guide to Operational

Technology Security" documents list possible incident indicators specific to typical roles and responsibilities. A decision tree or flow chart (see Figure 14) can be helpful. As part of the "detection" capability, utilities should document methods to report suspicious activity as well as procedures to analyze potential incidents and preserve evidence for later review.

> "The goal of an incident response plan is to establish a written systematic approach"
>
> – Michael Martin, Chelan County PUD

Containment and eradication require the utility to act swiftly, so playbooks for likely scenarios can be very useful. Incident response plans should briefly list common incident types (like malware, ransomware, account misuse) and their potential containment actions since these may be overlooked during an incident. An excellent playbook for ransomware is the U.S. Cybersecurity and Infrastructure Security Agency's (CISA's) "Stop Ransomware Guide." References to playbooks like this can be an excellent starting point or reference for an incident response plan.

Recovery may be an extended process and will highlight many opportunities for future improvements. Utilities should document all the steps necessary to restore the system back to full operation. Some essential strategies for recovery include keeping spare hardware for human-machine interfaces (HMIs), computers, PLCs, remote terminal units (RTUs), and network switches in case of supply chain delays. Equipment like this can have a long lead time—for example, Chelan's preferred network switch had a 180-day lead time—so spare inventory may be essential.

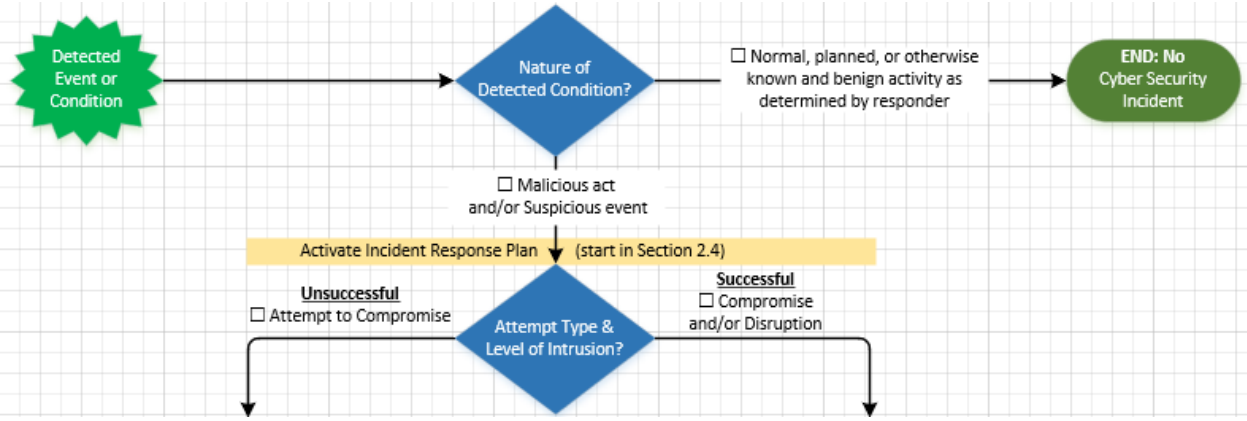


Figure 14. Example decision tree from Chelan PUD's incident response plan. (Source: Michael Martin, Chelan PUD)

Communication plans are often overlooked. Communication methods between coworkers is the most important aspect of incident response recovery. Everyone should know the preferred communication method such as cell phones, Slack, Teams, WhatsApp, Zoom. In addition to having a preferred method, include backup options in case one system is down, including a manual method of communication if there is no telecommunication method available. It is also important how information will be relayed from one response team to another, so that there is a clear point of contact and task delegation system in place. Lastly, in addition to internal communication plans, utilities should include a way to contact external groups such as law enforcement, neighboring utilities, and the general public.

Exercise Your Incident Response Plan

Regular practice through tabletop drills and simulation of recent scenarios is crucial for identifying plan strengths and areas for improvement. Annual exercises are recommended, focusing on real-world scenarios to enhance response readiness. A good way to simulate exercises is to test recent scenarios that occurred in the news to other utilities or organizations. The SolarWinds attack is an excellent example of a supply chain attack that utilities can adapt to their own situations. The Ukraine grid attacks and/or Colonial Pipeline attack as well as an insider threat scenario are also good examples to build from. To improve your plan, ensure that all members of the response teams actually use the plan during the exercise.

After the exercise, conduct a lessons-learned meeting to gather feedback to refine the incident response plan. This process helps identify performance gaps, informational needs, and potential improvements for future response efforts. These exercises are excellent ways to offer training opportunities for responders so that during an actual event, confusion is minimized. For example, Chelan found that their plan was too long, so they made it shorter and more actionable with decision trees and checklists. Similarly, by having the response team stay at their desks rather than gather in a conference room to test their plan, Chelan discovered several new communications challenges not reflected in their communication plan.

Finally, these exercises highlighted ways to improve the utility's cybersecurity and physical security posture. These included application architecture improvements, additional security cameras, penetration tests for specific networks, enhanced event notification (e.g., after-hours alerts), and additional tools deployed (e.g., network monitoring solutions to support operational troubleshooting and forensic analysis).

Case Study: Ghana GRIDCo

GRIDCo operates Ghana's transmission system, servicing 32 bulk customers and 10 generating companies, including independent power producers, with a significant installed generation capacity from hydro, thermal, and solar plans as well as more than 6,000 km of transmission infrastructure. GRIDCo separates IT and OT infrastructures, emphasizing the importance of robust cybersecurity practices to mitigate the potential financial and operational impacts of outages. GRIDCo's transmission infrastructure is interconnected with neighboring countries, Côte D'Ivoire, Burkina Faso, Togo, and Benin, which significantly extends the potential impact of an outage, including financial losses in the millions of US dollars per day, impacts to national gross domestic product (GDP), and sub-regional security and stability.

> "Supply chain has become one of the most challenging vulnerabilities to address"
>
> – Tony Assan, GRIDCo

OT Security and Incident Management Considerations

GRIDCo identified a compelling basis for developing an incident response plan for OT, with additional focus on the supply chain for OT. First, they recognized that threat actors could target any part of an OT system's lifecycle. Second, attackers have been increasingly targeting industrial control systems and third parties to carry out attacks. Finally, GRIDCo needed to understand their suppliers' maturity and security processes for connected products and services to have assurance that these practices aligned with their own expectations.

GRIDCo also approached security differently for their OT and IT systems, noting key differences between the two. OT systems, which directly control devices and processes, require unique considerations for incident response due to their specialized place within operations, long refresh cycles, and high exposure to zero-day vulnerabilities. In contrast, IT systems, focused on information management and security, generally have shorter refresh cycles and better-defined paths for threat identification and remediation. Solutions that work in the IT environment can be detrimental in the OT environment; equipment on the OT side, especially older equipment, have failed when scanned by security solutions designed for IT networks. Developing incident response plans unique to IT and OT may be essential.

GRIDCo's OT Incident Management Plan

Adhering to the NIST Guide to OT Security (800-82 Rev. 3), GRIDCo developed a comprehensive Incident Management Plan (IMP) that spans the four main phases shown in Figure 12.

Preparation and Prevention

GRIDCo prioritizes the identification and protection of critical systems, employing a business impact analysis to inform their cybersecurity posture. They have adopted a key performance indicator (KPI) that they must be able to restore 80% of operations within 48 hours of an outage. Their incident response plan is specifically designed to achieve this with 95% certainty.

The business impact analysis is driven by their existing risk analysis processes. This process relies on multiple teams from finance, procurement, and engineering to determine the probability of an incident and the potential impact of the incident. They draw on their experience as well as contract terms to estimate the probability. Similarly, GRIDCo uses financial analysis to estimate potential impacts to then calculate risk and business impact.

GRIDCo then compares the results of the business impact and risk analysis with the treatment costs (i.e., the costs to implement controls to address the risk), as well as any residual or remaining risk. In the end, GRIDCo has confidence that they have appropriately matched their controls with their risks.

Detection and Analysis

Because supply chains can have a large impact on their cybersecurity posture, GRIDCo emphasizes vetting and collaborating with vendors to ensure cybersecurity compliance from the design phase through implementation. Vendors must demonstrate that they meet GRIDCo's criteria to participate in the tender process. In addition, GRIDCo considers security in the design phase, so that security requirements are embedded within the product. They inspect and validate the vendor's documentation and claims, even going so far as to require factory acceptance testing (FAT). Similarly, GRIDCo tests cybersecurity functionality (e.g., validates firewall rules) as part of a Site Acceptance Test (SAT) during deployment. Because people are key to security, GRIDCo also reviews whether the vendor has a culture of security to understand whether the vendor is likely to be responsive if there is an incident.

Containment, Eradication, and Recovery

GRIDCo has not had a service interruption but has had incidents that required response. In the past, their detection created many false positives, which they have worked to reduce through iterative improvements, such as deploying new triage processes and new systems to help identify false positives. Fewer alerts mean GRIDCo can act on the alerts that do arise. Upon detection of an issue, GRIDCo quickly initiates a well-structured response process (see Figure 15), focusing on rapid containment and recovery to minimize operational disruptions. Their incident management process includes

communication internally as well as with three external groups that GRIDCo is required to inform according to local regulations.

Figure 15. GRIDCo's response process from incident logging to resolution and closure.

Post-Incident Activity

Regular testing and simulations drive continuous improvement of the incident response plan, with lessons learned integrated into future iterations. These simulations are as realistic as possible. GRIDCo maintains a log of all lessons learned and reviews their plan at least annually.

Recognizing the supply chain as a critical vulnerability, GRIDCo implemented measures to assess and manage the cybersecurity risks associated with suppliers and third parties. This includes maintaining a categorized database of suppliers for periodic cybersecurity compliance assessments and pre-tender cybersecurity evaluations.

