NAVIGANT

ENERGY

BEST PRACTICES FOR UTILITY CYBERSECURITY

Prepared by Doug Morrill, Associate Director and Sam Crawford, PhD, Managing Consultant, Navigant Consulting, Inc. May 2017

GENERAL DISCLAIMER:

This presentation was prepared by Navigant Consulting, Inc. (Navigant) for informational purposes only. The term "best practices" is used to reference practices which the authors currently believe to be generally accepted and recommended practices, and the views expressed in this paper are those of the authors and do not necessarily represent the views of Navigant. Further, Navigant does not make any express or implied warranty or representation concerning the information contained in this presentation, or as to merchantability or fitness for a particular purpose or function.

The intended audience for this guide includes network engineers, cybersecurity professionals, cybersecurity program managers and others that are interested in a general overview and comment on the highlights of cybersecurity for the utility industry. It assumes a reasonable level of general network architecture and administration as well as basic understanding of the major components of electric utility information and operations technology. The guide is not meant to be comprehensive or to be used as the foundation for a robust and complete cybersecurity program.[1]

1. This paper includes a high-level overview of best practices from various existing standards and includes Navigant's unique, informed analysis and interpretation of the frameworks in the context of current security threats in the industry and future technologies. These standards include the North American Electrical Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) requirements, the National Institute of Standards and Technology (NIST), the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), and others.

INTRODUCTION

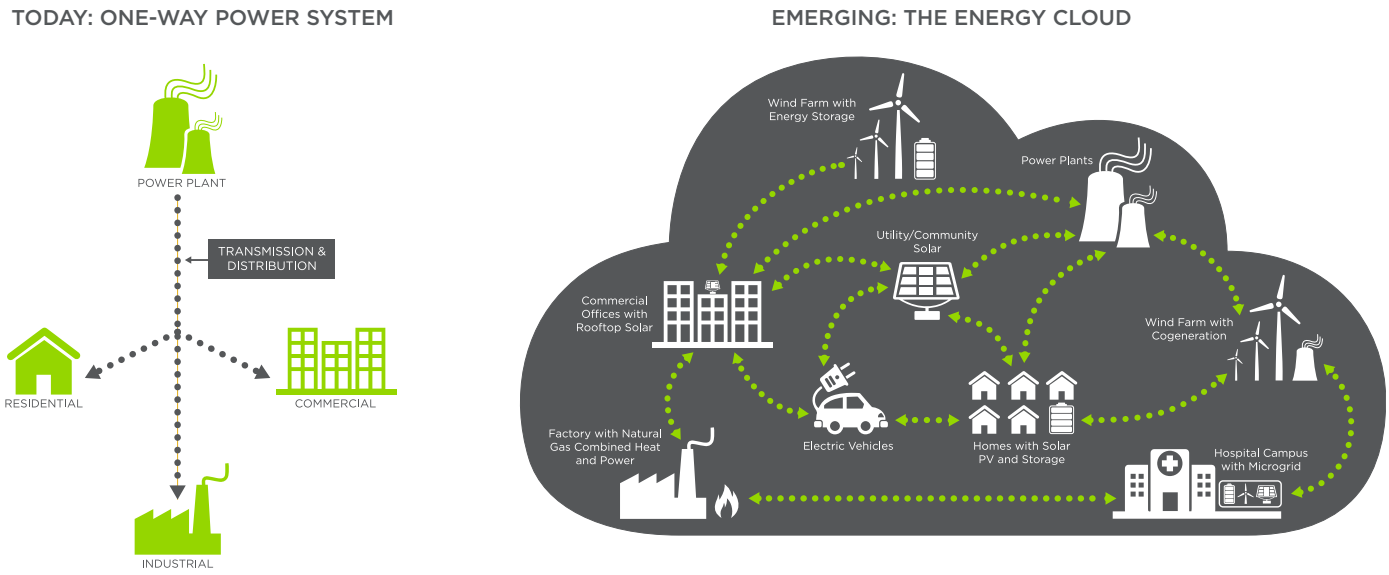
One of the key challenges utilities face as they work to keep pace with the industry's transformation is protecting the security of their critical infrastructure. As utilities develop more interconnected systems that make the grid smarter, more efficient, and more versatile, they also introduce cybersecurity vulnerabilities that bad actors may exploit. Recognizing these issues, regulatory and standards organizations such as the North American Electric Reliability Corporation (NERC) have developed cybersecurity requirements for electric utilities to ensure protection of critical infrastructure—notably NERC's Critical Infrastructure Protection (CIP) standards.

