NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Vendor-Identified Incident

Supply Chain Working Group Guideline

Steven Briggs, TVA
Supply Chain Working Group

RELIABILITY | RESILIENCE | SECURITY



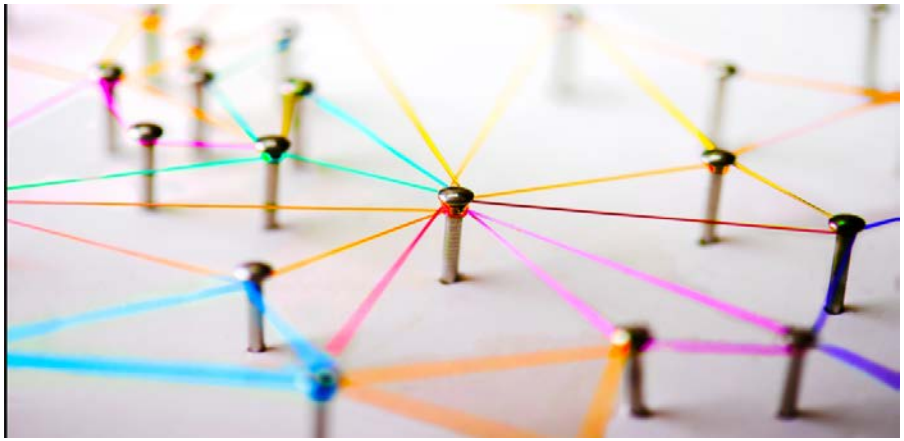

Introduction

- Vendor-Identified Incident
  - Definition: Based on the Supply Chain Cybersecurity Risk Management Plan ("Risk Management Plan")
    - Established during the procurement process
    - Inclusive of cyber-incident response elements
      - Identification
      - Notification
      - Mitigation
      - Remediation
      - Recovery

Potential Incidents

System Integrity Compromises

- Of the vendor code for patches, updates, software, installation or configuration files, used on a BES Cyber System at any point in the software development lifecycle
- Of vendor hardware such as malicious chip or board level implants or modifications, or malicious factory configuration
- Of manufacturing specifications or proprietary information that could be used by a malicious actor to exploit physical or cyber vulnerabilities
- Discovery of a back door or other potential for unauthorized electronic access to a BES Cyber System
- Vendor software (known or active exploitation of a software vulnerability by a malicious actor)



Vendor Network Compromises

- To a vendor's computer network used for access to an entity's BES Cyber System(s)
- Of a vendor's trusted communication channels that may have been used to transmit malicious messages to an entity, such as:
  - postal shipped items
  - compromised file transfer systems or
  - social engineering methods e.g. (phishing or vishing)
- Of a vendor's authorized remote access to an entity's network by a malicious actor

Vendor Employee Compromises

- Vendor employee or anyone acting on behalf of vendor
- Vendor employee or anyone acting on behalf of vendor perpetuating a cybercrime or physical crime that indicate an increased risk to their customers, such as
  - Computer Fraud and Abuse Act
  - Computer espionage
  - Theft
  - Trespassing
  - Acts of violence
- Linked to terrorist organization, or organizations that promote attacks against the electric power industry

Coordination of Responses to Vendor-Identified Incidents

Vendor Identification

- Actual or potential
- Notified by a third party (could be the affected utility)

E-ISAC ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER

- Publicly Disclosed
- The Vendor should implement its notification process in a mutually agreed upon time and method

Incident Information Needed

- Circumstantial and technical details
- Remedial steps being undertaken
- Recommended mitigations
- Method and timing for sharing updated information

Disclosure Options

- Direct Individual Entity notification based on methods established during procurement

Based on the size and scope of the incident, direct communications with the entity might not be a viable first means of notification.

- Disclose Publically
- Disclose through an advisory organization
- Follow up with entities through established communication channels.

Incident Response Lifecycle Considerations

- Be prepared to activate your established incident response plan.
- If an incident is discovered internally, determine the size and scope of the incident and report accordingly, as defined by the entity's plan.
- Establish ongoing communication methods between the vendor and the entity.
- Specific questions requiring vendor response should follow the methods for conveying these questions that were established and agreed upon during the procurement process.

Incident Response Lifecycle Considerations

- Incident action plans designed in accordance with the type of incident, impact, and stage of detection can support the response plan. Incident action plans establish standard response measures based on the stage and potential impact of the affected system or service.
- Be specific in reporting and notifications to E-ISAC as to your observations of the incident, and attach information that the vendor has already released.
- After the incident, conduct a post mortem review with the vendor, focusing on the interaction, coordination, and communication that took place throughout the response time.

Security Control Improvements

- After completion of the vendor-identified incident investigation and determination of its root cause, evaluate the associated security controls and improvements identified during the post mortem, to help prevent future incidents. The vendor should provide documented evidence of the implemented changes.
  - Apply internal mitigating security controls to reduce the risk
  - Document and communicate any issues which were not addressed
  - Engage management and/or senior leadership of the vendor as needed, to impress on them the importance of the control(s) or mitigation(s) and the need to implement appropriate measures
  - Communicate to the vendor that unresolved issues may impact future scoring or evaluation of new purchases of products or services or renewal of existing product and service contracts
  - Evaluate terminating the relationship with the vendor
  - If appropriate, take legal action

Security Control Improvements

- 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

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