Procurement Example: GRIDCo's SCADA Upgrade

GRIDCo applied the process when they upgraded their SCADA system and deployed a new disaster recovery site control center in 2023 through several key actions:

- Including security considerations during the scoping and requirements gathering phase, before seeking vendors, to ensure security-by-design.
- Pre-qualifying prospective vendors to ensure any vendor selected would meet their security requirements. Moreover, the tenderers had to accept responsibility for undeclared vulnerabilities.
- Traveling to Europe to evaluate vendors practices and their products at the source. Outstanding issues were documented to ensure that they were resolved before taking delivery.
- Conducting SATs including cybersecurity reviews (e.g., firewall configuration audits, hardware and operating system hardening, Active Directory configuration, and redundancy assurance).
- Finally, they conducted a red-team attack to demonstrate that the system operated as expected.

Cybersecurity Incident Response Plan Suggestions

- ✓ Make available response plans and related information in print and on intranet (contact list, vendor information)

- ✓ Put the plan revision date in a header/footer on each page to identify the current version
- ✓ Establish delegates or backups for each role, so incident response isn't slowed when someone is not available
- ✓ Empower relevant people to make decisions to facilitate efficient response
- ✓ Document incident response resources in your plan (contracted incident response service, government resources, insurance, etc.)
- ✓ Through Cybersecurity Awareness programs, make all users aware of the company's Incident Response protocols, including how to initiate them
- ✓ Include possible simulations in the plan to test the plan periodically to ensure effective compliance

Additional Resources

- ➢ American Public Power Association, Public Power Cyber Incident Response Playbook (2019)
- ➢ NIST SP 800-61 Revision 2, Computer Security Incident Handling Guide (2012)
- ➢ NIST SP 800-82 Revision 3, Guide to Operational Technology (OT) Security (2023)
- ➢ NIST SP 800-83 Revision 1, Guide to Malware Incident Prevention and Handling for Desktops and Laptops (2013)
- ➢ NERC Cyber Intrusion Guide for System Operators (2023)
- ➢ CISA #StopRansomware Guide (2023)

Governance Policies and Procedures for Third-Party Cybersecurity Risk Management

Presenters
Terri Khalil Ampyx Cyber (formerly Ampere Industrial Security) **Roland Miller III** Cyber Florida Webinar Recording Presentation Slides

The rapid rise of digitalization in the electric utility industry has necessitated robust and strategic cybersecurity governance frameworks to address supply chain risk management. By examining current best practices on policies and procedures, reviewing typical models for managing cybersecurity, and discussing different approaches to communicate cyber risk, organizations will have a clear pathway to safeguarding information and maintaining operational and data integrity in today's complex digital landscape. Governance policies and procedures are a necessary complement to the technology controls that are frequently thought of first when discussing cyber security.

When creating governance policies, an organization must build a governance function and set up a charter. An organization may be able to leverage existing governance models found in a code of business conduct, a corporate compliance committee, or a regulatory affairs team, among others, or start from scratch. During the formation process, there are three essential "tiers" to include: an officer-level executive/senior sponsorship committee, a director-level steering committee, and a working group consisting of subject matter experts from relevant areas, team leads, and managers. Then, in partnership with appropriate stakeholders, the newly formed committee must review and agree upon a charter that outlines the group's mission, purpose, responsibilities, scope, and guidelines.

As with the creation of anything new, issues and obstacles are inevitable. One of the foundational pieces to governance is centralized procurement that enables third-party risk management. Without an existing method to identify and manage third-party engagements and enforce requirements and selection processes consistently, organizations will face major challenges to implementing new governance policies and managing risk. For example, an employee may make a purchase for a business service on their personal credit card and expense it to the company, or they may have a company card that allows them to make purchases without formal review. Upon purchasing, however, the employee may have unknowingly agreed to inappropriate or unmanaged regulated data sharing and third-party retention of private company data in the terms and conditions of the purchase. Had the company utilized a centralized procurement system, the purchase and associated terms and conditions would have gone through a rigorous review to ensure risk is mitigated, and any caveats or concerns would have been flagged and either addressed via new, independent contract or a different supplier may have been selected. Other problems an organization may face include fighting an uphill battle due to lack of existing governance, ambiguous and inconsistent policy application, weak leadership, poor communication, and lack of executive buy-in.

When setting up third-party risk management policies and procedures, figuring out which stakeholders to include can be a daunting task. In addition to procurement, key stakeholders may include representatives from appropriate functional areas and different geographic areas or sites as well as key decision makers and influencers such as subject matter experts and opinion leaders. Each of these stakeholders can be documented or assigned a responsibility or involvement aspect in a responsibility assignment matrix (e.g., a RACI [Responsible, Accountable, Consulted, and Informed] matrix), and engagement can be managed and maintained via ongoing engagement plans and other defined departmental/organizational goals. Below are some questions to help guide stakeholder identification:

- Who in the company utilizes third parties or suppliers?
- Who manages the third parties/suppliers' work?
- Who makes decisions about the third party and supplier work program?
- Who needs to know about the third party and supplier work program?
- Who can benefit from the success of the third party and supplier work program?
- Who can be harmed from the failure of the third party and supplier work program?
- Who can influence the third party and supplier work program culture?

Note that it is crucial for organizations to include third parties as stakeholders. Without including them, an organization will miss key input and feedback when identifying procurement-risk. Other potential sources of strain include lack of consensus, prioritization issues, misidentification of opinion leaders, including third parties in the governance process either too early or too late, varying company cultures between countries/parent companies/affiliates, and poor communication leading to uninformed stakeholders or obsolete policies.

As previously mentioned, lack of executive buy-in hinders implementing third-party risk management policies. If the requirement for supply chain risk management policies does not come from the executives themselves or from a regulatory requirement, other strategies may be useful to gain executive buy-in. It is crucial to speak in terms executives care about and address fundamental questions in the business language. The executive-level audience typically cares most about costs and revenue, so solutions should address how they mitigate potential loss of revenue, for example, revenue lost via decreased business operation or reputational impacts along with relevant likelihood. At a high-level, costs should focus on the cost of ownership before, during, and after implementation. Another consensus-gaining strategy uses a phased approach for implementation that demonstrates small, short-term wins and highlights the near-term qualitative benefits in addition to the broader, quantitative revenue implications.

Obtaining executive buy-in can be challenging for myriad reasons, but most challenges can be tied back to a lack of clarity. Examples include lack of clarity in cost/loss of revenue, in funding source (i.e., CAPEX

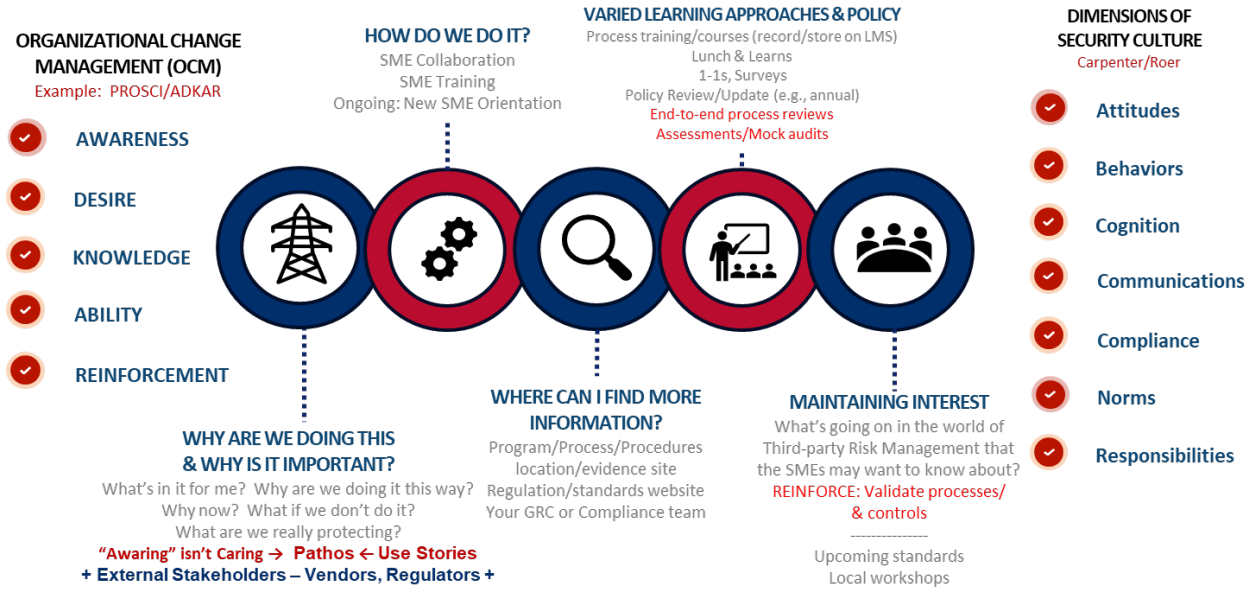


Figure 16. Organizational Change Management (OCM) model and considerations.

vs. OPEX), and in non-cyber risks due to inaction, as well as lack of consensus/other priorities. Although supporting a cybersecurity risk mitigation solution with cyber-related metrics is important, presenting potential non-cyber-related damages cannot be overlooked. If a cybersecurity risk mitigation strategy is not implemented, the organization may suffer reputational harm, relationships with third parties may be damaged, contracts may be breached, and/or regulatory bodies may impose fines or other sanctions.

Organizational change management (OCM) is a complicated process with many moving parts as shown in Figure 16, above. The ADKAR model is an example of an outcome-oriented change management method that aims to reduce resistance to organizational change. Shown on the left side of the figure, ADKAR stands for awareness, desire, knowledge, ability, and reinforcement. In the middle of the image, the five circles expand on each aspect of ADKAR and highlight key points and considerations to help improve acceptance and reduce opposition to new processes and policies in all levels of an organization. Note that OCM models and methodologies are similar, and it is typically most appropriate to leverage the model already in use by the organization.