This white paper discusses the cybersecurity challenges utilities will likely experience, as well as best practices for protecting critical infrastructure and ensuring compliance with cybersecurity standards and requirements.

GROWING CYBERSECURITY THREATS

The emerging Energy Cloud (Figure 1) is driving a dramatic transformation of the electric utility industry. Utilities, accustomed to the traditional model of one-way power flow from centralized generation, are working to adapt to a new model with two-way power flow from distributed energy resources (DER). To maintain high reliability with greater quantities of intermittent renewable generation and provide customers with improved services and power options, utilities are rapidly deploying smart grid systems that are more digital and interconnected with systems both inside and outside of their organization.

Figure 1. The Emerging Energy Cloud



Source: Navigant

Two prime examples are the advanced distribution management system (ADMS) and the demand response management system (DRMS). An ADMS merges the functions of distribution management systems with outage management systems and may include volt/volt-ampere reactive (Volt/VAR) optimization (VVO), workforce management, a customer information system (CIS), and geographic information systems. This high degree of interconnectedness provides conduits for hackers to exploit by gaining entry into one system, they may find pathways into another.

The DRMS also integrates with these types of systems to help utilities more effectively and economically balance supply and demand by leveraging customer-sited DER. Specifically, the DRMS blurs IT and OT functions so much so that utilities utilize vastly different models to manage it within their organization. Furthermore, the DRMS communicates with demand response (DR) enabling devices such as programmable communicating thermostats. These devices have a heterogeneous mix of protocols and encryption methodologies that have different cybersecurity maturity profiles and often lack both the physical security and cybersecurity afforded by typical utility systems and devices, making them an easy target for hackers. These Internet of Things (IoT)-type devices, including smart washing machines, dryers, and EVs, are the gateway to an increasingly intelligent and vulnerable grid. Over the past several years, industry experts have raised warnings regarding the lack of basic security in IoT devices. While Congress has mandated the deployment of real-time DR technology and integration of smart appliances and consumer devices, recent events confront us with the fact that we are woefully unprepared. Thousands of baby monitors, home surveillance cameras, printers and other IoT devices were exploited to launch a DDoS (Denial of Service) attack[2] that severely impacted dozens of sites including the BBC, the Wall Street Journal, Visa, HBO, Netflix and the Swedish Government. It is clear that current generation IoT demonstrates that demand-side technology lacks the cybersecurity maturity expected for utility-critical infrastructure security.

Utility Cybersecurity Trends

A recent survey compiled by one of the leading vendors in cybersecurity, Tripwire, found that over the last year almost all utility Chief Information Officers and Chief Security Officers felt that cybersecurity threats have increased. Not only are the threats more common, they are becoming increasingly successful. There is also decreasing confidence that the systems they have in place to control cyber threats can do the job. It is against this background that the need to have more secure and resilient energy systems is becoming imperative.

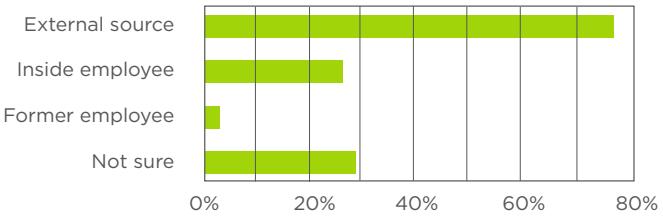
Key Risks

Attackers search for potential weaknesses, exploit those weaknesses to get into the system, and then may perform a variety of harmful activities after gaining access. Once hackers are inside the system, they may continue to operate for many months before their actions are noticed.

