FORTRESS
Information Security

Revised Nov 21, 2019

Asset to Vendor Network for Power Utilities

The cost-effective CIP-013 supply chain risk management solution

Contents

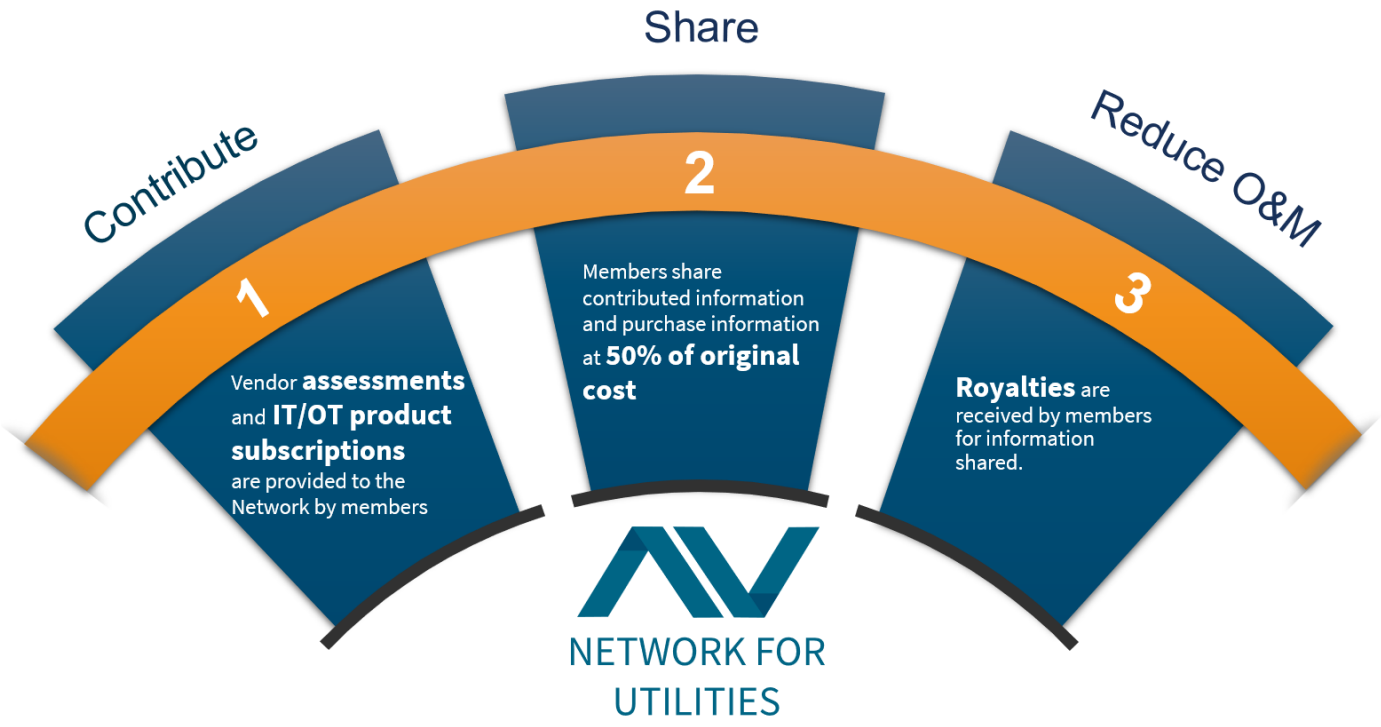
Abstract

1. Grid security has now expanded to encompass supply chain vendors.

2. Asset to Vendor (A2V) is a joint venture of utility companies and Fortress Information Security where members benefit from sharing risk information at a savings of up to 50% or more below traditional costs. **Contribute > Share > Reduce O&M.**

3. CIP-013 implementation guidance published by NATF[1] and NERC[2] suggests performing product risk assessments, vendor risk assessments, and verifying the integrity and authenticity of software (e.g., patches) which are all available on the A2V platform. The governance committee of A2V, held by utility members, ensures that the Network remains ahead of industry, security and regulatory requirements.

4. Vendors will benefit from reduced overhead by having a conduit for sharing their risk assessments in a standardized format which is acceptable by their clients.



[1] http://www.natf.net/docs/natf/documents/resources/natf-cip-013-1-implementation-guidance.pdf

[2] https://www.nerc.com/pa/comp/guidance/EROEndorsedImplementationGuidance/CIP-013-1-R1%20Implementation%20Guidance.pdf

Introduction

The digital revolution has created new opportunities, but it has also created new vulnerabilities. Globalization and technological transformation have vastly enhanced the efficiency of supply chains for companies and organizations in every sector but have also contributed to creating vulnerabilities and raising risk exposure.