Implementing new processes and policies at an organization is tough as it is and can be further complicated by barriers to change. Some examples include cultural differences, resistance to change, lack of sustainability, difficulties maintaining momentum after implementation, regressing to tactical thinking rather than strategic thinking, among others. Half-baked implementation of new policies and procedures also poses problems, such as missed milestones/deadlines, re-work resulting from not identifying and addressing issues upfront, and other delays in contracts with third parties. Fortunately, OCM methodologies have built-in strategies to help identify, combat, and reduce the barriers to change and downstream impacts from partial implementation. Ultimately, organizations need to establish and build a risk-informed and compliance- and security-focused culture as part of the organizational culture, especially around third-party risk, to prevent major business disruptions. It is important to note that companies do not really have a separate compliance culture—it is really part of organization culture.

To raise concerns and pitch solutions and strategies to mitigate risk, the risks must first be identified via risk assessment. Risk assessments should include employees with varying levels of visibility. The table below outlines the typical levels of visibility and their responsibilities with respect to risk assessments.

Table 3. Levels of Visibility

Position Title	Responsibility
Technical Staff	Involved in risk identification and remediation, including deviations (exceptions) from policies/standards
Cyber/Compliance Staff	Translate risk identification into business terms, track mitigation/remediation, review triggers, and manage exceptions
CISO/CSO	Sign-off on high-level risks and periodically review residual risks in third-party risk register (exceptions)
Business Leaders	Sign-off on risks
C-Suite/Board of Directors	Aware of all major risks in the context of enterprise risk/risk register

Ironically, even assessing risk poses risks of its own. As with any process, the risk assessment process can fail, so it is important to be aware of the potential areas where the process may break down. There could be risk identification issues, risk communication/explanation issues, poor documentation, tracking, and follow-up practices, rigid and strict processes or overly flexible and inconsistent processes, or employees could act on personal motivations and provide inappropriate approvals and signoffs. Thus, it

is crucial for organizations to walk through with governance stakeholders and communicate expectations to reduce the ways in which the process could fail.

Additional Resources:

- Miranda, Dana, and Watts, Bob, RACI Chart: Definitions, Uses and Examples for Project Managers – Forbes Advisor, June 2024.
- Athuraliya, Amanda, What is Stakeholder Identification: The Complete Guide with Templates | Creately, April 2024.
- Hiatt, Jeffrey M., ADKAR: A Model for Change in Business, Government and Our Community, Prosci Learning Center Publications, 2006.
- Roer, Kai and Carpenter, Perry, The Security Culture Playbook: An Executive Guide to Reducing Risk and Developing Your Human Defense Layer, Wiley, 2022.

Managing Cybersecurity Risks in a Rapidly Expanding Electric Grid

Presenters

Anuj Sanghvi
NREL

Ginger Wright
INL

Webinar Recording

Presentation Slides

Energy systems around the world are evolving across several dimensions, which may increase complexity in risk in addition to delivering the promised benefits. Two major changes include (1) the shift to more of a "prosumer" model where stakeholders that were formally just energy consumers are becoming energy producers as well, and (2) the evolving ownership models for generation resources. For example, homeowners or a third party may own the residential solar PV system, but an aggregator may have some level of control over that resource in addition to the distribution utility. The move from traditional centralized grid to more distributed energy resources brings with it complexity, especially at the grid edge. Energy is no longer just consumed, but rather it is generated, stored, managed, and traded, as shown in Figure 17 below. Doing so requires complex communication networks, which increases potential cyber vulnerabilities.

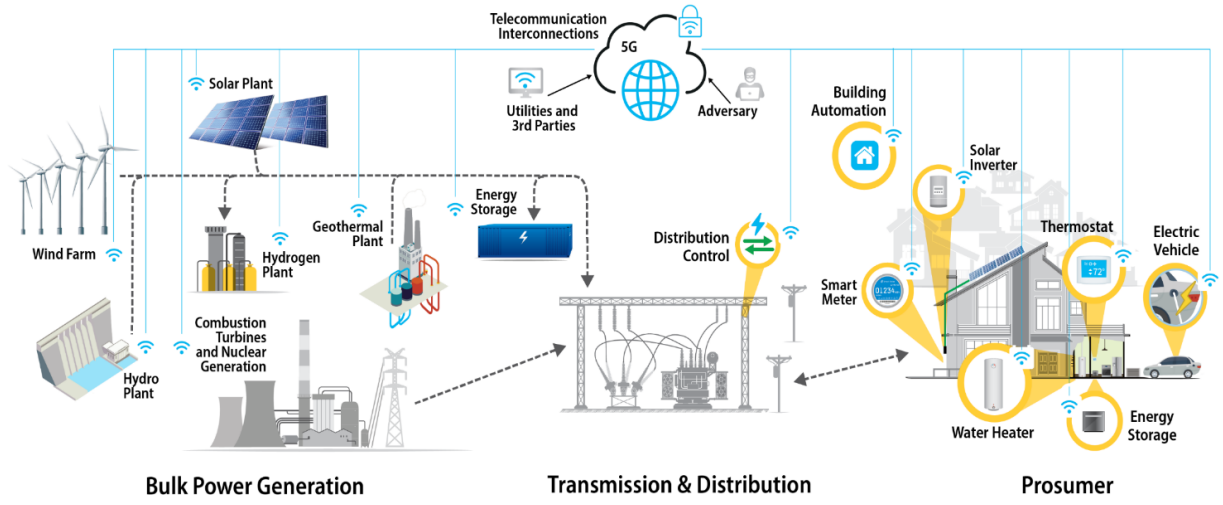


Figure 17. The evolving grid includes more communications and active participation from more stakeholders.

Distributed Energy Resources – Cybersecurity Framework

DER, like solar systems, wind systems, battery energy storage systems, and even electric vehicle charging equipment, are equipped with complex, data-driven communications networks to connect with the energy grid. These sophisticated devices often interact with legacy equipment that was not designed with security in mind. The growing number of devices that support DER can increase the number of access points outside a utility's administrative control. Unauthorized access to these systems could destabilize the local distribution system.

The National Renewable Energy Laboratory (NREL) developed the Distributed Energy Resources – Cybersecurity Framework (DER-CF) to help organizations assess and mitigate gaps in their cybersecurity posture for DER. The DER-CF covers key areas such as governance, technical management, and physical security. It offers a publicly accessible interactive version (hosted at dercf.nrel.gov) that provides tailored assessments, detailed results, and recommended actions for improving cybersecurity at individual sites.

The DER-CF is based on the U.S. Department of Energy's Cybersecurity Capability Maturity Model (C2M2) and uses the ten domains from the C2M2 to inform the assessment process. The DER-CF extends the C2M2 to new pillars, domains, and controls appropriate for managing the security of DER and is appropriate for both existing DER as well as new projects to understand existing or potential risks. The domains in the DER-CF also include two that focus on issues related to supply chain risk management: External Dependency Management, which is part of the Governance Security Assessment and Systems/Device Management (including software integrity), which is part of the Technical Management Security Assessment.

External Dependency Management domain focuses first on identifying and prioritizing third parties and their role within the organization's operations. This creates an understanding of the dependencies in the utility's operations on third parties. These dependencies can then be mapped to the delivery of critical functions within the utility (e.g., that support the reliability and resilience of the electricity delivery). Ideally, the mapping will highlight where additional consideration is needed, such as finding additional suppliers.

With Systems/Device Management within the Technical Management vertical, the primary focus is on understanding the software and hardware supply chain. The assessment leads utilities through managing the risks of deploying third-party products and services, like counterfeit or compromised software, hardware, and services.

As an outcome, DER-CF produces a prioritized list of recommendations based on the assessment results along with interactive dashboards for graphical representation of the organization's cybersecurity posture.

Cyber Informed Engineering

Cyber Informed Engineering returns the engineering side of operations to the consideration of the cybersecurity practices. This can be demonstrated by following a hypothetical cyber engineering problem and solutions at a Water Boost Station.

CIE Water Pump Booster

Imagine a very small municipal water utility whose mission is reliably treating and distributing safe drinking water to all the citizens and businesses of the town. Water Booster Pumps generate and maintain pressure at the right levels to ensure water reaches every location in the service area. When changes are needed, operators travel by truck to booster stations to make the appropriate adjustments. The same manual approach is used when they need to gather operational information.

The Call and The Opportunity

A cloud company called the water utility's General Manager saying they could deliver remote monitoring and control of the pump boosters, saving time and money and freeing up operators for higher value tasks. The cloud company had security credentials; it was SOC2 certified, and its solution was developed using the secure development lifecycle.

Considering the Offer

The water utility brought its engineers and cyber lead together as was the norm for big process changing decisions like this. An engineer asked how would the water utility know if someone accessed their equipment and made changes? Would they have to wait to see the actual physical changes in pressure via their pressure gauges, customer complaints, or by other means? The answer was somewhere between "we don't know, and we won't know."

Another employee asked what's the worst thing that could happen if a malicious attacker got access? The attacker could turn pump boosters off or on. Someone would have to go manually reset them, which would be annoying but not a catastrophe by any means.

Finally, an engineer asked what if the attacker turned a booster on and off so rapidly it caused physical damage, basically destroying the pump? And what if they did this to all the pump boosters? Six months to fully recover, huge costs, and ability to deliver water uncertain—a true catastrophe.

A CIE Solution

The group considered whether this risk was too much to bear and whether there could be any mitigation. One well-seasoned engineer suggested that a $20 time-delay relay—something he remembered played an important safety role back in the day—could do the trick. They could set the timer to allow only one change per 15 minutes or similar based on how long it takes the pump to shut down and for pressure transients to dissipate. A successful attacker would not be able to switch pumps off and on fast enough to damage them.

The only downside to this approach was that engineers would have the same limitation. They decided they could easily live with that, and in an extreme case, they could always suspend or ditch the cloud service and revert to the way they run their operations right now.