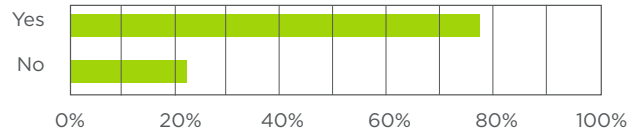
The current threat landscape includes individuals executing attacks for monetary gain as well as nation-state and terrorist threat actors capable of executing powerful cyber attacks to achieve political agendas. Hackers may access sensitive customer information or embarrassing company information and then extort the utility in return for disclosing the vulnerability or simply agreeing to not disclose the information publicly. The greatest risk for utilities is command and control over utility infrastructure, which can cause widespread blackouts. In December 2015, electric utility workers in Ukraine watched helplessly as cursors moved across their workstation screens at an intruder's commands shutting down substations. Other hidden commands destroyed vital equipment. According to Robert Lipovsky, a cybersecurity analyst who examined the Ukraine case, the events showed "that things such as this aren't just theoretically possible...that things like this can happen." Lipovsky also said, "It shouldn't have been so easy for the attackers."

Figure 2. Utility Cybersecurity Trends

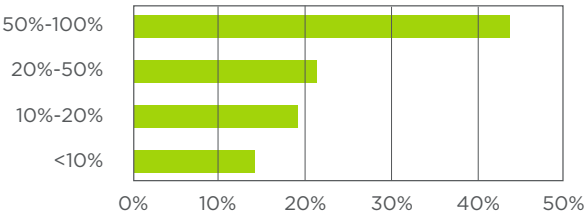
Over the past 12 months, has your organization experienced an attach from any of these sources? Choose all that apply.



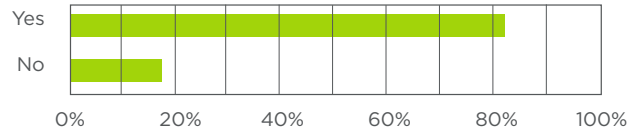
Has the number of successful cyberattacks your organization has experienced increased in the past 12 months?



How much has the rate of successful cyberattacks increased in the past month?



Do you believe a cyberattack will cause damage to critical infrastructure in 2016?



Source: 2016 Tripwire Utility Survey

2. Dyn DDoS 10/21/2016

With more digital, interconnected systems exchanging sensitive data, each attack can have profound consequences, particularly given the convergence of IT and OT systems. On Friday, October 23, 2016, many popular Internet sites could no longer be reached, including Amazon, Twitter, and Spotify. Others had noticeable difficulties, including Netflix, PayPal, CNN, and Fox News. In all, over 35 major websites—all using Dyn to help deliver Internet services—were impacted. A single individual targeted Dyn for this cyber attack and managed to hack into tens of thousands of IoT devices and take them over.

BEST PRACTICE METHODS

Effective utility cybersecurity requires not only strong technical controls—software and hardware components used to prevent, detect, and address cyber-attacks—but also effective cybersecurity management practices. While cybersecurity controls have become increasingly advanced, hackers continue to find new exploits and strategies to circumvent these controls, which requires that utilities continuously monitor and improve their controls. Furthermore, cyber attacks are nearly inevitable, which means that utilities need to not only put up strong defenses but also have plans and procedures in place for how to effectively manage attacks when they occur.

Cybersecurity Frameworks

To assist utilities in addressing growing cybersecurity threats, organizations have established frameworks to help guide them in protecting their critical infrastructure. The leading international frameworks include the following:

- The **National Institute of Standards and Technology (NIST) Cybersecurity Framework** includes specific information and guidance for implementing cybersecurity controls and practices for a number of different industries and situations. It is particularly useful for logically *identifying and implementing cybersecurity procedures and controls.*

- The **Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)** provides a framework for auditing a cybersecurity program to *assess the effectiveness of the procedures and controls that have been employed.*

- The **NERC CIP** framework supports the *ongoing operation and maintenance of cybersecurity procedures and controls for the electric utility industry.*

- The **ISO/IEC 27000 Series** of standards covers a wide and inclusive body of guidelines including privacy, confidentiality, IT, technical, and cybersecurity subjects. Like NERC-CIP, this framework *incorporates continuous feedback and improvement activities to respond to changes in the threats and vulnerabilities.*

The NIST Framework consists of five concurrent and continuous functions: Identify, Protect, Detect, Respond, and Recover. It also consists of four tiers (Partial, Risk-Informed, Repeatable, and Adaptive) to describe the degree to which an organization's cybersecurity risk management practices have matured and meet the content of the Framework. Profiles can be used to identify a current profile (the "as is" state) and a target profile (the "to be" state). This risk-based assessment based approach provides a standardized methodology to support informed prioritization and serves as a reliable means for measuring progress toward an Adaptive, or fully mature, target profile.

