NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Security Guideline for the Electricity Sector - Supply Chain

Vendor Risk Management Lifecycle

The objective of the reliability guidelines is to distribute key practices and information on specific issues critical to promote and maintain a highly reliable and secure bulk power system (BPS). Reliability guidelines are not binding norms or parameters to the level that compliance to NERC's Reliability Standards is monitored or enforced. Rather, their incorporation into industry practices is strictly voluntary.

Introduction

The supply chain cybersecurity risk management plan ("risk management plan") addresses risks that originate with vendors; these form part of the total set of supply chain cybersecurity risks. The stages of the vendor risk management lifecycle include vendor acquisition, procurement(s) from the vendor, installation and use of the product or service (including vendor support and patching), and termination of the vendor relationship. Vendor risks need to be mitigated during each of these stages.

As is the case for all supply chain cybersecurity risks, a NERC entity must identify, assess, and mitigate vendor risks. The vendor risk management lifecycle constitutes one component of the entity's supply chain cyber security risk management plan. The plan itself is the subject of a separate SCWG white paper, "Supply Chain Cyber Security Risk Management Lifecycle," which describes the general processes of identification, assessment, and mitigation of supply chain cybersecurity risks. Because this white paper provides examples of vendor risks and suggested mitigations for them, NERC entities should consider these as they develop their overall risk management plans.

Mitigating Risks during Vendor Acquisition

In some cases, acquiring a new vendor will occur as a separate process from actual procurements from that vendor; in other cases, the vendor acquisition and procurement steps will be combined. In the former case, the NERC entity will usually put out a Request for Proposal (RFP) to multiple vendors. Some possible steps for the entity to mitigate BES risk through the RFP process are:

- For closed RFPs, consider establishing a process for cyber risk informed invitations to participate in the RFP. Such a process should consider approved entity lists, intelligence sources, and public information such as history of vulnerability handling and web site hygiene.
- Require the vendor to sign a mutual non-disclosure agreement (MNDA), so that any information provided to the NERC entity will be protected, and vice versa.
- Include a questionnaire designed to gather information about the vendor's mitigations for the identified BES risks documented in the risk management plan. If a standardized questionnaire is used, questions that don't relate to the set of risks that the entity has decided to mitigate in their risk management plan should be omitted; it is a waste of both the entity's and the vendor's time

to require answers to questions that the entity has already decided don't deal with risks that are important enough to mitigate.

- The RFP can include sample contract language; the vendor might be asked to agree to this language or to suggest modifications. Similarly to the questionnaire, the entity should make sure there are no contract provisions that don't correspond to risks it has decided to mitigate.
- As an alternative to including security provisions in contract language, the NERC entity can make these deliverables in the RFP itself.
- If the vendor wishes to cite particular security certifications as risk mitigation measures, they should be required to provide supporting evidence such as an audit report.
- One risk mitigation measure is to request that the vendor provide a software bill of materials (SBoM) for all components of their software and/or firmware that were developed by third parties - whether purchased or open source. An SBoM allows the entity to identify components known to present risks and hold the vendor accountable for providing patches for those components, when available and applicable.

Assessing Vendor Risks after Acquisition

Once a vendor relationship is in place, the NERC entity needs to continually identify, assess and mitigate residual and new risks posed by the vendor. Following are some of the steps that NERC entities can take to assess vendor risk:

- Entity-developed questionnaires can be provided regularly (on a schedule determined during procurement) to the vendor. The questionnaire should address the set of BES risks documented in the then-current risk management plan. It should be designed to determine, for each risk in the risk management plan, if changes have occurred that would increase or reduce this risk, or if the vendor has effectively mitigated this risk. It is important to let the vendor know in the original RFP that failure to answer questions, or failure to take mitigation steps requested, may cause the entity to terminate the relationship.
- Before submitting a questionnaire to a vendor, the entity should go through any documents made available by the vendor (on their public web site or directly to their customers), to determine whether any of the questions have already been satisfactorily answered in those documents.
- The entity may also use questionnaires developed by industry organizations. If the vendor has already provided answers to such a questionnaire, the NERC entity should first review those answers, to determine whether these have addressed at least some of their questions. They should then submit the remaining questions to the vendor.
- The entity should consider a vendor's certification to an industry recognized third-party cybersecurity standard, such as ISA/IEC 62443, ISO 27001 or SOC2, if available from the vendor. Such standards require annual audits by accredited independent third parties, and provide constant oversight of the vendor's ability to meet industry best practices for supply chain security and secure development practices. Such a certification may address many of the questions in the entity's questionnaire, although the entity should not hesitate to ask the vendor to identify where

specifically in the certification document each of their questions is answered, and to still require the vendor to answer any questions not satisfactorily addressed by the certification. However, making certification to such standards an absolute requirement for the vendor may lead to cost increases or refusal by the vendor to sell to the entity.

