NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Supply Chain Cyber Risk Management Lifecycle

Tom Alrich, Owner, Tom Alrich LLC
NERC RSTC Supply Chain Working Group

RELIABILITY | RESILIENCE | SECURITY




Introduction

- One of the most important sources of cyber risk worldwide – across all industries – is the supply chain. The Target, Stuxnet, and NotPetya attacks all started in the supply chain.
- However, mitigating supply chain risks is very hard. Essentially, instead of just having to secure one organization (itself), the organization needs to secure each of its important vendors, then each of their vendors, then each of *their* vendors, etc.
- This is obviously impossible.

The SCCSRM Plan

- Given that no organization has infinite resources available for cyber risk mitigation, there is simply no way to mitigate all supply chain risks. The organization needs to develop a plan to identify, assess, and mitigate the most serious risks, then implement the plan.
- And given that resources are finite, they should be allocated so that the maximum possible risk is mitigated. You don't want to spend all of your resources mitigating a few unimportant threats that don't pose much risk to the BES.
- The NERC entity's BES supply chain cyber security risk management plan should be designed to achieve this goal, as far as possible.

Identifying Threats

- For NERC entities, the supply chain risks to be mitigated are risks to the BES, and only those. The entity, as a business organization, should also mitigate supply chain security risks to achieving other goals (such as financial well-being), but this should be a separate effort.
- Every NERC entity should consider developing two SCCSRM plans, one for IT assets and one for OT assets.
- This means that most of the supply chain risks that are discussed in documents like NIST 800-53 and 800-161 aren't relevant for a NERC entity's supply chain risk management plan because they only apply to IT, not OT. The only risks that apply to the BES are OT risks (although many risks apply to both, of course).

IT vs. OT risks

- For example, NIST 800-53 and 800-161 (and standards like ISO 27001/2) address risks like loss of intellectual property; privacy of personal data (including PHI); breach of the organization's financial systems and data, etc. Each of these is a serious risk to the organization, but not to the BES.
- This means that if, for example, you include non-BES-related questions in BES-related vendor questionnaires, or require non-BES-related contract terms in BES-related contracts, you will waste time and resources, and the vendor will waste time and resources.
- This is why your BES supply chain cyber risk management plan should just focus on OT risks.

IT vs. OT risks

- One standard that only considers OT risks is IEC 62443. The NATF Criteria also only consider OT risks. The same applies to the DoE Procurement Language document from 2014 and some other documents.
- All of these documents are good, but none of them are comprehensive of all BES risks. You will likely decide that you need to identify risks using a number of sources.
- You should list all OT risks that *might* have an impact on the BES, *in your entity's BES environment* (which will differ from other entities' environments). These are the risks you should consider for your plan.

Threats and Vulnerabilities

- Every risk has two components. The first is a Threat, which is simply something bad that could happen. Of course, here we're just concerned with Threats to the BES. The second component is a Vulnerability. A Vulnerability is something that allows a Threat to be realized.
- For example, there's a Threat that someone will compromise a computer on a vendor's network that is used to access systems attached to one of your OT networks, and through that cause damage to the BES. One Vulnerability that would allow this to happen is if the vendor doesn't properly protect that computer, including by isolating it from the rest of the vendor's network.
- If there are no Vulnerabilities that are likely to allow the Threat to happen, there is no risk. Your goal in your risk management plan is to put in place measures that will reduce the likelihood of each Vulnerability that allows a Threat to happen. When you have done that, you have mitigated the Threat itself.

A simple example

- Consider the Threat that someone will break into your house and steal your belongings. The main Vulnerabilities that enable that Threat to be realized are open or improperly secured doors and windows.
- How do you mitigate the Threat? By mitigating each Vulnerability. And you do that by making sure *all* doors and windows are secure. At that point, when all Vulnerabilities are mitigated, the Likelihood that anyone can break into your house is low, which I consider to be the same as mitigation of the Threat itself.
- But what happens if you have 10 doors and windows, but only 9 are well secured? The tenth has been left unlocked. Of course, the burglar will use that!

