NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

# Vendor Cyber Security Risk Management Lifecycle

Security Training Session

Tom Alrich, Owner, Tom Alrich LLC
Critical Infrastructure Protection Committee
June 4, 2019 | Orlando, FL

RELIABILITY | RESILIENCE | SECURITY

# Introduction

- One of the most important concerns of supply chain security is risks that originate through vendors.
- These risks need to be identified and mitigated at all stages of the vendor lifecycle, including acquisition, vendor risk assessment, securing vendor commitment to mitigations, verifying vendor performance of mitigations, individual procurement transactions, and transition to a new vendor.
- This paper describes some of those risks, as well as possible mitigations.

# Vendor Acquisition

- Many acquisitions of new vendors start with an RFP.
- If possible, the RFP should a) ascertain the state of each potential vendor's cyber security program, and b) require the vendor to commit – in their proposal – that they'll implement or maintain certain security controls.
- The former can be achieved by including a questionnaire in the RFP. The latter can be achieved through including security controls as deliverables of the RFP itself.
- One deliverable of the RFP might be a "software bill of materials".

# Assessing Vendor Risks

- After a vendor is in place, the entity should regularly assess the vendor’s security controls.
- Good tools for doing this include questionnaires (tailored to address only the threats chosen as most important by the entity), vendor certifications, and vendor review meetings.
- The goal should always be to determine how well the vendor has mitigated each of the threats that the NERC entity has determined it will mitigate in its supply chain cyber risk management plan. If possible, the vendor should be given a risk score of L/M/H for each threat.

# Securing Vendor Commitment to Mitigations

- Once the NERC entity has identified medium or high risks posed by a particular vendor, the entity should try to get the vendor to commit to mitigating those risks.
- The commitment can take different forms, including RFP language, contract language, letter from the vendor, and documentation of a meeting with the vendor.
- Contract language alone can’t be relied on to indicate vendor commitment, since in many cases it isn’t possible to use contract language – e.g. purchases through a dealer, rather than the manufacturer itself.

# Verifying Vendor Compliance with Entity's Requests

- No matter how a vendor's commitment to implementing what the NERC entity requested is documented – contract, letter, etc. – the entity needs to verify whether or not they're actually keeping the promises they made.
- There are various ways to do this, including a new questionnaire, emails, notes taken during face-to-face meetings or phone calls, audit by the entity or a third party, and direct evidence from entity staff members.

# If the Vendor doesn’t Comply…

- If a vendor doesn’t perform some or all of what it promised to do, the NERC entity should always take some action to change this situation.
- Actions can include meeting with vendor leadership, suspension of further purchases, legal action, and termination of the relationship.
- If the vendor refuses to implement required mitigations, yet it’s impossible to terminate them as a vendor, the entity will still need to mitigate the risk in some way. Mitigations will depend on the risk in question, but can include extra scanning or testing, denying vendor remote access to BES Cyber Systems, more detailed inspection of delivered products, etc.

# Risk Mitigation in Procurement Transactions

- Every procurement should start with an assessment of threats that apply to the procurement and to the installation. A "procurement risk score" could be assigned to each threat, equal to the sum of the vendor and product risk scores for that threat.
- If the procurement risk score is high or medium for a particular threat, that threat should be mitigated during the procurement or installation.
- Ideally the mitigation(s) chosen for each threat should reduce to low the likelihood of each vulnerability that enables the threat to be realized.

# Risk Mitigation in Transition between Vendors

- The final phase of the vendor risk management lifecycle occurs when the NERC entity terminates the relationship with that vendor and transfers it to a new vendor.
- There are a number of risks attendant to this process, including the risk to information on the entity’s BES systems held by the vendor.
- It’s important to conduct a complete risk assessment of this process, and take steps to mitigate any threats that pose a high or medium risk.

# Conclusion

Effectively identifying and mitigating vendor risks should be one of the most important elements of any NERC entity's supply chain cyber security risk management plan.

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.

# Questions and Answers