- The NERC Implementation Guidance for CIP-013-1[1] suggests "Periodic review processes…can be used with critical vendor(s) to review and assess any changes in vendor's security controls, product lifecycle management, supply chain, and roadmap to identify opportunities for continuous improvement."[2] The entity can conduct direct assessments or use a third party engaged by the entity. The entity and the vendor should agree during the procurement on the frequency and content of assessments, as well as who will bear the costs. However, these assessments can be expensive, both for the entity and for the vendor.

Means of Securing the Vendor's Commitment to Mitigations

No matter the means used to assess vendor risks, once it has identified risks applicable to a particular vendor, the NERC entity should try to get the vendor to help mitigate those risks. The vendor's agreement to do this should be documented using one or more of the following methods:

- Language in an RFP should provide clear criteria for vendor responses, so that the entity can determine to what degree the vendor has mitigated each of the risks it considers important.
- Language in a contract should document the vendor's commitment to implement specific security controls, provide for the entity to review the vendor's progress, and identify methods for future communication on these matters. If prewritten contract language is used, it should be reviewed and tailored only to include clauses that correspond to risks identified in the entity's risk management plan.
- Letter from the Vendor. If contract language is infeasible or impractical, a letter – preferably from a high-ranking official at the vendor - can also be used to document the vendor's commitment to implementing particular security controls to mitigate risks the entity considers important.
- Verbal commitment. If the commitment from a vendor can only be obtained verbally, record the conversation, with permission, or take notes. Document the person's name, title, date, time, and key points of the conversation. Document the vendor's exact words as closely as possible.
- Vendor meeting. The NERC entity might have regular meetings for vendors. At those meetings, the agenda should include a discussion of relevant risks and discussion of how the vendors can work with the entity to mitigate those risks. The entity should take notes during the meeting and publish minutes for all vendors, whether or not they were able to attend the meeting.

When evaluating the usefulness of vendor contract language for risk mitigation, it is important to consider:

[1] Implementation Guidance for CIP-013-1
[2] NERC, "Cyber Security Supply Chain Risk Management Plans - Implementation Guidance for CIP-013-1", July 2017, p. 3.

- Contract language governing purchases made from resellers or other intermediaries may not be binding on manufacturers or software developers; and
- Contract language may not apply to purchases made from stores or distributors, or products or services purchased from online-only vendors, since these transactions typically are not governed by a contract.

Verifying Vendor Compliance with the Entity's Security Requests

No matter how the entity has documented that a vendor agreed to comply with its request for risk mitigation(s), the NERC entity always needs to verify that the vendor is actually complying. There are many different means to accomplish this goal, which will vary according to a) the degree of trust the entity places in the vendor, and b) the nature of the mitigations agreed to. These means can include a new questionnaire, emails, face-to-face meetings, phone calls, audit by the entity or a third party, and direct evidence such as entity documents showing the degree to which a vendor has taken particular steps – e.g. notifying the entity when an employee with BES Cyber Systems access has been terminated.

However, there is always the possibility that the vendor will fail to perform some or all of what it promised to do. When that happens, the entity should always take some action. Possible actions include:

- Document and communicate with the vendor the gap in performance, the expected service, and applicable contract terms or documented commitment.
- Engage management or senior leadership of the vendor, to impress on them the importance of the control(s) or mitigation(s) and the need to implement remediation of the gap in performance.
- Communicate to the vendor that performance measures will be reflected in future scoring or evaluation of new purchases of products or services.
- Take legal action if needed.
- Evaluate terminating the relationship with the vendor.
- Apply internal mitigations to the risk, if the vendor simply will not cooperate. If the entity has committed to mitigating a particular risk in its risk management plan, it must do that, whether or not a vendor cooperates.

Mitigating Risk in Particular Procurement Transactions

Every procurement should begin with an assessment of the risks that apply to procuring a product or service, as well as threats that apply to installing a product. The entity should determine risk scores for each vendor and each product or service procured (preferably at the level of individual threats). The vendor and product risk scores can be combined to obtain an overall procurement or installation risk score.

The procurement or installation risk score can be used to determine the level of mitigations applied to the applicable risks during the procurement or installation. Higher scores could warrant strong mitigations, while low scores could warrant little or no mitigation beyond the entity's normal procedures.

Terminating a Vendor Relationship or Transitioning between Vendors

When an entity terminates an existing vendor relationship or transitions to a new vendor, a process should be in place to identify and mitigate the risks associated with the termination or transition.[3]

Additional topics and guidance for Supply Chain Security can be found at Supply Chain Risk Mitigation Program page.[4]

[3] For a good discussion of mitigating risks attendant on terminating a vendor relationship, see Utilities Telecom Council, "CYBER SUPPLY CHAIN RISK MANAGEMENT FOR UTILITIES - ROADMAP FOR IMPLEMENTATION", available at https://utc.org/wp-content/uploads/2018/02/SupplyChain2015-2.pdf, pp 13-14.

[4] https://www.nerc.com/pa/comp/Pages/Supply-Chain-Risk-Mitigation-Program.aspx