Takeaways

They deployed an affirmative, last ditch security defense that's under their complete control, which allows them to automate the right functions in ways that really help and make the operators jobs better. It's not an EITHER/OR switch, it's an AND. They get benefits of automation along with highest confidence security: A layered set of defenses.

Introduction to Cyber-Informed Engineering (CIE)

Cyber-Informed Engineering (CIE) is the concept of integrating cybersecurity into the engineering design process to mitigate risks before they manifest. It emphasizes the importance of designing physical systems with inherent security to prevent cyber-attacks, rather than relying solely on traditional cybersecurity tactics like firewalls and antivirus software. CIE uses the insights of engineers and operators to design engineering controls which minimize the impacts of cyber-attacks.

Application and Principles

CIE is applicable across various sectors, but the current work, funded by the U.S. Department of Energy, is particularly focused on the electricity sector. CIE is built around 12 principles, each with a key question that gets to the heart of the issue, as shown in Table 4. The first principle, Consequence-Focused Design, is critical to begin the CIE process. Utilities must understand their systems to develop solutions that extend engineering practices to address cybersecurity risks. Considering the impacts of cyber-attack as interruptions of desired functions highlights that cyber-attacks result in far more than the loss of data. They can impact operations, safety, and financial stability too.

Finally, CIE is a mode of working through the process of developing a robust security program. It complements many existing security best practices and standards like ISO/IEC 62443, the NIST Cybersecurity Framework, Process Hazard Analysis, and others.

Table 4. Cyber Informed Engineering Key Questions

Principle	Key Question
Consequence-Focused Design	How do I understand what critical functions my system must ensure and the undesired consequences it must prevent?
Engineered Controls	How do I implement controls to reduce avenues for attack or the damage which could result?
Secure Information Architecture	How do I prevent undesired manipulation of important data?
Design Simplification	How do I determine what features of my system are not absolutely necessary?
Layered Defenses	How do I create the best compilation of system defenses?
Active Defense	How do I proactively prepare to defend my system from any threat?
Interdependency Evaluation	How do I understand where my system can impact others or be impacted by others?
Digital Asset Awareness	How do I understand where digital assets are used, what functions they are capable of, and our assumptions about how they work?
Cyber-Secure Supply Chain Controls	How do I ensure my providers deliver the security we need?
Planned Resilience	How do I turn "what ifs" into "even ifs"?
Engineering Information Control	How do I manage knowledge about my system? How do I keep it out of the wrong hands?
Cybersecurity Culture	How do I ensure that everyone performs their role aligned with our security goals?

Additional Resources

DER-CF Resources:

- NREL's DER-CF
- NREL, Power System Cybersecurity Building Blocks
- USAID/NREL/CARILEC Cybersecurity Webinar Series
- NREL, Gap Analysis of Supply Chain Cybersecurity for DERs
- NREL, Supply Chain Cybersecurity Recommendations for Solar Photovoltaics

Cyber Informed Engineering Resources:

Websites

- DOE CESER CIE Website: https://www.energy.gov/ceser/cyber-informed-engineering
- INL CIE Website: https://inl.gov/cie/
- NREL CIE Website: https://www.nrel.gov/security-resilience/cyber-informed-engineering.html

Publications

- CIE Implementation Guide: https://www.osti.gov/biblio/1995796
- CIE Workbook for ADMS: https://www.osti.gov/biblio/1986517
- CIE Workbook for Microgrids: https://www.osti.gov/biblio/2315001
- CIE Workbook for Water Systems: https://www.osti.gov/biblio/2371031

- CIE Assessment Tool: https://github.com/inlguy/CIE/releases/tag/v12.2.4.0

Articles and Briefings

- SANS ICS Concepts Video: https://youtu.be/o_vIxW6UTeg
- Industrial Cyber: CIE and CCE Methodologies Can Deliver Engineered Industrial Systems for Holistic System Cybersecurity (June 11, 2023) with interviews from INL, 1898, and West Yost
- Harvard Business Review: Engineering Cybersecurity into U.S. Critical Infrastructure (April 17, 2023) by Ginger Wright, Andrew Ohrt, and Andy Bochman
- For more CIE articles and publications, visit: inl.gov/cie

Photo Credit: USAID Energy/Flickr

Procurement

Leveraging Procurement for Cybersecurity Resilience

Presenters:

- **Frank Harrill**, Vice President of Security, Schweitzer Engineering Laboratories (SEL, Inc.)
- **Jacob Phillips**, Midcontinent Independent System Operator (MISO)

This webinar focused on how procurement in the energy sector can be leveraged to strengthen cybersecurity across transmission system operators (TSOs), distribution system operators (DSOs), and generation entities. Topics explored included how systems associated with managing energy infrastructure, like SCADA and other industrial controls systems, energy market applications, advanced metering infrastructure and billing systems can be made more resilient by embedding cybersecurity specifications in procurement. Speakers considered how existing standards can be implemented to guide procurements through the lifecycle of operations. Webinar Recording

Coordinating Cybersecurity Risk Management with Hardware/Software Vendors

Presenters:

- **Claudia Iannazzo**, CEO and Founder, Catalisto
- **Sokol Mukaj**, Chief Information Officer, KESH (Albania Power Corporation)

This webinar focused on the remaining lifecycle of the operation of critical IT and OT systems in a utility. Whereas the previous webinar (Leveraging Procurement for Cybersecurity Resilience) focused on preparing for procurement and conducting procurement/reviewing proposals, this webinar discussed the process of negotiating contracts and maintaining the relationship with the vendor throughout the lifecycle of operations (e.g., receiving and applying patches), and offboarding vendors as needed. Webinar Recording

Leveraging Procurement for Cybersecurity Resilience

Presenters
Frank Harrill SEL, Inc.
Jacob Phillips MISO
Webinar Recording
Presentation Slides

Procurement in the energy sector plays a pivotal role in strengthening cybersecurity, particularly within transmission system operators (TSOs), distribution system operators (DSOs), and generation entities. By embedding cybersecurity specifications into procurement processes and requirements, utilities can ensure a higher level of security in critical infrastructure systems such as SCADA, energy market applications, advanced metering infrastructure, and billing systems, among others. The integration of cybersecurity into procurement processes not only enhances resilience but also ensures alignment with existing standards to guide and optimize procurements through the lifecycle of operations.

Vendor Cybersecurity Assessment Program

A vendor cybersecurity assessment program is one effective tactic to embed cybersecurity in the procurement process. Effective vendor cybersecurity assessment programs: (1) start addressing cybersecurity early in the procurement process, (2) leverage global industry standards, (3) use independent third-party assessors, and (4) plan for negotiations with vendors to address areas of weakness.

Early evaluation and management of key vendors is important to ensure that the solution meets the cybersecurity requirements of the organization. Moreover, early evaluation ensures that the cybersecurity requirements have been thought out and planned. Specifications should cover elements such as authentication, authorization, data encryption, and secure coding practices, among others.

By leveraging established global and industry standards, organizations can both better ensure reliability as the standards prove to be effective in industry and ensure that the procuring organization does not have to reinvent the wheel and create a standard to judge a vendor against, thus saving both parties time and money. In the cybersecurity arena, some common global and industry standards include:

- **ISO/IEC 27001:** This international standard provides specifications for an ISMS. By adhering to this standard, energy sector entities can manage the security of assets such as financial information, intellectual property, employee details, and information entrusted by third parties.
- **NIST Cybersecurity Framework:** Developed by the National Institute of Standards and Technology, this framework provides a policy framework of computer security guidance for how private sector organizations in the US can assess and improve their ability to prevent, detect, and respond to cyber-attacks. It includes guidelines that can be directly applied to procurement processes to enhance cybersecurity.
- **Cybersecurity Capability Maturity Model (C2M2):** Framework designed to help organizations in the critical infrastructure sector assess and enhance their cybersecurity practices by evaluating their maturity across various domains (i.e., risk management, asset management, incident response, etc.).
- **ISA/IEC 62443 Series of Standards:** This series of international standards, developed by the International Electrotechnical Commission, focuses specifically on the security of industrial automation and control systems (IACS). It aims to enhance the resilience and security posture of critical systems by providing guidance for risk assessments, system designs, security measure implementation and monitoring, among others.

Organizations can expedite the assessment process by employing independent third parties to assess vendor risk and quality. Many governments, including the United States, develop guidance, frameworks, and regulations that can be used to require compliance in vendors. A risk assessment vendor provides independent industry assessments and ratings of vendor offerings to evaluate their strengths and manage risks. A risk monitoring vendor helps organizations manage cybersecurity by continuously monitoring and assessing product vendors for changes in risk profiles. These monitors may also conduct audits to assure compliance with standards and requirements.

Lastly, effective cybersecurity programs have solid negotiation tactics, both internally and externally. External negotiation tactics aid in times when cybersecurity is not advertised as a strength of a solution despite the solution perhaps meeting or even exceeding all other requirements. In these situations, emphasizing the mutual benefit of strengthened cybersecurity features, offering incentives, or challenging suppliers that disclaim or minimize liability may be successful strategies. Internally, negotiations are needed when a decision-maker chooses to go through with a cheaper solution that meets the bare minimum or even falls short but is granted an exemption. Winning tactics include engaging leadership and gaining support for security as a priority, explaining that upfront costs may be lower, but the potential reliability, financial, and reputational damages later may cause much higher costs, providing examples of failures to appeal to pathos, and being open to compromise and alternatives.

The Procurement Process

Cybersecurity procurement programs are cross-functional efforts with several different units within an organization. The business area that deploys and uses the product or service should describe the need and their requirements. A supply management group or procurement office should assist with the request for proposal (RFP) process. IT establishes and evaluates the cyber requirements. Legal ensures that the terms and conditions address those requirements adequately. Finally, management provides the final approval, which can only be given if management understands the risks and supports the risk mitigations needed for implementation. Figure 18 below shows the vendor cybersecurity assessment process at MISO at a high-level.

