North American Transmission FORUM

Community *Confidentiality* *Candor* *Commitment*

NATF Supply Chain Initiative Overview

July 27, 2021

Valerie Agnew, NATF

NATF Supply Chain Security Assessment Model

- Streamlined, effective, and efficient industry-accepted approach for entities to assess supplier security practices
  - reduce burden on suppliers
  - provide entities with more information
  - improve supply chain security

Recent Accomplishments

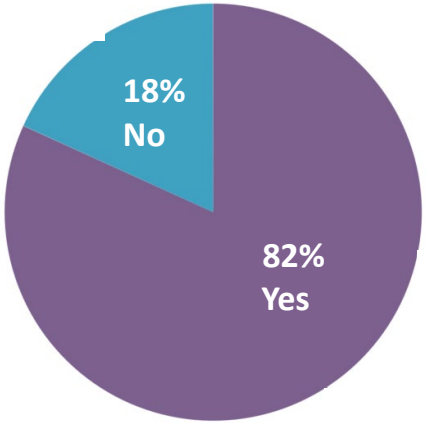
Posted NATF board-approved supply chain security assessment model, criteria, and questionnaire

Submitted NATF's response to DOE RFI

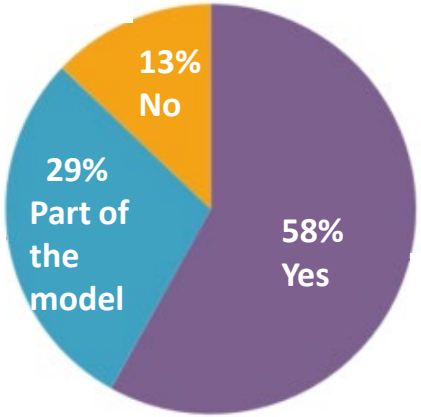
Issued model assessment adoption survey

Nearing completion of a guide for "Using Solution Providers for Third-Party Risk Management"

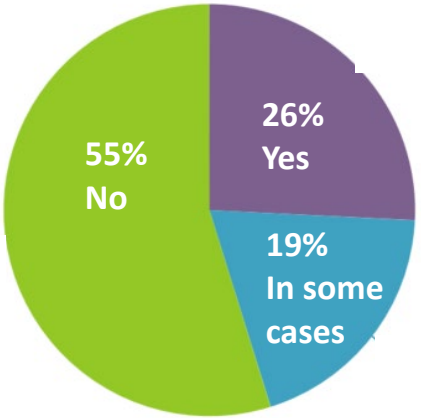
Supply Chain Security Assessment Adoption Survey



Is your organization an NATF Member?

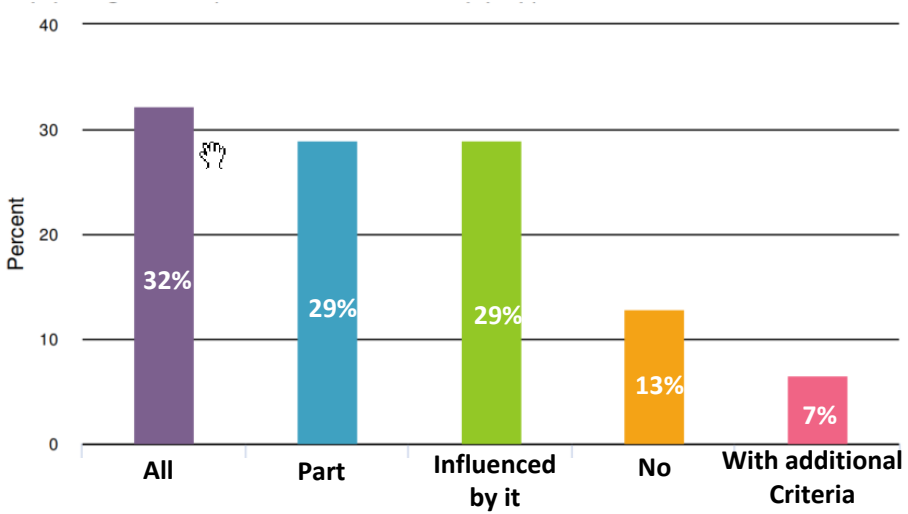


Has your organization adopted the model?