Power utilities, like many other industries, have embraced the digital transformation, realizing significant benefits in their interactions with vendors and customers. They have also experienced an increased attack surface. They are aware of the risks and the need for strong security. However, power utilities face many challenges in managing risk across applications and infrastructure.

Challenges in Supply Chain Risk Management

The Industrial Internet of Things (IIoT) creates great opportunities for efficiency, but also creates new vulnerabilities for attackers to exploit. Cybercriminals, motivated financially, attempt to exploit these vulnerabilities to install ransomware with the goal of taking down the grid until their demands are met.

Nation states are also attempting to penetrate our defenses. But, instead of looking for a payout, their goal is to either gain negotiating leverage, to make a political statement, or to surreptitiously embed themselves in preparation for the possibility of a war, at which point they could activate their embedded malware to disable our defenses.

In January 2019 the Wall Street Journal[3] reported specific examples of how nation states are using supply chain vendors as a "backdoor" to attack the power grid. This is the first of two primary attack paths: (1) vendors of the power utilities who have fewer resources to put towards cybersecurity, and (2) unpatched vulnerabilities in software.

Adversaries are multiplying, and their ability to exploit supply chain vulnerabilities is growing faster than the process of securing them can be achieved. Unless we change our methods, we are fighting a losing battle.

Supply Chain Attacks Spiked 78 Percent in 2018[4]
-NextGov.com

[3] How Russia utilized the vendor "backdoor" https://www.wsj.com/articles/americas-electric-grid-has-a-vulnerable-back-doorand-russia-walked-through-it-11547137112

[4] https://www.nextgov.com/cybersecurity/2019/02/supply-chain-attacks-spiked-78-percent-2018-cyber-researchers-found/154996/

Challenges in Vendor Risk Management

Vendor risk management poses unique security challenges for power utilities that even power utilities with mature security organizations may find daunting.

1. Risk Ranking Vendor Populations
   The large size of the population of supply chain vendors providing equipment, software, and services to power utilities makes the task of risk-ranking vendors costly and time-consuming.

2. Assessing vendors with access to medium and high impact BES systems
   Assessments are also time-consuming and costly. As a result, vendors are often only assessed when a new vendor contract compels it, or when an existing vendor contract is up for renewal, rather than on all existing vendors.

3. Non-responsive Vendors
   Vendors who remain "on-call" but who are not currently under contract may resist investing time and labor into completing assessments as they have no current financial incentive for doing so, while vendors who are actively serving utilities may not see the point of completing an assessment when their contract is not up for renewal. Internal procurement teams may be reluctant to impose another burden on their vendors for fear of failing to meet their procurement objectives. For these reasons, non-responsive vendors impede achieving risk management goals.

4. Remediating Vendors with Lower Hygiene
   Vendors may have challenges achieving security best practices and remediating security findings due to lack of resources. Resources are instead spent on responding to controls assessment requests.

5. Continuous Monitoring
   Conducting point-in-time assessments leaves large gaps of time during which vendors' security posture may change. Outsourcing continuous monitoring to service providers can be costly – up to $2,000 or more per vendor.

6. Supply Chain System of Record
   Traditional GRC systems do not meet the unique specifications required to efficiently execute a supply chain risk management program with customizable workflow, document management, approvals, analytics engine, customizable APIs, customizable surveys, rules automation, vendor portal, customizable scoring or other key features.

Vendor risk management can be challenging and costly for power utilities and can be perceived as burdensome by the vendors. These challenges are experienced by all power utilities.

Nearly 60% of organizations that suffered a data breach in the last two years cite as the culprit a known vulnerability for which they had not yet patched.[5]
-DarkReading.com

[5] https://www.darkreading.com/vulnerabilities---threats/unpatched-vulnerabilities-the-source-of-most-data-breaches/d/d-id/1331465

Challenges in Vulnerability Risk Management

Vulnerability risk management also presents daunting challenges to power utilities.

1. Patch Distribution is Insecure or Non/Loosely Compliant
   Any software that is to be used in the BES Cyber System must be verified for its integrity (unaltered from its original source) and authenticity (the identity of the software publisher is confirmed and linked with the software). This is typically a manual process.

