Utility Security: Exceeding Mandates to Mitigate Risk

A Greentech Media White Paper

Sponsored by

intel | cisco

gtm:

TABLE OF CONTENTS

Introduction 3

What Makes Utility Security Unique 4

Utility Cybersecurity Regulations: Compliance and Beyond 6

Key Insights and Best Practices for an Effective Utility Security Program 8

Cybersecurity and the Utility Supply Chain 11

Conclusion 13

CHAPTER 1

Introduction

Security is more than just a regulatory-driven necessity for utilities; it has become a business imperative. Most utilities can no longer do business effectively or efficiently without internet-of-things (IoT) technology; and recent events in the Ukraine have shown that large-scale attacks against power grids can succeed. Beginning July 1, 2016, U.S. utilities must comply with NERC's Critical Infrastructure Protection standard, v6, which features an expanded scope and greater emphasis on security, compared to previous NERC CIP regimes. Most utilities in the U.S. already possess a relatively high level of awareness and sophistication about cybersecurity, compared to other industries — but there are some common weak spots. To respond effectively to ever-shifting cyber threats and vulnerabilities, utilities must adopt a risk-based security approach that exceeds regulatory requirements. This paper recommends an integrated utility security program that encompasses physical and digital security technology, staffing and training, leadership support, cross-departmental collaboration and cross-sector coordination.

CHAPTER 2

What Makes Utility Security Unique

Utilities are especially popular, high-profile targets for cyberattacks. According to the Cisco Security Capabilities Benchmark Study 73% of utility IT security professionals say they've suffered a security breach, compared with an average of 55% in other industries. Yet Intel's Andrew Johnston recently found that cybersecurity didn't make the top-five list of utility executive technology priorities for 2016.

The threat to utilities became reality on December 23, 2015, when a coordinated cyberattack caused a six-hour outage in eastern Ukraine, affecting hundreds of thousands of customers in 103 cities and towns. This attack was enabled by malware introduced onto the utility's network months earlier via phishing.

How much damage might a cyberattack against U.S. electric power systems cause? In its 2015 modeling of a large-scale coordinated cyberattack on Northeastern U.S. utilities (improbable, but technically possible), Lloyds of London estimated economic impact from $243 billion to $1 trillion, with power restoration likely taking up to several weeks in some locations.

Most U.S. utilities have already undertaken substantial cybersecurity measures throughout many parts of their systems, and indeed, utilities tend to be more sophisticated about cybersecurity than many other industries. However, the landscape of cyber threats and vulnerabilities is constantly changing.

The legions of new network connections to more devices in more parts of utility power system enhance grid reliability, improve integration of renewables and other distributed energy resources, and help control operating costs, among other operational benefits. But there are tradeoffs — notably, increased complexity and new security challenges. Every network-connected device represents a potential entry or execution point for a cyberattack by insiders, criminals, terrorist groups or nations.

The following aspects of how utilities operate make this sector somewhat unique in terms of security:

- Geographic distribution. Very few industries control such a widely distributed infrastructure that connects so directly with consumers. Consequently, when there is a utility system failure, the impact to, and feedback from, customers is immediate and harsh. Often, failures rapidly bring about increased scrutiny from regulators and the media.
- Fast-growing networks. With the advent of smart grid and IoT technology, many utility OT departments are now managing networks far larger than their IT departments ever had to. Furthermore, efficiently managing and analyzing the volume of data that such a vast network generates is a considerable leap for many utilities. Thus, many utilities are challenged by the scale of securing IoT-enabled utility systems. They need security solutions that can be applied cost-effectively across hundreds of thousands, or even millions, of nodes.

This highlights the value of bridging the traditional organizational divide between utility IT and OT departments. Both types of teams can benefit by working with, and understanding, each other's priorities, policies, and perspectives. Such an approach is outlined in a recent Cisco white paper on IT/OT convergence for electric utilities.

- Training. The IoT technology now widely deployed at utilities often exceeds the skill set of the majority of utility workers. Many of the utility staff and contractors who work directly or indirectly with IoT devices know their own tasks, but they don't necessarily understand related security implications.

- Interconnections and information sharing between utilities. The interconnected nature of the power grid, especially for high-voltage bulk power transmission networks, presents another unique cybersecurity twist.