The ES-C2M2 helps utilities determine which security controls need to be implemented or improved. The intent of a C2M2 exercise is similar to the use of NIST Framework profiles, but it is intended to be a comprehensive and enterprise-wide measurement tool centered around 10 competency areas. The C2M2 evaluation process defines how the competencies are measured and how data collected during the evaluation should be analyzed and scored. The ES-C2M2 evaluation is designed to assist organizations in identifying specific areas to strengthen their cybersecurity program, prioritize cybersecurity actions and investments, and maintain the desired level of security throughout the IT/OT systems' lifecycle.

NERC is responsible for working with utility companies to develop and implement CIP standards and enforcing compliance with those standards. The standards assess resource adequacy and provide educational and training resources as part of an accreditation program to ensure power system operators remain qualified and proficient. NERC also investigates and analyzes the causes of significant power system disturbances to help prevent future events. The CIP lifecycle approach is segmented into six areas of activity: Analysis and Assessment, Remediation, Indications and Warnings, Mitigation, Incident Response, and Reconstitution. The first three activities take place prior to any actual event or incident. The last three activities take place during and after a cybersecurity event.

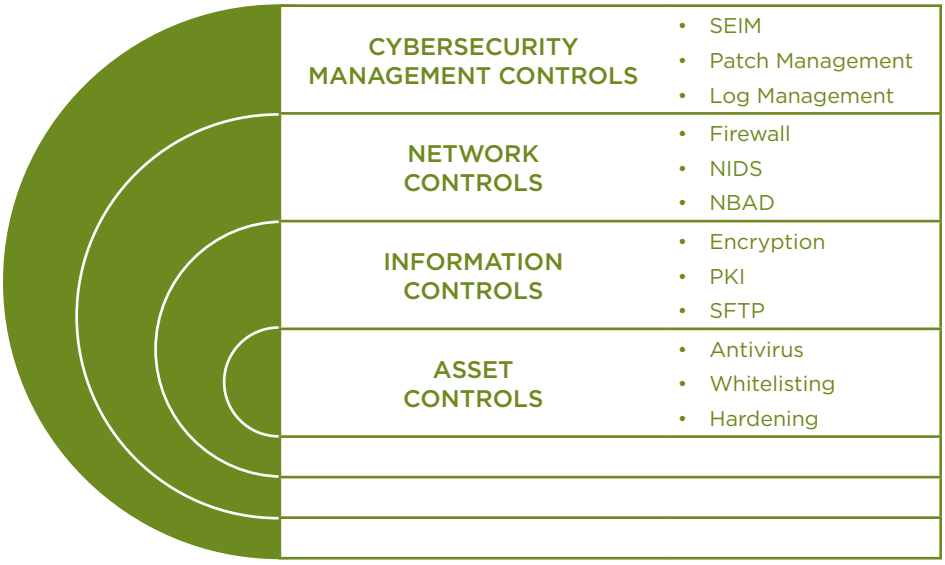
The ISO/IEC 27000 series is a subset of a larger and comprehensive set of guidelines that together make up the world's largest body of international standards. It is intended to provide a common set of standards between nations. The International Organization for Standardization (ISO) publishes international standards—almost 20,000 standards covering a wide variety of topics—for the private sector. These standards are developed by specialist expert groups made up of members from business, industry, government, academia, consumer, and other relevant groups.