2. Product Assessments are Complex
   Most industries have done little in the way of product assessments due to the cost. NERC CIP-013 implementation guidance suggests that Responsible Entities may consider assessing vendor risk management controls through obtaining a "summary of any internal or independent cybersecurity testing performed on the vendor products to ensure secure and reliable operations."[6]

3. Vulnerability Tools are Incomplete
   Traditional vulnerability tools only provide vulnerability information if there is a specific CVE (Common Vulnerabilities and Exposures published by Mitre.) Industry professionals are left with only half the picture, because (1) they don't know about vulnerabilities that do not have CVEs, and (2) scanners tend to leave a 50% gap even to the CVE list.

   Product patch scraping tools focus on automation but generally only provide up to 60% coverage, making it time-consuming to identify missing patches. Furthermore, a patch may not even be available, and mitigating controls have to be researched.

Vulnerability risk management can be challenging and costly for power utilities, and regulatory deadlines create additional urgency. These are problems also experienced by all power utilities.

Regulatory Challenges

To address emerging supply chain risks to the power grid, the North American Electric Reliability Corporatoin (NERC) has issued new standards that require utilities to develop a plan for managing cyber risks related to their supply chain. In order to comply, the plan should include procedures for prioritizing vendors based on risks, and requirements for completing standardized risk assessments on each vendor, as well as verifying the authenticity of software manufacturers and the integrity of software updates.

The deadline for implementing the plan is currently July 1, 2020. Utilities that fail to have a program in place (with ongoing compliance obligations) by this deadline can face various levels of penalties ranging as high as $1,000,000 per day.

---

[6] https://www.nerc.com/pa/comp/guidance/EROEndorsedImplementationGuidance/CIP-013-1-R1%20Implementation%20Guidance.pdf, page 4

This deadline applies only to power utilities based in the United States. Utilities outside the US that have security programs that track NERC requirements as a guideline for their own program may benefit from the sense of urgency conveyed by this deadline.

Duplicating Efforts

Power utilities share many of the same assets and vendors. For each utility to conduct the same assessment on a vendor wastes valuable resources for both the power utilities and the vendors.

Cybersecurity Limitations

The biggest challenge facing security teams at power utilities may not just be how to secure the grid, but how to do it without breaking the bank. Cybersecurity spending is rising, but not as fast as attacks are occurring or as fast as new regulation deadlines are approaching. The biggest challenge of all is securing the grid while reducing operations and maintenance (O&M) costs.

Corollary to budgetary challenges is staffing. Increased demand for trained cybersecurity personnel has made qualified human resources scarce and expensive.

The Asset to Vendor Network

Powered by Fortress Technology, and in collaboration with American Electric Power (AEP), Fortress has launched a new joint venture, the **Asset to Vendor Network (A2V)** for power utilities.

This new collaborative platform will be a cybersecurity information exchange where members will be able to access a library of supply chain vendor assessments, product assessments and cyber vulnerability solutions/patches at a savings of up to 50% or more. Members can also contribute their information to the Network and receive royalties as their information is shared.

A2V will increase the security of all members, reduce costs of assessments by up to 50%, and "bend the O&M curve," lowering costs and, in some cases, allowing members to capitalize security costs. A2V members will be able to 1) contribute, 2) share and 3) reduce O&M.

1. Contribute

   Member utilities contribute their completed vendor assessments and validated cyber vulnerability patches to the Network, or pay a reduced fee to have assessments completed, on both assets and vendors.

2. Share

   The completed assessments are made available to other power utilities at a cost that is projected to save them up to 50% or more of what it would cost them to complete themselves or pay another company.

3. Reduce O&M

Members who contribute completed assessments will earn a financial benefit, called a "royalty." In many cases, members can bundle components as an appliance for capital treatment.

"Power utilities already share the risk. Now they can share the cost."
- Alex Santos, Fortress CEO

How A2V Helps

A2V solves many of the challenges facing power utilities. It resolves issues for vendor risk and vulnerability risk management. It helps utilities achieve NERC CIP compliance in a timely manner. It reduces burdensome redundancies for utilities and vendors, and it reduces costs for utilities and vendors.

Solutions to Vendor Risk Challenges

The Asset to Vendor Network resolves many of the challenges vendor risk management teams face at power utilities.

1. Risk Ranking Vendor Populations
   A2V is pre-populated with the known vendors of the utility supply chain, with a prediction of the inherent risk of each organization (e.g., OT maintenance provider being critical risk, versus a travel agency being low risk.) This process utilizes data collection technology, machine learning, and analytics to make these predictions. A2V members can correlate their vendor list before performing manual inherent risk ranking, gaining insight into their overall risk on day one.

