accenture

FORGING STRONGER LINKS:

NERC CIP SUPPLY CHAIN CYBERSECURITY

NERC'S CIP-013-1 STANDARD SEEKS TO SAFEGUARD NORTH AMERICA'S ELECTRICITY SUPPLY CHAIN FROM CYBERATTACKS

Is an electricity provider's supply chain its weakest link in the event of a cyberattack? The evidence is compelling that third parties often play unwitting roles. For example, the NotPetya mock ransomware attacks in mid-2017 originally gained a foothold via a backdoor in third-party accounting software.[i] Tio Networks, a payment processing company, suffered a breach that exposed the private information of up to 1.6 million utility and cable customers who used the service to pay their bills.[ii] Likewise, the attack vector that led to the breaching of payment information involving millions of customers was found to be in one of retailer Target's Heating, Ventilation and Air Conditioning (HVAC) vendor's systems.[iii]

To safeguard North America's electricity supply, the North American Electric Reliability Corporation (NERC) has issued several critical infrastructure protection (CIP) standards. The proposed CIP-013-1 standard (subject to Federal Energy Regulatory Commission's approval[iv]) addresses the vulnerabilities and threat vectors that external third parties in the supply chain can have on the Bulk Electric System (BES). It helps to mitigate the risks of supply chain cybersecurity incidents that affect BES reliability, and requires responsible entities, which can include utilities and a wide variety of other stakeholders, to develop plans, policies and procedures concerning their supply chain vendors.

What the standard mandates

Electric energy players must develop and implement a comprehensive supply chain risk management plan that includes CIP senior manager reviews and approvals every 15 months. Mandatory elements of the plan focus on software integrity and authenticity, vendor remote access to BES cyber systems (BCSs), information system planning and procurement, and vendor risk management and procurement controls.

Each supply chain management program must also include planning processes that identify and assess the vendor products and services used for medium- and high-risk BES cyber systems. Plans require a process for vendors to notify responsible entities about incidents they have identified relating to the supply chain, and a formal way to coordinate responses between responsible entities and suppliers regarding such incidents. Other necessary elements include a notification process for when vendor personnel no longer require remote and on-site access to the BCS, the full disclosure of known vulnerabilities by the vendor to the responsible entity, and vendor verification as to the integrity and authenticity of all software and patches supplied to the network. CIP-013-1 stipulates the coordination of all controls for vendor-initiated interactive remote access (IRA) and vendor system-to-system remote access.

Addressing CIP-013-1 compliance challenges

When electric utilities and other responsible entities focus on CIP-013-1 compliance, three challenges can emerge concerning scoping, vendor relationships and interpretation.

ESTABLISHING THE NECESSARY SCOPE

NERC CIP-013-1 only addresses high- and medium-risk BES cyber systems, and responsible entities must make decisions regarding the scope of their activities in these areas. Goals could conceivably range from simply becoming and remaining compliant to rolling out compliance more broadly, encompassing low-impact BCS as well, for example, and potentially including the complete enterprise. This latter kind of expanded strategy should deliver higher consistency and greater cyber hygiene across the business in relation to supply chain risks, because the same vendors and products are often used in conjunction with high-, medium-, and low-risk BES cyber systems.

DEFINING VENDOR RELATIONSHIPS

One clear imperative involves ensuring strong, trust-based relationships and meaningful partnerships between vendors and energy players. Consequently, responsible entities will likely consider adding specific language and stipulations concerning supply chain vendor management to their contracts, along with reasonable expectations for fixing problems and other types of remediation. Helpful vendor relationship questions include: How will players define and determine that the selected supply chain management tools are reasonable and appropriate for addressing supply chain risk, and are they feasible for suppliers to adopt? Which approaches will work best for cybersecurity triage, response, and remediation when an incident occurs between a responsible entity and its suppliers? What repercussions should vendors face that fail to meet requirements, and what opportunities will they have to close their gaps to compliance?

Responsible entities also need to know what repercussions vendors could face that do not comply with stipulated incident and vulnerability reporting, and what the form and channel will look like for vulnerability and incident notifications between vendors and the responsible entity. They need to know who within the responsible entity will have the job of receiving and acting on notifications from vendors, how suppliers will provide evidence of their compliance with any new contractual stipulations, and how often responsible entities will require them to demonstrate this compliance. Other issues focus on whether teams within responsible entities will staff up to manage this new governance activity and, if vendors decide to withdraw from serving the BES, will their leaving drive an uptick in procurement activities to retender contracts?