In a sense, the U.S. power grid is one giant machine encompassing thousands of operating entities. Adjacent power providers must coordinate and connect with each other, to keep the grid balanced and support mutual aid efforts. Utilities already provide mutual assistance when recovering from large-scale outages caused by severe weather or natural disasters; such cooperation can also apply to protection, response, and recovery from cyberattacks.

The utility sector is expanding its own systems for sharing information about possible cyber threats across the sector, in order to promote common awareness. NERC is supporting this practice with its nascent Cybersecurity Risk Information Sharing Program (CRISP). However, there are other cyber risk information-sharing services not limited to the utility sector, such as alerts from the U.S. Computer Emergency Readiness Team (CERT), part of the Department of Homeland Security. Utilities can benefit from subscribing to, or participating in, such information-sharing programs.

- Budget. Regulated utilities can decide how to deploy their resources and reprioritize investments internally, but often they cannot easily transfer these costs to customers. Unlike private companies, investor-owned regulated utilities must ask for permission to raise prices — a notoriously slow process. The typical regulatory cycle for non-emergency utility rate increases can last from three to six years.

In general, state public utility commissions regulate rates, not security. However, PUCs have jurisdiction over regulated operations in-state, mandating renewable energy projects and other activities and financial decisions through what they allow in the rate base. When utilities seek rate relief for security compliance, they still must justify those expenditures to regulators and ratepayers.

Meanwhile, at the federal level, regulatory requirements for utility cybersecurity are increasing. More parts of utility operations (such as substations) are falling under the scope of compliance. This means that utilities no longer have the option of deferring substantial investments in cybersecurity upgrades. They must deploy their existing budget and resources to mitigate these risks effectively today.

In addition, there are some considerations that affect cybersecurity and that are crucial to utilities, but not necessarily unique to the utility industry.

- Third-party access. Utilities are increasingly reliant upon third parties to maintain the operational health of their equipment. This typically requires internet-based access to that equipment. Such third-party remote access introduces complexities for access control. Also, personnel who are issuing commands to devices might be less aware of critical context, such as unusual local conditions, planned downtime of related equipment, etc.
- Preventing errors and accidents. Most instances of human-caused utility system downtime result from automobile accidents, not malicious attacks. Still, errors and accidents can resemble attacks, since the consequences are often the same. Thus, effective cybersecurity offers the considerable added benefit of helping to protect utility systems from dangerous errors, such as commands that might exceed design parameters, fail to account for unusual current circumstances, or violate operational policies.

CHAPTER 3

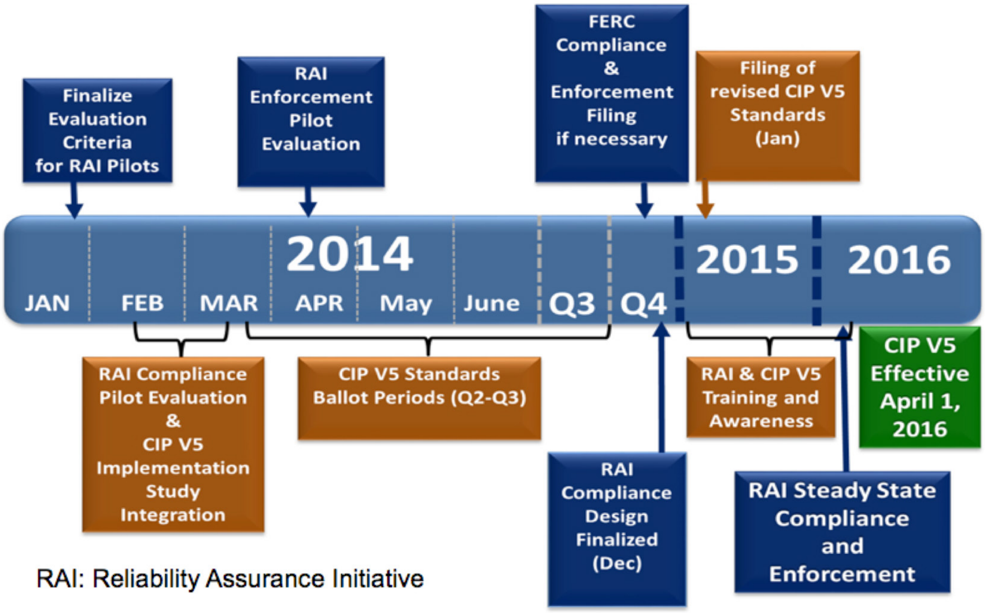
Utility Cybersecurity Regulations: Compliance and Beyond