2. Assessing Vendor Security Controls
   Power utilities already share the risk. Now they can share the cost. By performing assessments once and sharing with many, the O&M cost for each utility will be significantly reduced, and in some cases, eliminated by utilizing cost capitalization strategies.

3. Vendor Chasing
   Vendors without contractual obligations to comply might be unmotivated to respond quickly to requests for controls assessments. However, once the assessment is complete, vendors no longer have resource constraints to comply. A2V will work with vendors to achieve mutual benefits.

4. Remediating Control Deficiencies
   Just as problematic as non-responsive vendors is the case of unresolved security control deficiencies. The cost efficiencies offered by A2V allows vendors to remediate deficiencies while allowing them to show compliance to a wide audience of utilities.

5. Continuous Operational Monitoring of all Vendors
   A2V provides continuous monitoring of all active vendors and cyber assets on the Network.

Members receive alerts when any vendor has an incident or when vulnerabilities are discovered. Alternatively, members can alert other members through the Network when they discover vulnerabilities and provide patches and solutions through the Network. Monitoring is expanded beyond traditional cybersecurity scanners (looking at things like application security, configurations, malware, and spam propagation), to include legal, financial, anti-bribery, anti-money-laundering (AML), negative news, and regulatory compliance.

6. Fortress Platform as System of Record for Supply Chain Risk Management
   Members may optionally choose to use Fortress Platform (FP) instead of their GRC to document supply chain risk management. FP is not typically used as a replacement for the GRC, but to orchestrate the workflow prior to uploading the finding into the GRC (which can be done automatically with APIs.) FP includes customizable workflow, document management, approvals, analytics engine, customizable APIs, customizable surveys, rules automation, vendor portal, customizable scoring, and other key features.

Asset to Vendor resolves many of the most pressing vendor risk management challenges, lowering costs for power utilities and their vendors.

Solutions to Vulnerability Risk Challenges

The Asset to Vendor Network resolves many of the challenges faced by IT and OT vulnerability risk management teams at power utilities.

1. PatchChain File Verification and Integrity Tool
   Fortress' PatchChain verifies patch authenticity (the supplier source) and validates file integrity (that the file is unaltered). PatchChain uses a distributed ledger that compares file hash values to confirmed values. Further, patches are instantly available for subscribed products. Patches can also be validated back to PatchChain before deployment.

2. Product Assessment Repository
   Many vendors are being asked for product security assessments, and A2V is making it simple to share these assessments securely.

3. Vulnerability and Solution Monitoring
   Products monitored in A2V include full vulnerability details, including both CVE and non-CVE information, as well as utility-specific business context. Threat intelligence is overlaid on the vulnerability data to alert members to vulnerabilities that are actively being exploited.

   A2V ensures the solutions are well documented for products. Solutions are not always a patch but rather a configuration change or other mitigating control.

A2V helps bridge the silos between vendor risk, IT, and operations by connecting the assets to the vendors.

A2V Helps Utilities Achieve NERC CIP Compliance

Concerns relating to preparing for CIP-013 compliance by July 1, 2020 can be addressed through a partnership with A2V, which has this compliance standard as its priority. See below for CIP-013 requirements addressed by A2V.

Requirement[7]	A2V Solution
R1 Each Responsible Entity shall develop one or more documented supply chain cybersecurity risk management plan(s) for high and medium impact BES Cyber Systems. The plan(s) shall include:	Out of the box program policies vetted by member utilities.
1.1 One or more process(es) used in planning for the procurement of BES Cyber Systems to identify and assess cybersecurity risk(s) to the Bulk Electric System from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).	All vendor risk services (risk ranking, security controls assessments, vendor chasing, remediation, and continuous monitoring) and product security assessment.
1.2 One or more process(es) used in procuring BES Cyber Systems that address the following, as applicable: **1.2.1.** Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cybersecurity risk to the Responsible Entity;	Policies include recommended contractual language and master services agreement addendums. Further, members have the option to use Fortress Platform to track the implementation and operation of all CIP-013 requirements.
1.2.2. Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cybersecurity risk to the Responsible Entity;	
1.2.3. Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;	
1.2.4. Disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity;	Vulnerability and solution monitoring
1.2.5. Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System; and	PatchChain file verification and integrity tool
1.2.6. Coordination of controls for (i) vendor-initiated Interactive Remote Access, and (ii) system-to-system remote access with a vendor(s).	(same as 1.2.1 through 1.2.3 above)

[7] https://www.nerc.com/_layouts/15/PrintStandard.aspx?standardnumber=CIP-013-1&title=Cyber%20Security%20-%20Supply%20Chain%20Risk%20Management&jurisdiction=null

Buy or Build?

