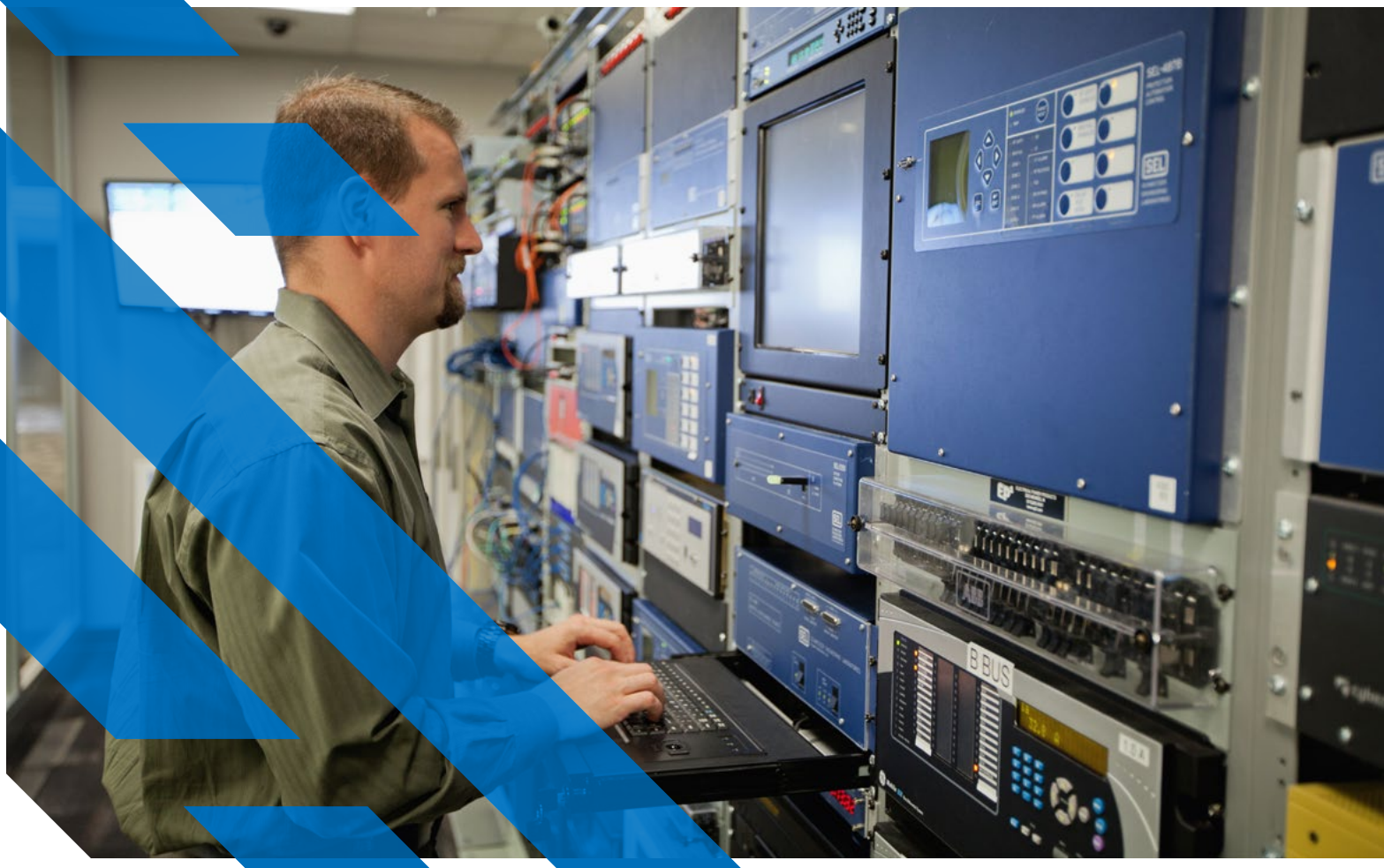
BURNS McDONNELL

WHITE PAPER / **UTILITY SUPPLY CHAIN CYBERSECURITY CONSIDERATIONS**

SECURING THE SUPPLY CHAIN

BY Jerome Farquharson, CISSP, **Donald Dustin Williams,** PE, AND **Courtney Buser**

The advance of smart grids, smart devices and increasingly interconnected systems provides exceptional potential to improve efficiency and operational excellence for the electric grid. These technologies also heighten cybersecurity risk. Utilities and independent power producers, reliant on vendors, need a range of best practices to secure supply chains, mitigate vulnerability and keep complex energy systems safe.



Malware is not an unusual approach for cyberattacks. However, the last few years have witnessed an increase in the use of these methods to infect and attack some of the industrial control systems (ICS) underlying power delivery, frequently targeting the vendors supporting electrical utilities and independent power producers (IPP).

In 2014, the Department of Homeland Security's Industrial Control System Cyber Emergency Response Team (ICS-CERT) reported an ICS-focused malware campaign that used multiple vectors for infection. These attacks include phishing emails, redirects to compromised websites and, most recently, Trojanized update installers on at least three ICS vendor websites, in what are referred to as watering hole-style attacks. These attacks exploit poor vendor and client patching, as well as updating processes. Attackers generally compromise a vendor of the intended victim and then use the vendor's information system as a jumping-off point for their attack.