One of the most important aspects of the procurement process is understanding the business needs that are driving the procurement. Utilities should have a clear understanding of the needs, the network connections that will be necessary to meet those needs, and what information the utility would share

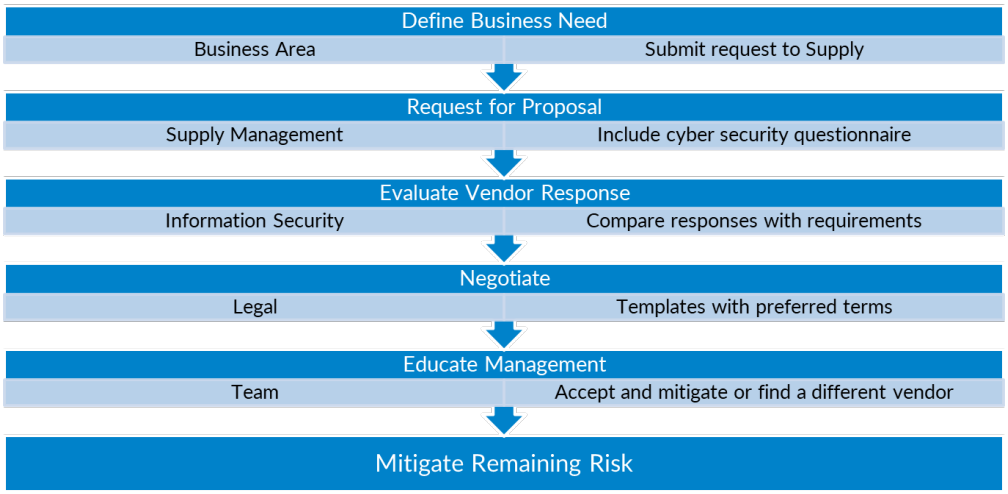


Figure 18. High-level view of the cybersecurity procurement process at MISO.

with a vendor to meet those needs. The specific cybersecurity capabilities required in the RFP for a product or service will be different whether the vendor's system will connect to the utility's sensitive cyber assets or whether it will be isolated from those assets.

It is important to be as surgical as possible about the actual needs and to be accurate upfront. Organizations should establish cybersecurity expectations for vendors early in the procurement process by including those expectations in the RFP. Vendors can then respond appropriately and adjust budgets and plans accordingly. The RFP may contain soft requirements as well, which the solution "should" have, but perhaps are not strictly necessary. The eventual contract will specify the hard requirements, and the utility can plan mitigations for any of the soft requirements that were not fulfilled. Note that if the RFP could contain any sensitive information, then the utility should be looking to trusted suppliers in a private RFP and should implement non-disclosure agreements with those suppliers.

Where and when applicable, organizations can and should use standardized assessments. An example of this is the NATF Questionnaire, a standardized tool developed by the North American Transmission Forum to assess and improve the cybersecurity posture of those involved in the transmission of electricity. Despite its name, the NATF Questionnaire is rooted in cybersecurity best practices overall and aligns with other international standards, and thus can be utilized globally. Using a standardized assessment lessens the burden on all parties involved as utilities do not have to develop their own questionnaire, nor do vendors have to respond to a unique assessment for each potential client.

Organizations should identify their critical and non-critical vendors. In general, critical vendors supply products or services without which the utility would have a disruption in operations (i.e., if the product were unavailable or not functioning). The utility should give critical vendors a risk rating, at least qualitatively (e.g., low, moderate, and high), based on the vendor's capabilities and the controls they have implemented. Standards can be useful to consider the vendor's capabilities and risk. For example, if a vendor is ISO 27001 certified and agrees to maintain their certification, then that vendor could be considered low risk.

Maintaining vendor relationships and bi-directional communication helps organizations react quickly to cybersecurity incidents. The contract and SLA should define these expectations and requirements, so it is imperative that the contract language is understandable, accessible, and achievable. The Edison Electric Institute (EEI) Model Procurement Contract Language document is a useful reference for contract language but may need to be adapted to other markets or standards.

Contract and Procurement Language

Contract and procurement language is a form of administrative control, and therefore not effective as a stand-alone control. It is one layer in a multilayered risk control strategy. To be effective, contract language needs to be clear and understandable. Similarly, all parties to the contract need to have the same understanding of the meaning of that language. Standards can be useful to convey this shared meaning. Contract language should also be as simple as possible, but no simpler. Finally, contract language should create flow-down obligations to second- and third-tier suppliers, in part to promote increased cybersecurity awareness and defensive strategies throughout the entire supply chain, especially in today's world of well-funded adversary groups.

The contract language contains only the hard requirements which the vendor must adhere to. Therefore, it is important for utilities to ensure that they are only requiring terms that they actually need, rather than wasting time and resources on extraneous things. Note that these requirements will likely change from one system to another, so including a "standard" list of technical controls in the

contract language could cause unintended consequences. A list of information technology controls might not be applicable on an internal network within the OT environment. For example, if contract terms require that every device that must support Azure AD/Entra ID, then the utility could end up requiring such functionality in something like a PLC that does not really need it.

Similarly, if contract language is too specific, the procuring utility might not have the flexibility to meet the particular needs of the project. This is especially true if the contract will be in place for years, while technology could change or threats can evolve. Instead, utilities can make it clear that requirements can be developed through the life of the contract.

Trust But Verify

Building trusted relationships with suppliers can be mutually beneficial for both the procuring utility and the suppliers. Procurement is more than driving to the lowest possible price and checking off boxes—it is a true business partnership that requires collaboration and communication to better meet the needs of both parties. Utilities should verify that suppliers deliver products and services as expected. Moreover, utilities should establish redundancy whenever possible. Trusting but verifying may involve on-site visits (if possible) to ensure that the supplier is delivering what was promised, or it may involve independent, accredited third parties to audit and certify that the necessary controls are in place, such as those required to meet ISO 27001 and IEC 62443. While certification to these international standards is widely respected, there can be a misunderstanding about the scope of the certification. Depending on the standard, suppliers may be certified only for specific products/product lines or only at certain locations. Thus, it is imperative that procuring organizations ask for and review the statement of applicability and the scope that is associated with each certification.

For suppliers that are not certified to one of these international standards, the NATF questionnaire can help ascertain the supplier's cybersecurity competence. In any case, utilities should verify that the supplier has business continuity and incident response plans in place, at a minimum. That said, disclosure of sensitive information can create undue risk for the supplier and utility, which may have concerns about data leaks and additional security for third party information respectively. Visual inspection of this information or reliance on independently audited third-party certifications may suffice.

Finally, utilities may also conduct a surface-level assessment of their suppliers by reviewing the security practices associated with the supplier's internet presence. Two notable tools to use are:

- https://securityscorecard.com/security-rating/[insert domain name of supplier]
- https://webscan.upguard.com/

Note that these sites are not foolproof and can return false positives, but they can still be a valuable preliminary assessment of potential suppliers and give the procuring organization a rough idea of if or how they want to proceed in subsequent conversations.

Evaluating suppliers is never a one-time action; suppliers must be continually assessed to confirm that expectations are being met.

Additional Resources

- Security Scorecard: https://securityscorecard.com/security-rating/[insert domain name of supplier]
- UpGuard: https://webscan.upguard.com/
- EEI, Model Procurement Contract Language Addressing Cybersecurity Supply Chain Risk, Version 3.0, October 2022

Coordinating Cybersecurity Risk Management with Hardware/Software Vendors

Presenters
Claudia Iannazzo Catalisto
Sokol Mukaj KESH
Webinar Recording
Presentation Slides

Utilities and other organizations could fall victim to a supply chain attack through no fault of their own as demonstrated in March 2023 by the 3CX supply chain attack (see call out box below). Rather than focusing on how to avoid a supply chain attack, utilities should focus on how to quickly detect and fully recover from such an attack by taking steps throughout the lifecycle of the relationship with the vendor from procurement and selection, during deployment, and through to offboarding. Best practices in coordinating cybersecurity risk management with vendors are exemplified by KESH, the Albania Power Corporation, which operates nearly 80% of the generation capacity, primarily from large hydropower plants, as well as guarantees the security of the Albanian energy system through balancing energy and auxiliary services. KESH implemented several advancements to its cybersecurity program through a program supported by USAID and carried out by Catalisto.

Their advancement began with a detailed specification criteria for the type of technology solution that KESH needed, including a mix of software and hardware. The second step was to issue the RFP to a selection of vendors. KESH had selected about 70 vendors of widely varying sizes from the large, established companies to smaller ones. The broad vendor pool gave them a better chance at finding the best pricing. Moreover, multiple responses identified useful ideas and approaches that could potentially be adopted by the eventual selected vendor. They compiled the responses in an Excel spreadsheet to analyze them and apply the scoring rubric, leading to a vendor recommendation for KESH's consideration.

Information Request through the RFP

Utilities collect critical information from the vendor either through the RFP response process or through the negotiation process. Utilities should understand whether the vendor themselves uses third party providers or outsourcing to deliver the software to the utility. Moreover, the location of those second-tier suppliers should be known, because they might be located in countries that increase the geopolitical risk of acquiring the product or service. That is, utilities should understand where the

3CX Supply Chain Attack Example

In March 2023, an employee of 3CX, a company that provides VOIP software, downloaded a compromised version of a futures trading software, X_Trader to their personal computer. While this compromised version of X_Trader appeared legitimate and came directly from the software developer, it had a malware installer. Two days later, 3CX recorded an attacker using that employee's credentials to access the company's VPN. The attacker then loaded a dynamic link library (DLL) payload into 3CX's Electron Desktop Application corrupting it such that when it executes on one of 3CX's clients' machines, instead of querying a legitimate location for the DLL, it looked for the compromised version. The compromised DLL would then allow the attackers to download additional malware onto the clients' machines. Note that, like the X_Trader software, the compromised version of 3CX's Electron Desktop Application appeared to be legitimate because the compromise had occurred prior to the legitimate distribution channels for that software. The attackers were able to gain access to a significant portion of 3CX's customers; victims included at least a US energy operator and a European energy operator. This attack is one of the first examples of a supply chain attack (through X_Trader), which lead to a second supply chain attack (through the Electron Desktop Application).

vendor's support team and/or development team is located. Another essential piece of information in contact information for a CISO such that the utility can reach someone in case of an incident.