New federal cybersecurity regulations for the bulk power grid are taking effect this year. As of July 1, 2016, U.S. utilities are required to be in compliance with the North American Electric Reliability Corporation Critical Infrastructure Protection v5/6 standard.

Unlike previous prescriptive CIP standards, v5 (and now v6) takes a risk-assessment-based approach: utilities must assign a risk level to all bulk power system assets and devise a compliance plan. This includes all substations, which were not always included under previous NERC cybersecurity standards.

Developing a NERC CIP compliance plan represents a valuable opportunity for utilities to gain a deeper understanding of their security priorities — including the areas where cybersecurity intersects with organizational governance, and how cross-departmental coordination and collaboration might help enhance overall security. This points to a holistic approach to security — not only across technologies, but throughout the organization.

Figure 3-1: CIP V5 transition timeline


Finalize Evaluation Criteria for RAI Pilots
RAI Enforcement Pilot Evaluation
FERC Compliance & Enforcement Filing if necessary
Filing of revised CIP V5 Standards (Jan)
2014
2015
2016
JAN
FEB
MAR
APR
May
June
Q3
Q4
RAI Compliance Pilot Evaluation & CIP V5 Implementation Study Integration
CIP V5 Standards Ballot Periods (Q2-Q3)
RAI Compliance Design Finalized (Dec)
RAI & CIP V5 Training and Awareness
CIP V5 Effective April 1, 2016
RAI Steady State Compliance and Enforcement
RAI: Reliability Assurance Initiative

Source: Greentech Media

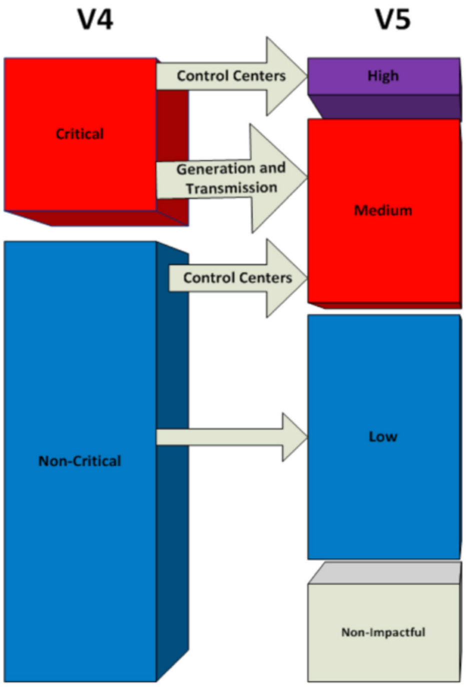
Version details aside, the current iteration of NERC CIP represents a substantial shift in how utilities are required to address cybersecurity. Rather than a prescriptive approach with predetermined measures, utilities must now take a risk-assessment-based approach, and devise their own plan to achieve compliance. Risk-based security offers these benefits:

- Greater efficiency through safer automation of formerly manual processes. This saves time and money.
- Increased system reliability and customer satisfaction. Security controls not only impede attacks, but they also guard against errors and accidents. This can help minimize damage while speeding up response and recovery — which helps keeps the lights on, pleasing customers and regulators.
- Reduced liability. Insurance providers and legal departments are increasingly wary of cybersecurity risks. Proactive, comprehensive cybersecurity can help mitigate their concerns and reduce associated costs or losses.

Risk-based security mainly boils down to the difference between telling utilities what the goal is, rather than how to achieve that goal. The shift from "how" to "what" requirements may help utilities focus on security, rather than paperwork. For instance, under previous NERC CIP regimes, utilities were often required to use antivirus software. The current CIP changes this to a requirement for malware protection.