Power utilities facing security challenges and regulatory deadlines are facing a difficult decision: build or buy? Benefits of buying with A2V include:

- Instant program maturity with CIP-013 compliant policies and procedures.
- Instant scalability and assessment availability.
- A single solution for point-in-time assessments and continuous monitoring.
- No additional staffing burdens.
- Ability to capitalize costs while receiving royalties that offset O&M.

FAQ's

- HOW WILL A2V ROLL OUT? HOW DO I GET ACCESS?
  Closed Beta is scheduled to begin on January 1, 2020. Open release is planned for April 1, 2020. Fortress Information Security is the current operator of the A2V Network exchange and is managing new registrations. Interests in A2V memberships should be directed to Nick Noll, nnoll@fortressinfosec.com.

- HOW WILL MEMBERS BENEFIT FROM SHARING THEIR SECURITY INFORMATION?
  Members receive royalties each time their security assessments or patch subscriptions are shared with another member. The royalty structure is tiered to return costs quickly back to the creator. The first share is 75% royalty; the second is 65%; third and on is 50% cost return.

- IS SECURITY INFORMATION NORMALIZED?
  A2V normalizes contributed assessments so that different assessment frameworks are correlated and members receive a consistent experience.

- HOW MANY VENDOR ASSESSMENT TYPES WILL BE AVAILABLE?
  The governance committee anticipates three tiers of vendor assessments with add-ons for onsite assessments and additional assessment certifications (e.g., certified by Big-4 or other).

- HOW DO MEMBERS PAY FOR SERVICES?
  A token system is used to provide simplicity. Token rates are utilized for assessments, risk ranking, and product subscriptions.

- WHAT INCENTIVES DO VENDORS HAVE TO PARTICIPATE?
  Proactive vendors will have the benefit of being seen as a first mover in securing the grid. By participating in A2V, vendors who serve multiple utilities will save time interacting with each utility individually. Vendors, just like utilities, may join A2V as members where their own assessments, both vendor and product, can be resold for royalties.

- HOW ARE "MASTER" ASSESSMENT CONFLICTS MANAGED?
  If two member utilities both want to initiate (or master) an assessment, the member who is willing to complete the assessment first receives the right to do so. Further tiebreakers are resolved based on their A2V membership date.

- WHO IS DRIVING THE A2V NETWORK?
  Members are represented by a governance committee that is appointed by the utility members. Fortress Information Security performs operations for A2V.

- WHY IS A2V ANY BETTER THAN OTHER RISK EXCHANGES?
  A2V is the only exchange that offers financial benefits to those who contribute, is utility-specific, offers comprehensive solutions to address the specific needs of the utility sector, and is run by a governance committee of utilities.

Summary

The Asset to Vendor Network creates a platform where utilities can collaborate to solve the supply chain cybersecurity challenges they face today and prepare for tomorrow. This is an opportunity to make the power grid more resilient.

Power utilities who join A2V will strengthen security and meet compliance deadlines while reducing duplication of efforts, and "bend the O&M curve," lowering costs.

Collaborating to Address Supply Chain Security Challenges

Utilities have long held a philosophy of cooperation and mutual assistance. They work together to identify, defend, and recover from storms or threats to any member so that they can continue to serve their customers and shareholders. This is exemplified by initiatives such as:

- Electricity Subsector Coordinating Council (ESCC) with the mission of coordinating efforts to respond to national-level disasters or threats;
- Cyber Mutual Assistance Program by ESCC to counter cyber-attacks;
- Electricity – Information Sharing and Analysis Center (E-ISAC) which analyzes and shares security and threat data;
- Regional Equipment Sharing for Transmission Outage Restoration (RESTORE) program maintains costly spare parts to recover from catastrophes, and
- American Nuclear Insurers (ANI) is a joint underwriting association that acts on behalf of member organizations, such as operators of nuclear power plants, to provide insurance for public liability resulting from nuclear disasters.

The storm on the horizon now is a virtual one, a cybersecurity storm. By pre-emptively invoking the need for mutual assistance, power utilities can minimize costs and reduce the risk for all. By sharing threat intelligence, best practices, vendor assessments, and asset integrity verification, progress toward security and compliance can be accelerated.

The future of cybersecurity is collaboration. The future of cybersecurity for power utilities is to collaborate to secure industrial assets and their supply chain.