Additionally, utilities should have a decent understanding of the solution description and capabilities. Utilities should understand the solution architecture, including the hardware needs, integration needs, deployment environment (e.g., on-premises or cloud-based), and whether it contains open-source resources. Data flows through the product are also important. Utilities should determine what data of theirs will go to the product or service as well as where the service might be sending data. Similarly, where the data is stored, how long it is kept, and how it is backed up should all be known. These details should align with the needs of the utility as described in the RFP. Finally, utilities should ask about multi-factor authentication for administrators at a minimum and for additional users if applicable. Many vendors do not yet support MFA, so utilities should ask.

Response Packages

For some vendors, the NATF questionnaire may be excessive and a barrier to responding to the RFP if the questionnaire is a part of it. Table 5 below lists six questions that may be useful without being too burdensome on the vendor along with some guidance on why to ask the question and how to interpret responses.

Table 5. Recommended questions for vendors and notes on interpreting their responses.

Question	Response Interpretation
1. Do you have any security related certifications/ standards you commit to (e.g. ISO27001, SOC Type II, NIST 800-171, CMMC etc.) and if so describe whether you are independently audited to the standard or self-certified to that standard.	The specific standard is not necessarily important so much as the vendor's level of maturity and therefore level of risk that the procuring utility should plan for.
2. How many successful cybersecurity attacks has your organization experienced in the last 2 years? Successful means the attacker was able to gain unauthorized access to systems or information (including solution source code).	Most companies have experienced some type of breach, so an answer of "zero" may be suspect. It could indicate that the vendor has poor detection or that they are unwilling to be forthcoming.
3. When was the last time your technical solution was manually penetration tested? (meaning human specialists were used to systematically identify vulnerabilities, navigate the application/ system and attempt to exploit vulnerabilities)	Penetration tests, whether focused on a technical solution or an entire organization, are more involved than an automated vulnerability scan. These questions can indicate the vendor's sophistication and how seriously they take their own cybersecurity capabilities.
4. When was the last time your organization was manually penetration tested? (meaning human specialists were used to systematically identify vulnerabilities, navigate the application/ system and attempt to exploit vulnerabilities)	
5. Will you agree to disclose the name, nationalities and countries of residence of all personnel involved in implementation of the solution on our systems (that are of national importance)?	As critical energy infrastructure, it may be inappropriate for citizens of countries with problematic relationships with the utility's country to support the project.
6. Will you agree to sign a mutual NDA with the operator to ensure any information disclosed to you during implementation or otherwise is kept in strict confidence?	Reputable vendors will be willing to sign an NDA. Utilities should not rely solely on the procurement contract, so a separate NDA is worthwhile.

Compliance Checks

Utilities should conduct checks on their suppliers and their products using one or more public databases before signing a contract to look for sanctions or known vulnerabilities. Three useful resources include the Sanctions List Search, the UN Consolidated List, and the NIST National Vulnerability Database.

- **U.S. Treasury, Office of Foreign Assets Control, Sanctions List Search**
  https://sanctionssearch.ofac.treas.gov/
  Utilities can check the name of the company, the current leadership, and or the company owner or founder with this database of US sanctions.
- **United Nations Security Council Consolidated List**
  https://main.un.org/securitycouncil/en/content/un-sc-consolidated-list)
  The UN Security Council Consolidated list contains information on international sanctions that utilities should be aware of before signing a contract.
- **NIST National Vulnerability Database (NVD)**
  https://nvd.nist.gov/
  The NVD contains a list of public vulnerabilities across many different products. Utilities can check the product they are procuring, find vulnerabilities, look at the severity score for the vulnerability, and potentially find a vendor advisory with additional information and patch if available.

Vendor Negotiations

Once the utility has selected a vendor, they will typically enter negotiations to finalize the contract. Utilities should clarify any remaining questions about the vendor's response to the RFP. In addition, utilities should check the vendor's references, preferably in a similar industry (e.g., other energy operators). Rather than ask whether the vendor is good or bad, ask process-oriented questions like "what are the things we should do to get the best value from the vendor?" or "Can you explain the implementation process the vendor took you through?" to get more insightful responses.

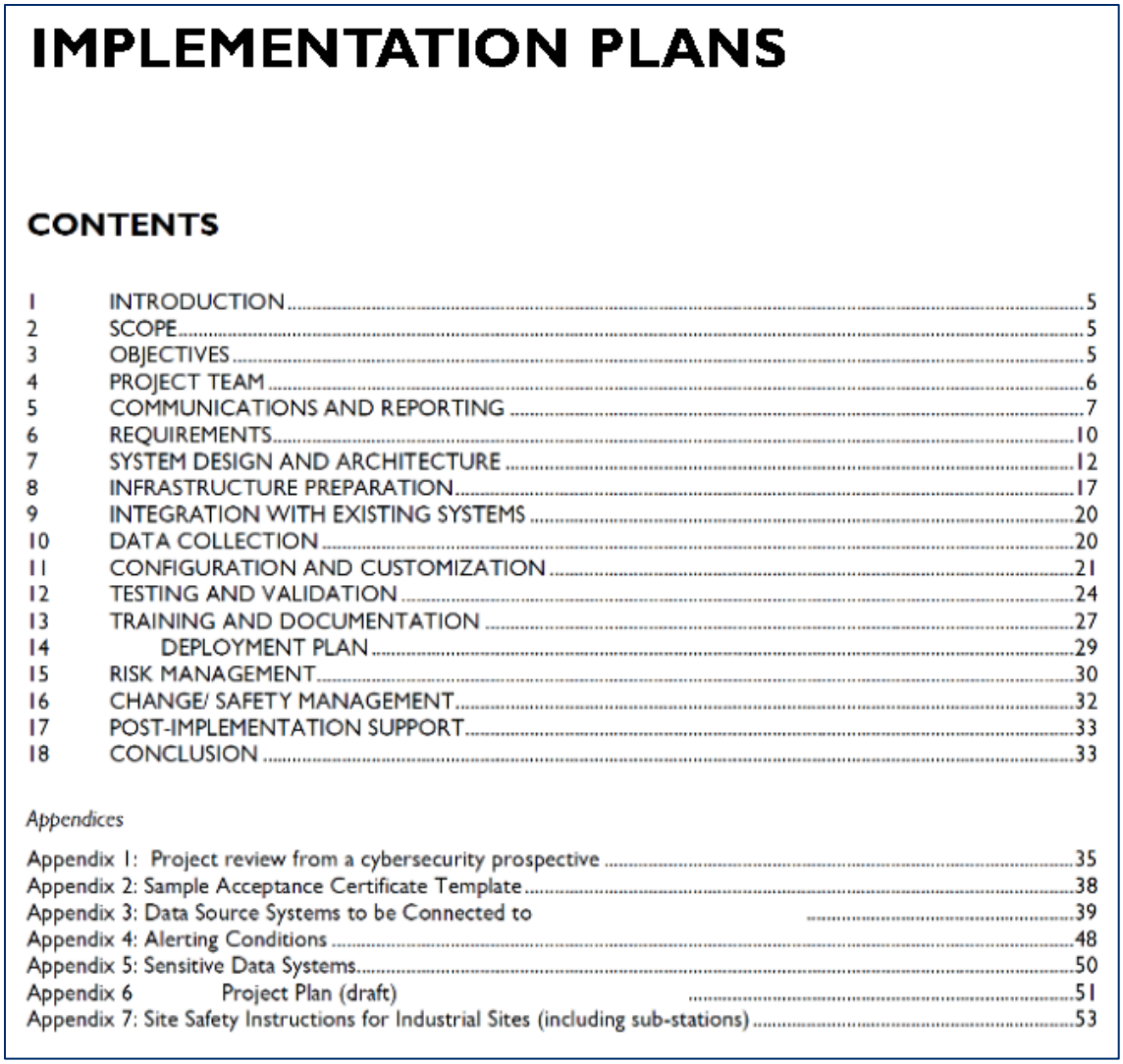
This negotiations phase may uncover changes that should be included in writing in the contract and statement of work.

Finally, utilities should conduct a vendor risk assessment, which can consider many different dimensions beyond just cybersecurity risk specifically. Utilities can consider compliance risk, reputational risk, credit/ financial risk, operational risk, strategic risks, and transaction risks.

Implementation Phase

During implementation, utilities should use a documented *Implementation Plan* to capture all the details of the implementation. This should be a living document that is updated throughout the implementation, including a final update at the end of the project to capture the final details. This document becomes a record of how the implementation was done and what decisions were made and why. An example Table of Contents for an implementation plan is shown in Figure 19.

In addition to the vendor risk assessment, utilities should conduct a risk assessment specific to the implementation of the vendor's product within the utility's network. The risk assessment will identify specific risks related to the implementation. The utility can develop recommendations and measures that the vendor should take prior to implementation. For example, if the vendor requires remote access for maintenance, then they must implement (or agree to utility implemented) secure remote access in line with zero-trust principles.



IMPLEMENTATION PLANS

CONTENTS

Figure 19. Example Table of Contents from KESH's Implementation Plan

Post Implementation Phase & Offboarding

Utilities should conduct vendor management beyond the implementation phase. Continuous post-implementation management includes regular security audits and compliance checks to ensure that the implementation aligns with the requirements and that controls are functioning as intended. Utilities should keep a detailed log of interactions and changes to ensure traceability. Finally, utilities should establish clear communication channels with vendors for reporting and resolving issues.