Also, the current CIP requires utilities to inventory each asset associated with their bulk power grid and rate it as having low, medium or high potential impact. Consequently, several utility assets that previously were deemed non-critical (including some smaller substations) must now be brought into compliance. Previously, some utilities claimed to have few or no critical bulk power system assets. Today, cybersecurity is required for every substation — it's just a matter of how much.

Figure 3-2: Categorizing assets as part of new NERC CIP standards



Source: Greentech Media

Inventorying and categorizing these assets is specified in CIP-002. Also, there are tools, guidance and consultants available to support utilities in this process, as well as in developing their compliance plan.

Equipment vendors are starting to offer technologies tailored to support NERC CIP compliance. For instance, Cisco offers a Substation Security Solution which offers utility-specific switching with its ISA-3000 security appliance additional capabilities such as VPN and intrusion prevention for SCADA. Both are properly ruggedized for operation in harsh environments with high electromagnetic interference.

Protecting distribution grids. Distribution grids are not covered by NERC CIP; they are regulated mostly by a complex patchwork of state and local authorities. This gap in regulatory coherence is yet another reason why utilities may wish to take the initiative to adopt a comprehensive program for grid security that looks beyond regulatory mandates to achieve greater operational and business benefits.

A notable benefit of NERC CIP compliance is that measures implemented for bulk power grid assets can also be voluntarily applied to local distribution grids — minus the cost and labor of regulatory paperwork. Doing this can be beneficial, since hackers and saboteurs probably don't distinguish much between distribution and bulk power systems. Also, within a utility's infrastructure, the line between these systems is blurred, since many substations include both transmission and distribution assets.

CHAPTER 4

Key Insights and Best Practices for an Effective Utility Security Program

Since threats evolve constantly, utilities need an agile mindset in order to mount an effective — and cost-effective — security response. Across many industries, risk assessment has become a foundational security practice. Historically, utilities have tended to pursue more prescriptive (and thus predictable) security strategies. Predictability and homogeneity tend to facilitate, rather than thwart, cyberattacks. As such, the risk assessment focus of the current NERC CIP can be a helpful catalyst to shift this mindset.

Compliance does not guarantee security. Regulatory mandates create a useful baseline across an industry, but attackers are constantly seeking, and finding, new vulnerabilities. Consequently, a narrow focus on regulatory compliance can yield complacence and overconfidence in a utility's security program.

Following are several processes and practices for utilities to consider as they enhance their security programs.

Cross-departmental leadership and collaboration. In large measure, cybersecurity is about people, not technology — which means people are a critical part of the solution. One exceptionally effective, though not necessarily easy, way to support sound utility security is to create an organizational security council (physical and cyber security) that includes key staff from all utility departments, as well as top executives. Building these relationships around security can take time and be an uncomfortable process, but once formed, these relationships can fuel considerable progress.

In addition, it's helpful to designate a security officer to serve as a focal point for such an effort. This person needs the support of top executives (and should report directly to them), as well as real authority to make decisions and resources to mount investigations and implement solutions. Without such backing, effective security tends to languish.

As mentioned, bridging the organizational silos of IT and OT is another crucial element of enhancing cybersecurity. IT and OT may not always share systems, but they should at least be able to easily share information relevant to cybersecurity.

Physical and digital security are no longer separate. As utilities focus on meeting the requirements of NERC CIP v5, it's important to remember that physical and digital security have become inextricably intertwined. Therefore, a utility may spend millions on cybersecurity — but if attackers can still disable a substation with rifles (or perhaps even a hammer), how much security has been achieved? Selecting network equipment that supports a fail-safe mode is a key strategy for maintaining physical security, and ensuring system availability, during problems that compromise the functioning of IoT devices or their communications.