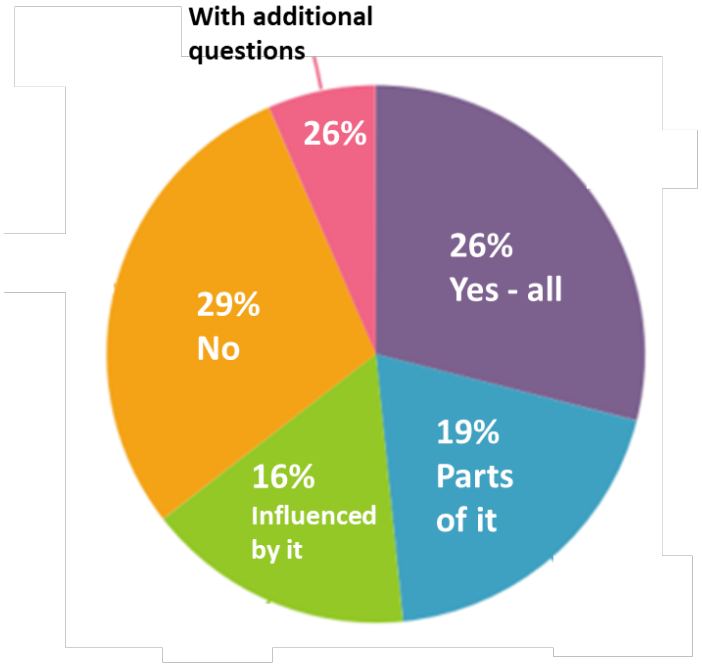


Does your organization use a solution provider?

Supply Chain Security Assessment Adoption Survey



Does your organization use the NATF Criteria?



Does your organization use the Questionnaire?

Survey Results Support Current Activities

Low response rate but responders provided thoughtful information

Indicates need for simplicity – would like to have a database/portal to access information

Indicates need to streamline – less information to collect and analyze (reduced number of questions/criteria)

Need information from smaller and medium-sized suppliers

The Next Steps

Current Activities

Development of central repository/library

- Industry solution
- Request DOE Support

Assistance for smaller suppliers to establish strong security postures

- Exelon is setting the foundation
- Establishing a lead organization

Add scoring capabilities to criteria and questionnaire

- To assist entities with streamlining risk assessments

Regulatory endorsement of model, criteria, and questionnaire

- To provide assurance of high-level compliance acceptance

Vendor Security Risk

Preliminary Discussion on Industry Trends and Considerations

Exelon

Today's Presenters

Betsy Soehren Jones
Director, Cyber and Physical Security Strategy

David Chaddock
Director, Cyber Security

AJ Brown
Senior Manager, Energy & Utilities

Sean Murphy
Manager, Energy & Utilities

Exelon Case Study

As attacks are increasing, the challenges associated with third-party security will only continue to intensify.

- Exponential rise in vendor incidents
    - Not just cyber impacts – operational/reliability impacts starting to occur
- Assessment results are not promising
    - Failure rate for NATF cyber hygiene questions (no anti-virus software)
    - No specific “vendor profile”
- Lack of awareness for rules of engagement. New regulations will cause disruption in the supply chain
- Cost of the program
    - Assessors
    - Trust but verify reviews
- Industry-wide approach fixes many of the issues

While there have been ad hoc efforts to ensure third-party vendors have robust security protocols in place before contracting with utilities, the industry lacks a consistent approach

Disparate Industry Standards

- Each electric & gas utility has their own set of security standards and requirements with which vendors must comply
- Heavy lift for utilities to evaluate vendor security posture where no standard approach exists
- Variance in vendor security for utilities

Varying Vendor Security Maturity

- Departure from operational norms and core business for some vendors where cybersecurity is not inherent
- Burdensome process for vendors to attempt to comply with security protocols across each unique utility
- Lack of budget for external support (assessments, remediation, cyber insurance, etc.)

Inability to Assess and Verify Security

- May be designed based on other industry requirements (e.g., ISO 27001, PCI, FedRAMP)
- Utility-focused offerings are not designed to an industry-specific standard
- Difficult to evaluate effectiveness of cybersecurity offerings

As attacks are increasing, the challenges associated with third-party security will only continue to intensify. There is a need to migrate from a model of "trust" to model of "trust, but verify"

Other industries facing similar challenges aimed to improve their security posture by standardizing requirements for third-party entities

Financial Services

Payer Card Industry (PCI) Standards

- Created in 2004 by the five major credit card brands to increase controls around cardholder data
- PCI Security Standards Council is an independent non-profit entity responsible for maintaining PCI standards, training assessors, and quality checking assessor reports
- Council is funded by opt-in from assessors and training fees paid by assessors
- Council is governed by executive committee and board of advisors comprised of card brands and vendors to represent the interests within the framework (such as merchants and third-party security firms)
- Enforcement of the standard is the responsibility of the acquiring banks and card brands; fines are assessed to the card brands, and the brand assess fines to merchants

KY3P

- Increase in regulatory pressures in 2000s requiring financial service firms to proactively manage suppliers, leading to an increase in due diligence questionnaires (DDQ)
- Collecting and distributing the data led to duplicated efforts, costly errors, and delayed responses.
- These challenges prompted an industry consortium of financial institutions, buyside firms, and third-party service providers partnered to create KY3P in October 2015
- KY3P (Know Your Third Party) is a cloud-based solution platform used for vendor onboarding, collection and verification of due-diligence data and vendor-risk monitoring
- The platform offers a subscription-based service with 5,000+ users, 25,000 vendor profiles, and 100+ clients in the network that mostly include regional banks and other financial institutions.