Eventually, the utility may decide to pursue another solution and therefore will need to offboard a previous vendor. Utilities should document a thorough offboarding process to prevent data leakage and maintain security even after the relationship. The utility should understand the uninstallation process for software and hardware. The vendor should attest that data destruction policies are followed at the vendor's site. Finally, the utility should update its asset and systems inventories to reflect the removal of vendor systems.

Vendor Risk Management from Cradle to Grave

Vendor Risk Assessment Components:

- ✓ Evaluate the vendor's cybersecurity strategy, awareness, and controls.
- ✓ Assess the geographical location of developers and operations personnel to identify potential risks.
- ✓ Conduct checks to ensure there are no international sanctions or known vulnerabilities.
- ✓ Assess financial stability to ensure the vendor can perform as required.
- ✓ Evaluate operational risks, including the vendor's business continuity and disaster recovery plans.
- ✓ Consider strategic risks, such as alignment with business goals.
- ✓ Assess transaction risks, including the vendor's capacity to perform due to technological failure or human error.

Cybersecurity Risk Mitigation Measures:

- ✓ Implement access controls, restrict access to authorized personnel, and enforce role-based access controls.
- ✓ Ensure sensitive information is encrypted using secure protocols.
- ✓ Conduct regular backups and store them securely.
- ✓ Keep all software and firmware updated with the latest security patches.
- ✓ Use next-generation firewalls and intrusion detection/prevention systems.
- ✓ Segment the network to limit the impact of potential attacks.
- ✓ Employ advanced threat detection and response solutions like EDR or extended detection and response (XDR).
- ✓ Continuously monitor the infrastructure for potential threats using SIEM systems and other tools.

Steps to Take Post-Implementation:

- ✓ Update asset and systems inventories to reflect the new hardware and software.
- ✓ Review and update business continuity plans and incident response processes.
- ✓ Conduct annual risk audits with the vendor to maintain ongoing security and compliance.
- ✓ Ensure all critical data and system configurations are backed up and tested regularly.

Offboarding Considerations:

- ✓ Understand the uninstallation process for the vendor's software and hardware.
- ✓ Ensure all data is deleted according to retention policies and vendor site data destruction procedures.
- ✓ Update all inventories to reflect the removal of the vendor's systems.
- ✓ Ensure a smooth transition to new vendors, if applicable.

Additional Resources

- ➢ U.S. Treasury, Office of Foreign Assets Control, Sanctions List Search
- ➢ United Nations Security Council Consolidated List
- ➢ NIST National Vulnerability Database
- ➢ Catalisto, Vendor Risk Analysis Template (xlsx)

Appendix A: Cybersecurity Supply Chain Risk Management Checklist

The actions listed below reflect the guidance from throughout this handbook. They have been re-organized and streamlined. Note, the activities below are not necessarily performed in order from top-to-bottom; some may need to happen concurrently. That said, governance considerations are typically needed at the outset to set scope and ensure leadership buy-in.

Governance, Policies, Planning, and Risk Management

- Create a charter that outlines the governance mission, purpose, responsibilities, scope, and guidelines with respect to supply chain cybersecurity
    - Identify stakeholders from across the utility, and key suppliers, that could be affected by changes in third-party risk management (e.g., centralized procurement processes)
    - Use an outcome-oriented change management model to implement new processes and policies
- Perform risk assessment at an organizational level and on critical operational segments
    - Identify vendors for systems and services in critical operations
    - Identify severity and impact for individual risks and individual vendors
    - Implement risk treatments for identified risks
- Develop policies and procedures to manage existing supplier relationships and onboard new suppliers:
    - Adopt one or more international standards as source(s) for policy requirements (e.g., NIST Cybersecurity Framework version 2.0, ISO/IEC 27001, ISO/IEC 62443)
    - Tailor requirements in standards to organizational needs
    - Centralize procurement processes as appropriate
    - Develop RFP processes that define cybersecurity requirements for vendors and/or pre-qualify vendors
    - Include cybersecurity requirements and expectations in contractual terms and conditions, including clean consequences for failure to comply with these terms
    - Apply internal mitigation measures
- Develop and maintain an Incident Response Plan
    - Include key elements addressing roles and responsibilities, detection, containment, eradication, recovery, and communication plans
    - Consider threat scenarios that could impact critical systems/operations
    - Develop playbooks to respond to potential threats/incidents
    - Conduct tabletop exercises to test incident response plan and playbooks
    - Update incident response plan with lessons learned

Asset Management

- Understand business processes and identify critical systems/operations
- Identify operational and business constraints
- Identify internal capabilities and gaps in capabilities needed to implement desired level of cyber security program
- Implement Defensible Architecture. Some key characteristics include:
    - Segmentation between IT and OT (Purdue Levels 5 and 4)

    - Multiple DMZs as appropriate to separate traffic between IT and OT (within Level 4)
    - Segmentation of all processes (in Level 2) from the site-wide supervisory (Level 3)
    - Segmentation between processes within OT environments (in Level 2)
    - Separate management services (e.g., AD) for IT and OT
- Implement Secure Remote Access / Cloud Access
    - Separate DMZs for remote access and cloud access as appropriate
    - 2-step authentication for humans
- Monitor OT network and physical power system
    - Monitor OT networks, especially gateways/bottlenecks for anomalous user activity
    - Monitor physical power systems as essential data source for anomalous activity
- Periodic review of critical systems and security practices
    - Assess which systems are critical as the utility grows or evolves
    - Reconfigure network architecture to align with risk and capabilities

Procurement Processes: Vendor Risk Management from Cradle to Grave

- Vendor Risk Assessment Components:
    - Evaluate the vendor's cybersecurity strategy, awareness, and controls (note: an established questionnaire like the NATF Energy Sector Supply Chain Risk Questionnaire may be a useful starting point)
    - Assess the geographical location of developers and operations personnel to identify potential risks
    - Conduct checks to ensure there are no international sanctions or known vulnerabilities
    - Assess financial stability to ensure the vendor can perform as required
    - Evaluate operational risks, including the vendor's business continuity and disaster recovery plans
    - Consider strategic risks, such as alignment with business goals
    - Assess transaction risks, including the vendor's capacity to perform due to technological failure or human error
- Cybersecurity Risk Mitigation Measures for Individual Systems
    - Implement access controls, restrict access to authorized personnel, and enforce role-based access controls
    - Ensure sensitive information is encrypted using secure protocols
    - Conduct regular backups and store them securely
    - Keep all software and firmware updated with the latest security patches
    - Use next-generation firewalls and intrusion detection/prevention systems
    - Segment the network to limit the impact of potential attacks
    - Employ advanced threat detection and response solutions like EDR or XDR
    - Continuously monitor the infrastructure for potential threats using SIEM systems and other tools.
- Steps to Take Post-Implementation:
    - Update asset and systems inventories to reflect the new hardware and software
    - Review and update business continuity plans and incident response processes
    - Conduct annual risk audits with the vendor to maintain ongoing security and compliance
    - Ensure all critical data and system configurations are backed up and tested regularly
- Offboarding Considerations:
    - Understand the uninstallation process for the vendor's software and hardware

- Ensure all data is deleted according to retention policies and vendor site data destruction procedures
- Update all inventories to reflect the removal of the vendor's systems
- Ensure a smooth transition to new vendors, if applicable

Appendix B: Additional Resources

Risk Management

The Emerging Cyber Threats to Industrial Control Systems (ICS) – Supply Chain Cybersecurity

- National Renewable Energy Laboratories (NREL), Resilient Energy Platform
- TSA Pipeline Security Directive 2021-01B (see also the full list of Security Directives)
- ISA Standards
- IEC Standards
- ISASecure Certification: ISASecure - IEC 62443 Conformance Certification
- IECEE CMC Certification
- Common Vulnerabilities and Exposures website (CVE.org)
- U.S. Cybersecurity and Infrastructure Security Agency (CISA)
- MITRE ATT&CK
- Relevant Webinars
  - USEA Webinar on Standards and Best Practices
  - USEA Webinar on ISO 27001

Standards on Third-Party Risk Management and Cyber Risk Assessment Methodologies

- NIST SP 800-161r1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations
- NIST Cybersecurity Framework v2.0
- European Energy Information Sharing & Analysis Centre (EE-ISAC)
- ISO/IEC 27001 – Information Security Management System
- ISA/IEC 62443 Standards – Security of Industrial Automation and Control Systems
- IEC 62531 – Cyber Security Series for the Smart Grid
- ISO 31000 Risk management

Conducting Cyber Risk Assessments for Supply Chain Risk Management

- NATF Documents
- NATF Energy Sector Supply Chain Risk Questionnaire (xlsx)
- NATF Supply Chain Risk Management Guidance
- NATF Supply Chain Security Criteria (xlsx)
- EEI, Model Procurement Contract Language Addressing Cybersecurity Supply Chain Risk, Version 3.0, October 2022

Asset Management

Best Practices for Secure Remote Access and Cloud Security in the Electricity Sector

- SANS, The Five ICS Cybersecurity Critical Controls (November 2022)
- ISA/IEC 62443 Standards – Security of Industrial Automation and Control Systems
- Williams, T. J. "The Purdue Enterprise Reference Architecture." IFAC Proceedings Volumes, 12th Triennial World Congress of the International Federation of Automatic control. Volume 4 Applications II, Sydney, Australia, 18-23 July, 26, no. 2, Part 4 (July 1, 1993): 559–64. https://doi.org/10.1016/S1474-6670(17)48532-6.