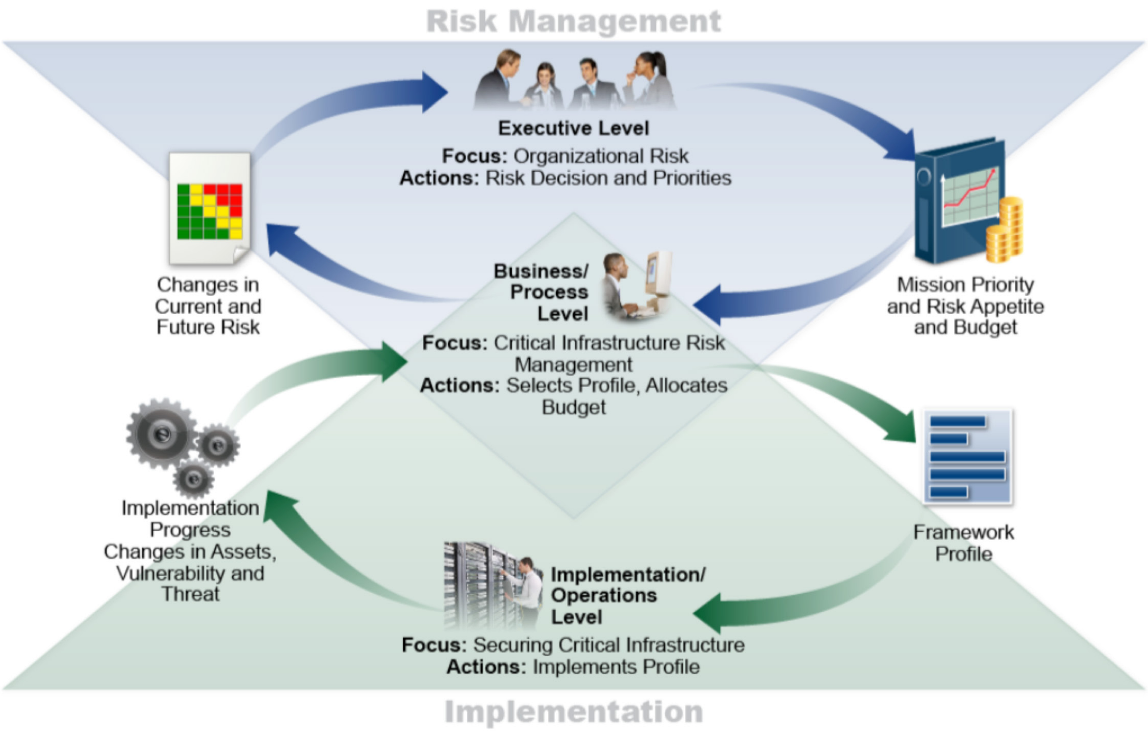
In 2010 NIST published its interagency report NISTIR 7628. This document remains some of the best guidance on integrated security for the smart grid — which includes technology such as smart meters for distribution networks, as well as IoT technology deployed on bulk power networks.

Also, in 2014, FERC enacted NERC CIP 014-1, which sets requirements for physical security of bulk power system facilities and equipment. Similar to NERC CIP v5, this standard takes a risk-assessment approach, with third-party review of utility-crafted security plans.

Physical security hardware also should be included in cybersecurity plans. Cameras, sensors and key card panels all use software and common protocols that can be disabled or tricked.

Identity management: Context is the new perimeter. Access control is a key area of security focus for many utilities — that is, determining which individuals have permission to access certain equipment, facilities, networks or command functions. This includes promptly terminating key cards and login credentials when an employee leaves the company.

Figure 4-3: Decision flows within an organization


Risk Management
Executive Level
Focus: Organizational Risk
Actions: Risk Decision and Priorities
Changes in Current and Future Risk
Mission Priority and Risk Appetite and Budget
Business/ Process Level
Focus: Critical Infrastructure Risk Management
Actions: Selects Profile, Allocates Budget
Implementation Progress Changes in Assets, Vulnerability and Threat
Framework Profile
Implementation/ Operations Level
Focus: Securing Critical Infrastructure
Actions: Implements Profile
Implementation

Source: Greentech Media

Identity management goes beyond simply observing who goes where within a utility's facilities or systems. It also means examining what individuals are doing, and when and how they're doing it. In this way, the context of people's activities becomes a crucial perimeter to be guarded. This applies not just to utility staff, but also to vendors and contractors who also may need physical or remote access to utility equipment or systems — and it includes detecting whether the devices (such as laptops or tablets) that remote operators are using to gain access might be compromised.

Effective identity management complements more established security technologies (such as firewalls and network segmentation) and techniques (such as whitelists/blacklists, network mapping, scanning). An important part of implementing identity management is deploying network devices that can passively monitor and analyze network traffic. This enables utilities to learn what normal traffic looks like on their networks and to better be able to flag abnormal traffic. Aside from spotting possible intrusions, this can help identify a wide variety of risks — including errors and accidents.