INTERPRETING THE STANDARD

The current language in NERC CIP-013-1 is not completely prescriptive, leaving some areas open to interpretation. For example, while the standard addresses new contracts, it does not require the renegotiation of existing ones. Nor does it require the modifications of terms, conditions, service level agreements (SLAs), penalties for non-compliance, or adherence to terms for existing contracts. Likewise, although a CIP senior manager must review the supply chain risk management plan, no provisions or requirements exist for updating it based on revised threat intelligence. This raises some questions. For example, how should responsible entities rate, quantify and measure risks? Should they consider "zero-day" threats? How do they ensure they are up-to-date and focused on emerging vulnerabilities and concerns, along with the mitigation measures needed to handle them?

Other concerns arise regarding how vendors will collaborate with the CIP senior manager to improve the process. Additionally, the term "incident" remains undefined, making it difficult to determine the scope of an attack, and the term "representative" also remains ambiguous, along with whether it refers to onshore or offshore resources.

Next steps toward CIP-013-1 compliance

Utilities and other energy players have anticipated the arrival of CIP-013-1 for years; now is the time to act. That means developing a strategy, empowering the CIP-013-1 team, and taking steps toward consistent, sustainable performance right from the start.

GET STARTED: DEVELOP A STRATEGY

If responsible entities have not already started, we recommend they do the following now. First, determine CIP-013-1 responsibility and ownership in terms of the business and the compliance organization. Second, begin a dialogue with key stakeholders and vendors on the impact CIP-013-1 compliance will have on their organizations. Third, make sure the organization has enough time to define and implement the new controls and to demonstrate evidence of compliance within the enforcement timeframe. These initial discussions should address several important items, including identifying all the key internal and external stakeholders and understanding the differences between the CIP-013-1 requirements and existing supply chain cybersecurity practices, if any. Organizations also need to determine the timeline and phases for implementation and discuss with suppliers the impact regarding both current and future contracts and service level agreements. Yet another topic is understanding the interrelationship between CIP-013-1 and other CIP standards.

MOBILIZE YOUR CIP-013-1 TEAM

The core of any CIP-013-1 initiative is the team assembled by a responsible entity to achieve supply chain cybersecurity compliance. This team operates best if a responsible entity's executives provide oversight and sponsorship regarding its governance and steering. It also makes sense to align all NERC CIP-013-1 compliance efforts with the architectures and strategies of other organizational cybersecurity and risk programs, such as those supported by the National Institute of Science and Technology (NIST), the SysAdmin, Audit, Network, Security (SANS) Institute, and the IEC/ISA 62443 standards established by the International Society for Automation and the International Electrotechnical Commission.

In addition to the CIP-013-1 standards, several other important supply chain requirements appear in CIP-005-6 and CIP-010-3 regarding the governance of vendor remote access and the verification of the source and integrity of procured software. Responsible entities can also gain critical insights regarding cybersecurity automation from the broader NERC CIP compliance program on topics such as ensuring that evidence collection follows the leading practices developed through prior cycles of regulatory auditing.

PLAN FOR SUSTAINABILITY FROM THE OUTSET

While responsible entities typically have their hands full staging and launching a CIP-013-1 initiative, success mandates that they also plan for sustainability from the outset. That means designing CIP-013-1 controls to include periodic reviews (for example, every 15 months) and approaching all approval requirements in an orchestrated way that requires only minimal manual reviews. Organizations should put mechanisms in place to validate and verify that vendors meet CIP-013-1 controls, and that they proceed through supply chain procedures with a minimum of manual monitoring. They should also automate audits as much as possible, standardizing, and orchestrating evidence-gathering processes and associated tools.

Establishing a robust change control program in accordance with CIP-010 will be crucial for ongoing maintenance and governance of the initiative. The program should clearly identify, approve, and document all modifications and updates made to BES high- and medium-impact cyber systems and associated technologies. Additionally, the change control process should identify and document the retirement of BES cyber systems and the removal of vendors from an approved vendor list.