Cybersecurity Controls

A strong cybersecurity approach uses a "defense in depth" (Figure 3) with multiple layers of cybersecurity controls that provide overlapping protection, including:

1. **Asset controls:** Measures including server and desktop hardening, antivirus, and whitelisting to improve the resiliency of systems if attacked
2. **Information controls:** Protections for information at rest and in transit from unauthorized access through data or communications encryption
3. **Cybersecurity management controls:** Tools and processes to monitor systems and networks, ensure continuous compliance with cybersecurity standards, and address any potential cybersecurity threats
4. **Network controls:** Measures to manage and protect data transmission across networks, including managing the ability of different users to gain access to sensitive systems and data compliance with cybersecurity standards, and address any potential cybersecurity threats

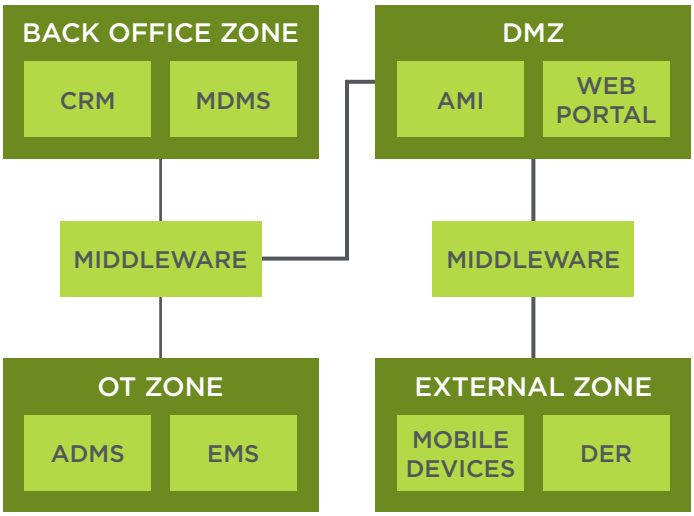
Figure 3. Layers of Defense



Source: Navigant

Highly interconnected systems require segmentation into different cybersecurity zones. Assets and controls are grouped together for multiple systems with similar vulnerabilities that require similar cybersecurity controls. Figure 4 provides an illustrative example of such segmentation. In this example, the back-office zone contains systems that are housed on the utility's internal network, while the de-militarized zone (DMZ) contains systems that communicate with those systems and devices in the external zone. The DMZ requires more stringent controls than the back-office zone because its systems interface with systems outside of the utility's network and control, thus presenting greater risks for both physical security and cybersecurity. The OT zone requires the most stringent controls, as it houses the utility's most critical infrastructure. The safest approach for the OT zone is to have it completely air-gapped so it does not interface with systems outside the zone. However, the smart grid capabilities are more limited in that case, which why many utilities are embracing the convergence of IT and OT.

Figure 4. Cybersecurity Zones



Source: Navigant

Cybersecurity Management and Audit Programs

A secure network architecture that integrates cybersecurity controls requires a defined set of activities and procedures that support the day-to-day operations of the enterprise. At the highest level, executive leadership sets policies for the organization. These policies form the foundation on which specific procedural business functions are created.

A common concern for management is how the company knows that its procedures are working as intended and are fulfilling the intent of company policy. Audit frameworks have been developed to use standard evaluation processes created to deliver consistent results across different organizations.

The US Department of Energy (DOE) developed ES-C2M2 at the request of the White House specifically as an audit tool. The DOE, Department of Homeland Security, and private sector experts developed it to address the unique characteristics of the electricity subsector. ES-C2M2 allows for effective and consistent benchmarking of a company's capabilities and is just one of many other audit frameworks such as CoBIT and IEC 27002 that have a broader cybersecurity focus.

The NERC-CIP standards are the mandatory standards formed though an alliance of industry and government. These standards provide a framework tailored specifically for the electric utility industry. As there are mechanisms that include stiff fines for non-compliance, it is generally the set of rules most people worry about when discussing generation, transmission, and distribution cybersecurity. It is important to understand that CIP is not just about how to implement cybersecurity, it is also about the process a utility should follow to accomplish a secure outcome. The guidelines are set up to ensure that utilities create specific policies and procedures that result in effective programs for meeting stated objectives. The criteria have evolved over time and sections have been retired and replaced as new criteria come into play. As a rule, the United States and Canada are focused on these regulations. Mexico also recently expressed interest to NERC officials in adopting this set of standards.