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) has developed an example solution for a crucial aspect of NERC CIP compliance: identity and access management. Intended as a complement to NERC CIP, this how-to guide demonstrates how utilities might comply with regulatory requirements through controlling access to facilities and devices from a single console. This can yield efficiencies in access management, while also saving money on research and proof-of-concept tests.

Situational awareness: Using the network as a sensor. A core cybersecurity function is to make sense of data to identify possible problems and risks. This requires consistent, comprehensive situational awareness — which the Pacific Northwest National Laboratory defines, in the context of a power grid, as "understanding the current environment and being able to accurately anticipate future problems to enable effective actions."

This approach entails a paradox: The aspects of communication protocols that make them easier to monitor also make them easier to attack. However, using modern communication protocols connects systems more easily, while also adding tools to support both productivity and security.

Education. Across all departments, it's common for utility staff members (even some who regularly work with technology) to have an incomplete understanding of how attacks occur. In this manner, they may unwittingly facilitate such attacks.

As such, educating staff about security hygiene — safer ways to use tools such as thumb drives or laptops, to be cautious of e-mail attachments and aware of phishing and other social engineering ploys, and to avoid risky practices such as charging cell phones via USB connections — can pay off by giving attackers far fewer opportunities to access utility networks.

In addition, defense training is crucial — learning how to design and implement strong network defenses, with proper network security monitoring. Many utilities are particularly lacking on this front. In an environment that has been focused on OT more than IT, this is a primary challenge.

Education should include IT and OT staff. Periodic cybersecurity refresher training across both departments helps increase security program effectiveness.

Paperwork does not necessarily boost security. Even though NERC CIP v5 requires utilities to assess their own risks and craft their own compliance plans, there remains a tendency at many utilities to continue "checking the boxes" to comply with a security plan, or with regulatory paperwork. This can lead utilities astray from the ultimate goal of enhancing cybersecurity.

A common security program flaw occurs when utilities purchase security technology without a clear understanding of what they're buying and how it can (and can't) be used. This often stems from an endemic assumption that cybersecurity is primarily a technology problem. The impact of the human element extends to being able to make educated choices about technology procurement and deployment.

CHAPTER 5

Cybersecurity and the Utility Supply Chain

Utilities procure IoT devices through a variety of vendors and distributors, and individual devices include components (such as processors) which in turn come to be embedded in devices via a variety of vendors and distributors. Every point in this supply chain — from the manufacturing of a processor to the installation of devices in a utility's system — presents potential security vulnerabilities, as well as opportunities to make IoT devices more secure. Malware can be introduced, and counterfeiting happens.

As of this writing, a new FERC rulemaking seeks to set requirements for utility supply-chain security. Utilities, vendors and other organizations submitted comments to this rule, and in January 2016 FERC held a technical conference to gain more input. A final rule is expected later in 2016.

Through this rule, FERC is attempting to manage security risks presented to bulk electric system by vulnerabilities in industrial control systems. Specifically, it would cover hardware or software components used for bulk power operations, as well as tools used to perform maintenance or other services on network components. The rule also would address transient devices on a utility network, such as thumb drives and laptops.

Both security and performance requirements are key — any security requirement must be implemented efficiently, in terms of both processing and bandwidth. Communication networks should be designed keeping in mind the bandwidth requirements for security, as well as operations.

FERC cannot directly set requirements for manufacturers or distributors, especially in a global, commoditized, price-driven supply chain. However, the requirements of this rule would probably substantially increase cybersecurity requirements in utility procurement policies — and not just for bulk power systems, but in general. Indirectly, this would influence manufacturers and distributors to upgrade their own practices in order to remain competitive with the lucrative electric power market.

The electric power sector has begun to insist that OT vendors meet security requirements, but progress on this front has been gradual. NERC CIP supports this evolution, but there is much more that utilities, vendors, and regulators can do today to protect themselves and their customers.