A real example

- Now consider the Threat that your entity will procure a BES Cyber System that has a backdoor planted in it. After you've installed the BCS on your ESP, someone will penetrate it and impact the BES.
- One Vulnerability that might enable this to happen is poor security in the supplier's development environment, which would allow someone to plant the backdoor.
- You need to require the supplier – through contract language, phone calls, emails, etc. – to take measures like separate the development network from the IT network and require separate authentication, perhaps even multi-factor.
- You need to do this for each Vulnerability. The Threat itself isn't mitigated until all* of the Vulnerabilities are mitigated.

What's with the asterisk?

- In many cases, you won't have to mitigate every Vulnerability for a particular Threat, because one or two Vulnerabilities is sufficient to mitigate the Threat.
- For example, there are a number of Vulnerabilities that enable the Threat of compromised vendor remote access to be realized. If you allow vendor remote access, you will need to make sure all of those Vulnerabilities (on the vendor's and the entity's side) are mitigated.
- However, if you don't allow vendor remote access, you've mitigated all of the other Vulnerabilities. You don't have to worry about the others.

Mitigating Threats

- There are many ways to mitigate supply chain Threats and Vulnerabilities. Vendor questionnaires, contract language, organization procurement policies, RFP terms, procurement and installation risk assessments…All of these are tools that can be used to mitigate supply chain security risk.
- In fact, most of what has been written about supply chain security can be considered primarily suggestions for mitigating risk – including the other guidelines documents on the NERC website.
- The entity's supply chain cyber risk management plan should identify, for each Vulnerability, appropriate mitigations for that Vulnerability – using tools like those just listed.

Identifying Appropriate Mitigations

- The goal of mitigation should be to decrease the risk posed by each Vulnerability from medium or high, to low. Once the risk is low, the Vulnerability is mitigated. There is always a small amount of residual risk. No risk can be completely eliminated.
- Mitigation may require multiple actions. For example, the Vulnerability of a backdoor might be mitigated by having the supplier tighten their development security. But if the supplier doesn't fully mitigate the Vulnerability, the entity needs to take further steps on its own, such as scanning and testing products before installation.

Likelihood Scores

- One of the most important tools of supply chain risk mitigation is risk scores. A risk score is usually a combination of likelihood and impact.
- However, I have found it very hard to find a case when impact to the BES is anything but high.
- For that reason, I think likelihood is all that varies, and you should assess Threats and Vulnerabilities according to their Likelihood alone.

Assigning Likelihood Scores

- An important step is to assign a Likelihood Score (1 = low, 2 = moderate, 3= high) to each Vulnerability. The Likelihood Score for the Threat will be the highest of the Vulnerability scores.
- There are two types of Vulnerabilities: those that come from the entity itself (e.g. that the entity might procure a counterfeit hardware product containing malware), and those that apply to the supplier (e.g. that the supplier doesn't perform backgrounds checks on people in its development environment).
- For Vulnerabilities that apply to your entity, you need to ask "Do we have a *documented* procedure, policy or technology that mitigates this Vulnerability?" If so, the Likelihood Score is 1 (low). If not, the score is 2 or 3 (moderate/high).

Vendor Likelihood Scores

- Vendor Likelihood Scores are determined for each vendor. It isn't very helpful to have a single score for the vendor; instead, the NERC entity needs a score for *each Vulnerability* that applies to the vendor.
- You can obtain these scores by a) developing a questionnaire that asks a question based on each vendor Vulnerability that you have identified; b) getting the vendor to respond to the questions; and c) scoring each answer based on the likelihood that the Vulnerability it's based on has been mitigated by that vendor. If the vendor has mitigated the Vulnerability, their likelihood score will be low. If they haven't, their score for this Vulnerability will be medium or high.

An example

- Suppose you have a Vulnerability that reads “A supplier doesn’t monitor their network, meaning a malicious party could compromise the network and use that to penetrate the NERC entity’s OT systems. Through those systems, the malicious party could damage the BES itself”.
- You might ask your supplier “How do you monitor your network for intruders: a) SIEM or log management (with appropriate maintenance of the system); b) regular log review; or c) no monitoring?”
- If the supplier answers a), you might say there’s a low likelihood that this Vulnerability is found at this supplier. If they answer b) or c), you might say there’s a medium or high likelihood.