Key Considerations & Lessons:

- Consider holsitic representation for governance (including service providers)
- Identify a tiered threshold for compliance (e.g., based on volume / risk)
- Ensure training program is well defined, maintained, and consistent
- Quality assurance checks on assessor reports

Key Consideration & Lessons:

- Primarily focused on regional banks to help standardize approach to due diligence and risk assessments
- Cloud-based solution that offers workflow from vendor on-boarding and management

In contrast to the self-governance of PCI-DSS, information security in the healthcare industry was driven largely by federal regulation

Healthcare

HITRUST

- HIPAA enacted in 1996 and amended several times to include security, privacy, and enforcement provisions to ensure patient healthcare information is adequately protected
- Industry-driven group known as **HITRUST** formed in 2004 to help healthcare entities comply with HIPAA through a suite of frameworks and tools
- For-profit company that sells access to its proprietary framework and services, such as assessments
- Since expanded to support all industries aiming to comply with a number of standards, such as NIST, ISO 27000 series, and others
- Governed by an Executive Council made up of industry leaders and supported by working groups made up of experts across the public and private sectors

H-ISAC

- The sector launched the Health ISAC (H-ISAC) in 2010 with the mission to 'empower trusted relationships in the healthcare industry to prevent, detect and respond to cybersecurity and physical security
- The global non-profit adopted a member-driven governance model to create forums for sharing threat intelligence and best practices
- The non-profit organization's funding model consists of membership fees and sponsorship programs; offers eight tiers of membership based on the revenues and funds raised by for-profit and non-profit organizations
- Rapid growth of both the threats from cybersecurity and the myriad of vendors offering solutions creates a significant burden on H-ISAC to accurately verify membership requests; created volunteer program to review and validate the legitimacy of membership requests

Key Considerations & Lessons:

- Consider holsitic representation for governance (including service providers)
- Identify a tiered threshold for compliance (e.g., based on volume / risk)
- Ensure training program is well defined, maintained, and consistent
- Quality assurance checks on assessor reports

Key Consideration & Lessons:

- Tiered membership structure allows for equitable participation for membership
- Verifying membership / vendor legitimacy can proactively mitigate risk through validation

Key barriers must be addressed in order to stand up such a framework and ensure vendors of all sizes, category, and background have the resources and accessibility to participate

	BARRIER / CHALLENGE		POTENTIAL SOLUTION
1	Disparate Standards	Electric & Gas utilities must align on a common set of security standards and requirements to which third-party vendors must comply	Create a common security questionnaire and central repository to drive clarity and consistency across the industry while alleviating the burden on third-party vendors of completing security assessments for each new utility partner or contract
2	Lack of Governance	Utilities and other key stakeholders must collaborate to define an operating and cost model to support this common security framework	Review other industries and seek stakeholder input to understand the advantages and risks with adopting one model over another
3	Inequitable Vendor Support	Smaller, diverse suppliers may not have the internal expertise or the budget to hire external suppliers to implement the necessary security measures	Provide vendor support and funding to ensure diverse suppliers are not being factored out of the procurement process due to inaccessibility of security solutions and expertise
4	Audit Fatigue	Third-party vendors in some categories (i.e., financial services, manufacturers) may already be certified through other security frameworks and are facing audit/compliance fatigue	Evaluate potential of mapping requirements to existing frameworks to improve audit efficiency by only requiring third-party vendors to comply with unique utility-specific requirements

Enacting an industry-wide centralized library for third-party risk data is a win-win-win for the industry, national security, and third-party vendors alike

Utility Industry

Ability to leverage a common source of vendor security posture data while sharing relevant knowledge and the cost of reducing third-party risk across industry peers

National Security

A standard approach will improve the security for the Nation's critical infrastructure to reduce the threats and impacts on customers and related markets

Third-Party vendors

Supporting vendors as they work to improve their security hygiene, enable access to opportunities with utility industry partners, & reducing the burden (and cost) of demonstrating their security posture with each new utility partner

The establishment of a library must consider a minimum set of requirements

- ❑ Centralized library of vendor response to security risk assessments
- ❑ Industry governed definition of questionnaire contents and validation criteria and approach
- ❑ Supports security controls to ensure others cannot view individual utility details, including vendor-specific activities
- ❑ Maintenance model that encourage vendors to keep their submissions up-to-date while complementing the current vendor monitoring efforts of individual utilities
- ❑ Cost model that enables “a-la carte” approach to support service functionality tailoring for utilities