Defensible Architecture and Asset Management for Electric Utility Cybersecurity

- Scott Fitch and Michael Muckin, *Defendable Architectures: Achieving Cybersecurity by Designing for Intelligence Driven Defense*, (2019)
- SANS, The Five ICS Cybersecurity Critical Controls (November 2022)

- Dragos, OT-CERT
- E-ISAC
- WaterISAC

Governance, Policies and Planning

Cybersecurity Incident Response Plan Development

- American Public Power Association, Public Power Cyber Incident Response Playbook (2019)
  NIST SP 800-61 Revision 2, Computer Security Incident Handling Guide (2012)
- NIST SP 800-82 Revision 3, Guide to Operational Technology (OT) Security (2023)
- NIST SP 800-83 Revision 1, Guide to Malware Incident Prevention and Handling for Desktops and Laptops (2013)
- NERC Cyber Intrusion Guide for System Operators (2023)
- CISA #StopRansomware Guide (2023)

Managing Cybersecurity Risks in a Rapidly Expanding Electric Grid

DER-CF Resources:

- NREL, DER-CF
- NREL, Power System Cybersecurity Building Blocks
- USAID/NREL/CARILEC, Cybersecurity Webinar Series
- NREL, Gap Analysis of Supply Chain Cybersecurity for DERs
- NREL, Supply Chain Cybersecurity Recommendations for Solar PV

Cyber Informed Engineering Resources:

Websites

- DOE CESER CIE Website: https://www.energy.gov/ceser/cyber-informed-engineering
- INL CIE Website: https://inl.gov/cie/
- NREL CIE Website: https://www.nrel.gov/security-resilience/cyber-informed-engineering.html

Publications

- CIE Implementation Guide: https://www.osti.gov/biblio/1995796
- CIE Workbook for ADMS: https://www.osti.gov/biblio/1986517
- CIE Workbook for Microgrids: https://www.osti.gov/biblio/2315001
- CIE Workbook for Water Systems: https://www.osti.gov/biblio/2371031
- CIE Assessment Tool: https://github.com/inlguy/CIE/releases/tag/v12.2.4.0

Articles and Briefings

- SANS ICS Concepts Video: https://youtu.be/o_vIxW6UTeg
- Industrial Cyber: CIE and CCE Methodologies Can Deliver Engineered Industrial Systems for Holistic System Cybersecurity (June 11, 2023) with interviews from INL, 1898, and West Yost
- Harvard Business Review: Engineering Cybersecurity into U.S. Critical Infrastructure (April 17, 2023) by Ginger Wright, Andrew Ohrt, and Andy Bochman
- For more CIE articles and publications, visit: inl.gov/cie

Procurement

Leveraging Procurement for Cybersecurity Resilience

- Security Scorecard: https://securityscorecard.com/security-rating/[insert domain name of supplier]

- UpGuard: https://webscan.upguard.com/
- EEI, Model Procurement Contract Language Addressing Cybersecurity Supply Chain Risk, Version 3.0, October 2022

Coordinating Cybersecurity Risk Management with Hardware/Software Vendors

- U.S. Treasury, Office of Foreign Assets Control, Sanctions List Search
- United Nations Security Council Consolidated List
- NIST National Vulnerability Database
- Catalisto, Vendor Risk Analysis Template (xlsx)

Appendix C: List of Webinars

Risk Management

The Emerging Cyber Threats to Industrial Control Systems (ICS) – Supply Chain Cybersecurity

Presenter:

- **Camilo Gomez**, Global Cybersecurity Strategist, Yokogawa

Webinar Recording | Presentation Slides

In a world of increasing global cybersecurity threats, organizations need to understand the nature of the threats, as well as to recognize the role that organizations play in end-to-end supply chain cybersecurity in responding to them. Critical infrastructure like energy utilities often lack a workforce with specialized skills needed to address cyber security.

Standards on Third-Party Risk Management and Cyber Risk Assessment Methodologies

Presenters:

- **Frances Cleveland**, President and Principal Consultant, Xanthus Consulting International
- **Gigi Pugni**, START 4.0 Competence Center

Webinar Recording | Presentation Slides

Internationally accepted standards and guidelines support identifying and managing cybersecurity risks associated with the supply chain risk from third parties/suppliers. A survey of these resources (e.g., the U.S. National Institute of Standards and Technology [NIST] Cybersecurity Framework, NIST SP 800-161, ISO/IEC 27036-1:2021, NISTIR 8276) is presented.

Conducting Cyber Risk Assessments for Supply Chain Risk Management

Presenters:

- **Frank Honkus,** Associate Director of Intelligence Programs / Director of the Cybersecurity Risk Information Sharing Program (CRISP), E-ISAC
- **Mikhail Falkovich,** Chief Information Security Officer, Con Edison

Webinar Recording | Presentation Slides

This section examines risk management practices for supply chain related cybersecurity risks, including considerations for supply chain vulnerability management and equipment country-of-origin. Risk management implies understanding threats, vulnerabilities, and potential impacts. Effective risk management also addresses prioritization, developing projects to mitigate risks, and evaluating the effectiveness of mitigations.

Asset Management

Best Practices for Secure Remote Access and Cloud Security in the Electricity Sector

Presenter:

- **Justin Searle**, Director of ICS Security, InGuardians

Webinar Recording | Presentation Slides

Remote access has become a requirement for many organizations, including electric utilities. In addition, cloud services have been used more and more for certain applications. This webinar presented best practices for secure remote access (e.g., by equipment suppliers for monitoring and maintenance) as

well as the considerations needed to implement cloud services. This webinar delved into how utilities are using remote access and cloud services, what are the risks, what is the software lifecycle (e.g., challenges of onboarding and offboarding cloud-based services), how to do it securely now and in the future, and how to deal with changes on the supplier side.

Defensible Architecture and Asset Management for Electric Utility Cybersecurity

Presenters:

- **Markus Mueller**, Principal Industrial Consultant, Dragos
- **Jason Shea**, Senior Cybersecurity Manager, Southern California Edison

Webinar Recording | Presentation Slides

Shifting to a defensible architecture model allows utilities to use an intelligence-based approach to protect their assets from the risks that cyber threats present today. A defensible architecture is not a static design but a process of deploying people, processes, and technology that any utility can follow for more effective asset protection. This practice includes asset management efforts to understand what needs to be protected and what capabilities exist within the environment. The webinar covered best practices for utilities when developing defensible architecture and conducting asset management, addressed the difference between planning for security during new deployment versus reviewing and improving existing ICT networks, network and access control, network configuration, onboarding, and offboarding third-party suppliers for on-premises software/hardware.

Governance, Policies and Planning

Cybersecurity Incident Response Plan Development

Presenters:

- **Michael Martin**, Control Systems Engineer, Chelan County PUD
- **Tony Assan**, Head of IT, GRIDCo (Ghana)

Webinar Recording | Presentation Slides

An incident response plan (IRP) is an essential tool for utilities to prepare for an event and can help drive the utility's overall cybersecurity activities. This webinar discussed how utilities should incorporate supply chain cybersecurity considerations into an IRP. Important steps include identifying scenarios, identifying critical utility systems/assets, identifying supporting systems/assets, calculating business impacts, using existing risk analysis, and developing and testing playbooks. This webinar also discussed key strategies to testing and improving the incident response plan and highlighted several useful resources to developing the IRP.

Governance Policies and Procedures for Third-Party Cybersecurity Risk Management

Presenters:

- **Terri Khalil**, Senior Consultant, Ampyx Cyber (formerly Ampere Industrial Security)
- **Roland Miller III**, Ambassador for Cyber Florida, The Florida Center for Cybersecurity

Webinar Recording | Presentation Slides

This webinar focused on developing and maintaining organizational cybersecurity governance and the best practices on policies and procedures to address supply chain risk management. The webinar highlighted typical models for managing cybersecurity (e.g., the role of a CISO or CSO) and level of visibility into cybersecurity risks from the senior management to technical staff. The presenters also discussed strategies and approaches to communicating not only within an organization about cyber risks,

but also with regulatory authorities, especially in support of review and approval of CAPEX and OPEX cyber investments.

Managing Cybersecurity Risks in a Rapidly Expanding Electric Grid

Presenters:

- **Anuj Sanghvi**, Researcher III-Cyber Security & Resilience, NREL
- **Ginger Wright**, Cyber-Informed Engineering Program Manager, INL

Webinar Recording | Presentation Slides

As utilities rapidly expand electric grids and prepare for transitions from centralized to distributed grids and create new interconnections, consideration of cybersecurity requirements is paramount. Transmission system operators, distribution system operators, and market operators must incorporate distributed energy resources into the electric grid and accommodate independent power producers, generally, but this creates new communication and control requirements which must be secure. This webinar addressed considerations for security of integrations between transmission, distribution, and market operations systems through Cyber Informed Engineering (CIE) and applying the Distributed Energy Resources Cybersecurity Frameworks (DERCF).

Procurement

Leveraging Procurement for Cybersecurity Resilience

Presenters:

- **Frank Harrill**, Vice President of Security, SEL, Inc.
- **Jacob Phillips**, Senior Corporate Counsel, MISO

Webinar Recording | Presentation Slides

This webinar focused on how procurement in the energy sector can be leveraged to strengthen cybersecurity across TSOs, DSOs, and generation. Topics explored included how systems associated with managing energy infrastructure, like SCADA and other industrial controls systems, energy market applications, advanced metering infrastructure and billing systems can be made more resilient by embedding cybersecurity specifications in procurement. Speakers considered how existing standards can be implemented to guide procurements through the lifecycle of operations.

Coordinating Cybersecurity Risk Management with Hardware/Software Vendors

Presenters:

- **Claudia Iannazzo**, CEO and Founder, Catalisto
- **Sokol Mukaj**, Chief Information Officer, KESH (Albania Power Corporation)

Webinar Recording | Presentation Slides

This webinar focused on the remaining lifecycle of the operation of critical IT and OT systems in a utility. Whereas the previous webinar (Leveraging Procurement for Cybersecurity Resilience) focused on preparing for procurement and conducting procurement/reviewing proposals, this webinar discussed the process of negotiating contracts and maintaining the relationship with the vendor throughout the lifecycle of operations (e.g., receiving and applying patches), and offboarding vendors as needed.