CONCLUSION

This white paper focused on the three main elements of modern cybersecurity, the new triad: frameworks, controls, and management/audit programs. Many readers recall C-I-A as the founding principal triad: confidentiality, integrity, and availability. This cornerstone concept imbued the notion that cybersecurity is not a concrete formula or goal. It is a balance that must be struck between different objectives: data must be secured; it may not be tampered with; and it can be accessed when needed by the right person. The best outcome is to achieve a state of optimal efficiency such that any reallocation reduces the sum of the whole.

The NERC-CIP framework is mandatory for many utilities and it is not always easy to discern a clear path forward towards preparing for the new energy marketplace while maintaining compliance. This set of standards has evolved from a compliance and audit perspective and uses a divergent vocabulary that can oftentimes be difficult to interpret for the uninitiated. It is important to recognize that NERC-CIP represents a set of legally binding standards, and audit failures carry significant fines that can run into the millions of dollars. These facts can force one to view the entire subject of cybersecurity with a somewhat different set of optics. The focus can shift toward policy and procedure paperwork that supports compliance with a specific set of actions defensible within the language of the guidelines as opposed to interpreting the guidelines as a set of objective outcomes that require the cybersecurity practitioner to not only meet the letter of the regulation but also the spirit of it.

To combat this, utilities can reference NIST or ISO standards in their CIP documentation as evidence of best practices to help inform and improve their program. In addition to the exercises required under CIP, performing a periodic C2M2 can help provide an independent confirmation of the overall health of a cybersecurity program to utilities.

When discussing the new triad of frameworks, controls, and management, the idea of an optimal balance between the three disciplines is a valuable notion to keep in mind. Frameworks must provide an integrated and coherent approach to current and future best practices and procedures. Cybersecurity controls must provide multiple layers of defensive technology. Most importantly, integrated compliance and audit and management practices that combine the strengths of NIST and ISO with NERC-CIP policies and procedures must be developed.

For the smart grid to evolve, everyone that works in securing these systems under NERC-CIP is going to have to do a better job at getting to know their colleagues—compliance and audit, operations, systems management, and finally, the people in the SOC (security operations center) that must deal with the real-time cybersecurity threats daily. The professional cybersecurity expert of tomorrow is going to have to know more than just one discipline. To be successful, the industry is going to need to put an emphasis on developing interdisciplinary teams that can develop integrated solutions to handle the complex challenges of the industry's current transformation from unidirectional electric supply grids to highly complex "meshworks" of energy actors.

We at Navigant recognize that utility industry cybersecurity is a unique challenge. We have helped our clients learn how to productively manage the competing requirements and priorities that face transmission and distribution operators, regulatory and compliance staff, and the IT and OT technical experts that build and maintain these increasingly complex systems. Our goal is to build the bridges within your organization and fill the gaps where required. Our team can help you bring together the cybersecurity resources you need in place today to plan for tomorrow. If you are not thinking about DR-driven technologies, integrated microgrids, home-based renewable generation and storage, energy aggregators and transactional brokers, and the explosion of IoT devices underway, give us a call today and start the conversation.

CONTACTS

DOUG MORRILL, CISSP

Associate Director
860.874.5181
Doug.Morrill@Navigant.com

MATT BLIZARD, PE

Director
360.464.3944
Matthew.Blizard@Navigant.com

KEN LOTTERHOS

Managing Director
631.678.7302
Ken.Lotterhos@Navigant.com

navigant.com

About Navigant

Navigant Consulting, Inc. (NYSE: NCI) is a specialized, global professional services firm that helps clients take control of their future. Navigant's professionals apply deep industry knowledge, substantive technical expertise, and an enterprising approach to help clients build, manage, and/or protect their business interests. With a focus on markets and clients facing transformational change and significant regulatory or legal pressures, the firm primarily serves clients in the healthcare, energy, and financial services industries. Across a range of advisory, consulting, outsourcing, and technology/analytics services, Navigant's practitioners bring sharp insight that pinpoints opportunities and delivers powerful results. More information about Navigant can be found at navigant.com.

linkedin.com/company/navigant

twitter.com/navigant