THE ACCENTURE VIEW ON CIP-013-1

When dealing with any NERC CIP standard, it is critically important to ensure sustainability from the start. That means designing for compliance using automation and orchestrated workflows and working with the CIP compliance team during the planning phase to gather necessary information and evidence. When assessing an energy player's gap to compliance with NERC CIP-013-1, organizations must create and maintain an accurate inventory of all supply chain products and services that could have an impact on the BES. In fact, depending on the number and types of vendors, products, services, contracts, and supply chain relationships involved, NERC CIP-013-1 could affect numerous business stakeholders, from legal and contract management to IT support systems. Close collaboration among security, NERC CIP compliance, and other organizational responsible entity workstreams will be necessary. Additionally, the NERC response to the FERC's Order 829 on supply chain risk management contains proposals for modifications to current CIP-005 and CIP-010 standards to tighten restrictions on vendor remote access sessions and increase the integrity of software and patches used by energy entities. Upon implementation, the maintenance and ongoing management and governance of NERC CIP-013-1 processes may also require additional resources to support ongoing awareness campaigns, remediation, and compliance monitoring and reporting.

Protection, starting now

Complying with NERC CIP-013-1 is an important first step in safeguarding the nation's electric infrastructure from cyberattacks that originate among supply chain vendors. Taking steps early on to ensure sustainability and developing a coherent strategy can make compliance a solid foundation upon which to establish additional tailored supply chain cyber protections. Responsible entities and their vendors should view CIP-013-1 as a "win-win" opportunity since it can help to protect both parties from cyberattacks and strengthens already-established links.

CIP-013-1 TIMELINE

The NERC Board of Trustees adopted NERC CIP-013-1 on August 10, 2017. However, as of the date of this publication, FERC has not approved NERC CIP-013-1 and an effective date has not been set. However, the industry expects the effective date to occur in the first half of 2020.

PAVING THE WAY FOR CIP-013-1

Revisions 4 and 5 of the NIST SP 800-53 standard combine elements of cybersecurity with an increased emphasis on third-party vendors and suppliers. Furthermore, NIST 800-161 specifically addresses 19 areas of supply chain risk management. The IEC/ISA 62443 standard and the SANS Institute also provide guidance focused on supply chain risk management. In line with NIST and SANS, FERC and NERC have recognized that this area also affects utilities, which now rely more heavily on third parties in their supply chains. As a result, FERC Order 829, issued in July 2016, resulted in the drafting of the proposed NERC CIP standard 013 focused on "supply chain risk management for industrial control system hardware, software, and computing and networking services associated with bulk electric system operations."

References

i **Is This Ukrainian Company The Source Of The 'NotPetya' Ransomware Explosion?** Reuters, June 27, 2017. https://www.forbes.com/sites/thomasbrewster/2017/06/27/medoc-firm-blamed-for-ransomware-outbreak/#43b2cc1e73c8P

ii **PayPal shelled out $238 million for company that may have 1.6 million customers breached,** *USA Today,* December 4, 2017. https://www.usatoday.com/story/tech/2017/12/04/paypal-acquired-company-reports-many-1-6-million-users-breached/919090001/

iii **Contractor charged with leaking classified NSA info on Russian hacking,** CNN, June 6 2017. https://www.cnn.com/2017/06/05/politics/federal-contractor-leak-prosecution/index.html

iv On January 18, 2018, The Federal Energy Regulatory Commission (FERC) issued a **Notice of Proposed Rulemaking (NOPR)** approving NERC's proposed CIP-13 Standard but also instructing NERC to "include EACMS [Electronic Access Control and Monitoring Systems] associated with medium- and high-impact bulk electric system cyber systems within the scope of the supply chain risk management Reliability Standards as well as to evaluate the risks presented by PACs [Physical Access Controls] and PCAs [Protected Cyber Assets] as part of a study already proposed by the NERC Board." FERC has not yet issued a final rule in response to the comments provided.

CONTACTS

Gilbert Sorebo
Senior Manager
Accenture Security
gilbert.n.sorebo@accenture.com

James Wright
Senior Manager
Accenture Security
j.a.wright@accenture.com

Thomas Ryan
Principal Director
Utilities Industry
Accenture Consulting
thomas.c.ryan@accenture.com

Jamie Bass
Managing Director
Accenture Security
james.bass@accenture.com

ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With approximately 449,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at **www.accenture.com.**

ABOUT ACCENTURE SECURITY

Accenture Security helps organizations build resilience from the inside out, so they can confidently focus on innovation and growth. Leveraging its global network of cybersecurity labs, deep industry understanding across client value chains and services that span the security lifecycle, Accenture protects organization's valuable assets, end-to-end. With services that include strategy and risk management, cyber defense, digital identity, application security and managed security, Accenture enables businesses around the world to defend against known sophisticated threats, and the unknown. Follow us @AccentureSecure on Twitter or visit the Accenture Security blog.