Based on information ICS-CERT obtained from private cybersecurity firms Symantec and F-Secure, the software installers for these three ICS vendors were infected with malware known as the Havex Trojan. ICS-CERT also identified a sophisticated malware campaign that compromised numerous ICS environments using a variant of the BlackEnergy malware. Analysis indicates this campaign had been ongoing since at least 2011.

In 2015, a spear-phishing campaign using similar BlackEnergy malware targeted the IT staff at several Ukraine power distribution companies, causing the first known power outage hack and resulting in a six-hour power disruption for 80,000 energy customers.

In response, the Federal Energy Regulatory Commission (FERC) issued Order 829, which requires the North American Electric Reliability Corp. (NERC) to issue new or revised Critical Infrastructure Protection (CIP) standards updates to utilities and IPP. FERC has directed NERC to address the following issues:

1. software integrity and authenticity;
2. vendor remote access;
3. information system planning; and
4. vendor risk management and procurement controls.

TYPES OF EQUIPMENT THAT RELY ON CYBERSECURITY FOR PROTECTION

- **NETWORK MANAGEMENT SUITES:** Provide real-time monitoring, alarm management and configuration interfaces
- **DISTRIBUTED CONTROL SYSTEMS (DCS):** Used to control large processes
- **REMOTE TERMINAL UNITS (RTUs):** Used for SCADA, control, data aggregation
- **PROGRAMMABLE LOGIC CONTROLLERS (PLC):** Used for control of standalone equipment
- **COMMUNICATION PROCESSORS:** Used to gain engineering access to critical systems such as:
  - Protective relays
  - Reclosers
  - Cap bank controllers
  - Breakers
- **FIREWALLS:** These act as an electronic access point, used to manage inbound and outbound access
- **ROUTERS:** Used as the core for utilities' backbone network; often uses encrypted sessions
- **SWITCHES:** Used for communication at the LAN level
- PHYSICAL ACCESS CONTROL SYSTEMS (PACS):
  - DVR and IP camera controllers
  - Card access reader controllers

Expanded network capabilities enable greater use of the internet and digital automated technologies, but utilities and IPPs rely on vendors to provide virtually all products, controls, hardware and software. Protecting electricity generation, transmission and distribution from cybersecurity risks relies heavily on providing a robust and secure supply chain.

SUPPLY CHAIN RISK MANAGEMENT

The power industry successfully dealt with most physical security risks and events, quickly rebuilding infrastructure affected by weather and catastrophic events and working with established networks of local and national public service partners during emergencies. However, as operations shift reliance to an evolving environment of online and virtual assets, utilities are pressed to develop strategies and programs that can prepare for, and recover from, cybersecurity events.

Based on extensive utility-specific security evaluation by organizations including the National Institute of Standards and Technology (NIST), Utilities Technology Council (UTC) and Energy Sector Control Systems Working Group (ESCSWG), best practices and procurement language guides utilities and IPPs in meeting their NERC CIP compliance obligations.

SUPPLY CHAIN GOVERNANCE

Cybersecurity risks cut across even the most siloed organizations, functional areas, and among utilities and suppliers. New governance models are needed to connect traditionally separate operating functions to facilitate broad understanding of the scope of digital assets, prioritize risk, raise personnel security awareness and effectively secure supplier partnerships.

Instead of a single functional area owning cybersecurity responsibility, a cross-functional internal technical review board needs to examine and manage vulnerability, evaluate language in critical agreements, and broaden organizational awareness of cybersecurity risks and accountability.

The importance of the technical review team is reflected by business leader involvement and should include areas such as purchasing, operational and information technology (OT and IT), legal, asset owners, security, and others in the organization that can contribute to creating and enforcing cybersecurity goals. While the supply chain organization continues to lead the charge on supplier management, the broader team develops priorities and guidelines that help hold all partners to new utility security standards.

RISK MANAGEMENT IN THE UTILITY SPACE

Not all assets are created equal. NERC and the energy sector have developed a risk management process that is based upon the risk of the Bulk Electric System (BES) asset (e.g., substation, generation plant, control center, etc.) to the BES if its BES Cyber Systems (BCS) are compromised. NERC Standard CIP 002-5.1 identifies high, medium and low impact BCS using bright-line criteria. The bright-line criteria requires that applicable Responsible Entities categorize their BCS based on the impact of their associated facilities, systems and equipment, which — if destroyed, degraded, misused or otherwise rendered unavailable — would affect the reliable operation of the BES. These risk identifications are then used to determine the level of protection needed to be compliant, factoring in the number of requirements associated with the BES Cyber Assets.

INFORMATION SYSTEM PLANNING

Members of a utility's internal technical review board may be unaware of current suppliers. In implementing best practices for supply chain security, it is important to achieve transparency regarding the many partners supporting the organization and, potentially, increasing risk. Identifying and assessing vendors and their supply chains helps lower risk and can improve overall operational performance.