Procurement Risk Assessments

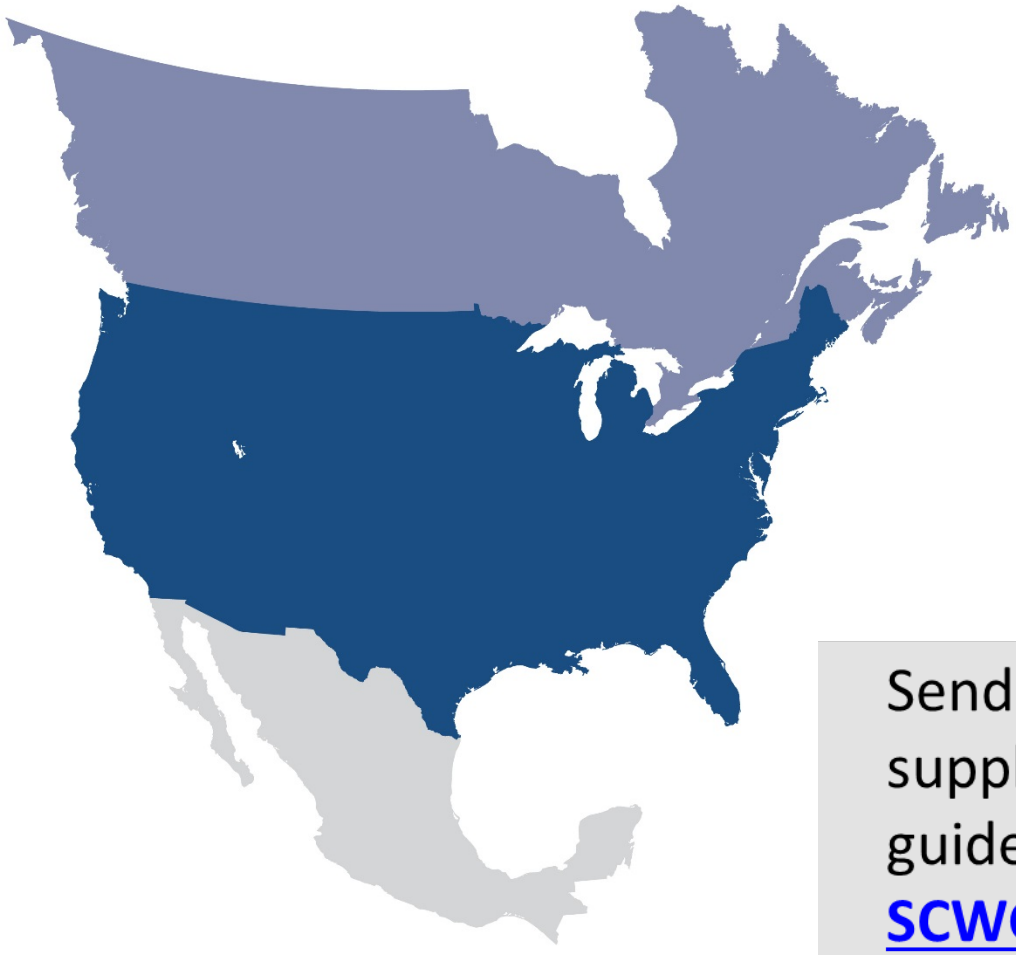
The most important mitigation step is the Product or Service Procurement Risk Assessment. In the PPRA, the NERC entity:

1. Lists all of the Vulnerabilities that apply to this Procurement;
2. Enters the entity or vendor Likelihood score for each Vulnerability;
3. Removes each Vulnerability with a score of 1, since it is already mitigated;
4. For the remaining Vulnerabilities, identifies one or more Mitigations that can be applied during the Procurement or Installation of the product; and
5. Provides the list of Mitigations to the team carrying out the Procurement and Installation, for them to carry out.

Conclusion

The fundamental problem of supply chain cyber security for the BES is that no NERC entity has the resources to mitigate all supply chain security risks. Following an approach like the one described above is the best way to ensure the entity's SCCSRM plan mitigates the greatest possible total supply chain security risk, given its available resources.

Additional topics and guidance for Supply Chain Security can be found at https://www.nerc.com/pa/comp/Pages/Supply-Chain-Risk-Mitigation-Program.aspx.



Send questions about the supply chain security guidelines to SCWGWebinars@nerc.net.