Some leading device and component vendors are already acting to enhance the cybersecurity of their offerings — especially by increasing built-in encryption and other features. For instance, Cisco has partnered with Intel to include, in Cisco's IoT security products for power grids, Intel Atom C2000 processors equipped with the latest virtualization, security, and cryptography features. These processors also include an out-of-order execution engine and advanced power management, and are designed for small-footprint, thermally constrained environments such as utility substations.

Utilities don't need to wait for the new FERC rule to further strengthen the cybersecurity of their supply chain. Much of this can happen through upgrading procurement policies, and enforcing them consistently across the extended enterprise. This can include product specifications for contractors and anyone with access to utility systems.

For instance, utilities can insist during procurement that processors embedded in network-connected devices utilize established cybersecurity standards such as the Advanced Encryption Standard (AES), and related features to support excellent performance with strong encryption. For instance, Intel's AES New Instructions technology (AES-

NI) accelerates certain key AES encryption and decryption functions to improve security without slowing response time. Also, Intel's QuickAssist hardware acceleration technology enhances cryptographic performance, while also improving how internet traffic gets secured and routed.

Attestation is a key concept in supply chain security: The process of authenticating the provenance and security of a device or component, to ensure that equipment received is what was ordered, and was not tampered with.

One way to do this, which Intel employs, is Enhanced Privacy ID (EPID) — a cryptographic mechanism by which a single public key is associated with a very large number of private keys. Each CPU Intel produces is signed with one of those private keys, then Intel erases their record of this signing. When each Intel CPU goes live in the field, it conducts a boot attestation — demonstrating that it can appropriately sign a message. This allows Intel to authoritatively assert that the CPU is not counterfeit and hasn't been tampered with.

System integrators can play a key role in enhancing the security of the utility supply chain. They can become a powerful tool for taking utility security requirements and implementing them with feature sets from vendors — but so far, this mechanism has been underutilized and is not well understood. Utilities have considerable leverage with system integrators and manufacturers to obtain the security they need.

System integrators design solutions for utilities, take components from various manufacturers, pre-integrate them, and install them in utility systems. Since they assume some risk for the solutions they package and install, they are motivated to mitigate security risks.

In order to scale across customers and earn acceptable margins, system integrators build internal frameworks that they can use across many customers. Commonly used security functions, platforms, and frameworks can support the development of useful standards.

Utilities overhaul their field assets in a major way only very rarely; usually, enhancements are incremental. System integrators can be especially helpful with incremental change.

For instance, substations are vulnerable to cyberattacks through two primary vectors: legacy devices and legacy protocols. Field assets often rely on older, less secure communication protocols, and fixing that is no simple task. To compensate for this vulnerability, a system integrator could package and deploy network gateways for substations. These devices offer security and identity management features, and serve as a proxy to shield assets from the network. Most importantly, they transform communications using older protocols to more secure IP protocols.

Gateways also can provide cryptographic identity services on behalf of devices in a substation. Effectively, the gateway represents these devices on the network, and it talks upstream to other controllers in the system on behalf of the substation assets. Thus, the other network devices can communicate with substation devices as if the substation assets have become more intelligent. Then, when the utility eventually upgrades to more secure field devices, the gateway can be removed.

In addition, a smart gateway can augment fail-safe operation for field assets. A gateway can be configured for fail-safe mode, in which it only communicates with local nodes, to maintain system availability. This not only helps respond to, and recover from, cyberattacks, but it also helps build out autonomy and analytics capability at the grid edge.

By bringing system integrators into conversations and planning for security programs and equipment upgrades, utilities may realize new opportunities and capacities that allow them to get more security, and other operational benefits, from limited existing budgets.

CHAPTER 6

Conclusion

In general, cyberattackers prefer the path of least resistance. Utilities that invest in security are rarely the path of least resistance. With proper planning, this investment can occur within budgetary constraints and regulatory requirements. But stronger security regulations for the grid can help utilities prioritize allocating resources for security.

Effective security is holistic — encompassing components, devices, systems, communications and personnel. It is also flexible and adaptable, responding to emerging threats, and sensitive to changing circumstances. Collaboration and communication with regulators, security experts, other utilities, service providers, vendors, and system integrators is essential to achieve holistic security.

Utility Security: Exceeding Mandates to Mitigate Risk

Sponsored by

For more info please visit www.greentechmedia.com/sponsored/resource-center/