Using outcomes from the prioritized critical business and data security process, **identify vendors who support these assets**. The internal technical review board and other stakeholders can aid in the identification process.

Utility supplier relationships can vary considerably. Some vendors will provide commodity components while others will serve as integrators with extensive access to configurations, drawings, facilities and other assets to perform needed services. These types of high-

value suppliers also bring high risk. **Understanding the comprehensive supply chain and matching it to the prioritized list of critical assets** provides clarity on how to move forward with securing the supply chain.

Establish evaluation review criteria to understand the vendor's process for product evaluation. Each SCADA system, programmable logic controller, computer and software technology warrants assurance of its security and quality. **Determine the supplier's process for product upgrades and life cycle management**.

Include cybersecurity questions in vendor selection and rating processes. Understand vendor use standards and policies in critical areas such as disaster management; personnel, network, system and data security; access control for physical and cyber assets; product quality; and life cycle support.

Suppliers are an integral part of utility operations, and understanding organizational partners is critical. **Cybersecurity requirements, standards and audit rights must be developed and documented** in terms, conditions, contracts and agreements.

VENDOR RISK MANAGEMENT AND PROCUREMENT CONTROLS

Recognizing cybersecurity as a core threat to utility operations — and developing plans and processes to guard against potential issues — falls short without clear communication. In addition to making sure shareholders, employees and regulators are aware of plans to mitigate potential damage, a utility must share its vision and expectation with the supply chain. New priorities, processes and policies are only valuable if they are adequately supported by specific language in vendor agreements that reinforce cybersecurity requirements and practices.

Empower the internal technical review board, including supply chain leaders, with the responsibility and accountability to manage cyber risks. Instill urgency so these key personnel help shape the organizational culture of the importance of cybersecurity and **raise awareness that responsibility for security rests with all personnel**, not only in the IT department.

Include security requirements in vendor procurement documents, agreement, contracts and negotiations. Use critical asset prioritization and vendor assessment to determine the level of language rigor establishing high-level security and risk management stipulations. Incorporate comprehensive language to address all aspects of products and services supplied, including control, data acquisition, distribution, sensors and actuators, data analysis and storage, networks, communication pathways, and services. Language, specifications and requirements are vital to enforce the necessary cybersecurity performance required from all vendor partners.

Contracts should include notification by the seller of any breaches in security within its operation, and specify in procurement documents how the utility and supplier will communicate about any events or incidents. Include obligations for monitoring compliance of vendors and methods used to enforce security stipulations, product quality and testing, third-party certifications, and any personnel screening or training requirements.

In certain global supply chains, it may become difficult to identify and stipulate requirements for the entire supply chain. The technical review board must **consider what assurances, demonstrations and explicit processes** or standardized contractual language will be required of primary suppliers to maintain robust supplier management throughout the supply chain.

Determine expectations on how information will be shared between the utility and vendor, within the utility and broader energy sector, and among stakeholders and industry associations. Managing and **understanding cross-industry vulnerabilities and incidents supports continuous improvement** of the overall supply chain security process.

CONCLUSION

While daunting and continuous, developing an approach to securing the supply chain while meeting compliance requirements is achievable. Understanding areas of cyber asset vulnerability, raising awareness of the network of critical suppliers, communicating security expectations among all operational partners and elevating cybersecurity as a utility's core value provide

the framework. By dedicating a cross-organizational team to drive the initiative, utilities and IPPs may find that the results surpass compliance and safety goals and help realize a higher-functioning, safer and more reliable enterprise.

BIOGRAPHIES

JEROME FARQUHARSON, CISSP, CRISC, is the manager of the Burns & McDonnell Compliance and Critical Infrastructure Protection practice. He leads with a multidisciplined background of physical and cybersecurity, information systems and business advisory consulting. Jerome is an experienced security network engineer with 17 years of IT experience, including network design implementation, support and troubleshooting of CISCO routers, switches, firewalls, VPN devices, intrusion detection systems and network management systems. He has spent the past seven years as a policy and procedural development specialist for both medium- and large-sized utility environments. He has performed compliance audits for large investor-owned utilities to determine the level of regulatory exposure and define mitigation strategies to minimize penalties. Jerome is actively involved with the NERC subcommittees and regional Information Systems Audit and Control Associations (ISACA).

DONALD DUSTIN WILLIAMS, PE, is an electrical computer engineer specializing in telecommunications and network engineering. His experience includes MPLS WAN, substation LAN and SONET network design and implementation. He is currently a lead engineer for the design of an installation that encompasses protective relaying transport and critical systems backhaul.

COURTNEY BUSER, BSEE, works in the substation department of the Transmission & Distribution Group on the design of multiple projects ranging from 12-kV through 765-kV. She leads in protection and controls design, physical design, grounding analysis, and AC and DC station sizing and design. She earned a bachelor's degree in electrical engineering from the University of Evansville and is a member of the Institute of Electrical and Electronics Engineers.

12750-CYB-0117