NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Secure Equipment Delivery

Security Training Session

Wally Magda, Senior Standards and Training Advisor
Critical Infrastructure Protection Committee
June 4, 2019 | Orlando, FL

RELIABILITY | RESILIENCE | SECURITY




Agenda

- Introduction
- Assessing Risk and Cost-Benefit
- Transportation Decisions
  - Enhanced Packaging
  - Tracking versus Chain-of-Custody
- Delivery and Storage
  - Incoming Inspection
  - Secure Facilities and Staff
- Incident Management
- Working with your Vendor
- Conclusion
- Q&A

Introduction

- An important element of an organization's Supply Chain Risk Management Program is:
  - **safeguarding the transportation of "information systems and components, or applicable system and communications interfaces."**
- Guidance in ISO / IEC 27002:2013 help ensure that**:**
  - **"the delivered information and communication technology products are functioning as expected without any unexpected or unwanted features"**.
- This paper highlights some of the aspects to consider regarding secure transportation and delivery of systems and components, from component manufacturers to integrators, to vendors, and ultimately to the Bulk Electric System (BES).

NIST SP 800-161 – *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*
ISO/IEC 27002:2013 – *Information technology – Security techniques – Code of practice for information security controls*

Assessing Risk and Cost-Benefit

- Risk management starts with an estimate of the risk to the BES should a product be received already compromised.
- First evaluate
  - the nature of the equipment,
  - the sensitivity of the operation for which the equipment is intended to take part, and
  - its ability to affect networks and other elements of the system.

Assessing Risk and Cost-Benefit

- Consider
  - possible methods by which the device can be compromised and
  - how easily this might be discovered at incoming inspection.
    - For example,
      - if compromise would require disassembly of the device and reprogramming chips, the security risks will be different from a device that can be reprogrammed through a communications interface.
      - Include in procurement language that the vendor must have processes in place to address supply chain risk for component vendors, including incident response and secure delivery where appropriate.

Assessing Risk and Cost-Benefit

- The risk presented by the device is a combination of
  - the likelihood that it might be compromised,
  - the criticality of its function and placement in the system, and
  - the probability that a compromise would be discovered before the device is placed into service.
- Enhanced controls for shipping, handling, and storage should be considered for devices that are both critical to the operation and difficult to inspect.
- A cost-effective strategy for secure equipment delivery must consider risk and the cost to secure the equipment in question.
  - If the security cost outweighs the potential impact a compromised product would have on the BES, other strategies should be considered.

Transportation Decisions

- Once you have analyzed the
  - type of equipment and
  - level of risk, and the
  - options available for secure delivery,
    - choose the carrier and services required to ensure the appropriate level of security.
- Maintain a list of carriers that meet the requirements for transport of particular components or systems.

Transportation Decisions

- Enhanced Packaging
  - Risks can be further reduced through enhanced security measures such as:
    - Tamper evident tape;
    - Security inks;
    - Truck/trailer serialized steel bands or security seals;
    - RFID (tracking only);
    - Blister or clamshell packaging.

Transportation Decisions

- Tracking versus Chain-of-Custody
  - Based on the analysis discussed above,
    - the equipment can be tracked (an available option for most carriers including USPS and courier services) or
    - you can require additional chain-of-custody procedures.
  - Tracking records the movement of a package from facility to facility.
  - Chain-of-custody provides evidence of the identity of each person or entity who had access to it during its movement.
    - This helps to ensure that equipment remains
      - "***in the same condition from the moment it was sealed in the container at origin until the moment it was released into the receipted custody of another***", and
      - provides accountability for discrepancies.

https://www.maritime-executive.com/article/tracking-and-chain-of-custody-the-difference

Delivery and Storage

- Security does not end once the equipment is delivered to its destination.
  - consider incoming inspections and processes
  - secure storage facilities
  - internal chain-of-custody through deployment of the equipment.

Delivery and Storage

- Incoming Inspection
  - Incoming inspection provides an opportunity to
    - formalize awareness and
    - reduce risk by applying simple checks and recording evidence of findings, including
    - careful documentation of exceptions.
  - The receiving inspection procedure should dictate
    - who the receiving operator should contact for further scrutiny of the package if any damage or other compromise is detected.
    - For freight deliveries, it is advised to take several photos of the unopened package while the product is still in the truck when any damage or possible compromise is found.
  - Inspection records should be retained, as they may become of interest if the subject item is involved in an incident.

Delivery and Storage

Here are some inspection steps to consider:

- Is the carrier the one(s) normally used by the vendor?
- Was there any unexpected delay between shipment by the vendor and receipt of the item?
- Was the packaging and its condition consistent with other shipments from the same vendor?
- Was there any evidence on the packaging or the device indicating it may have been opened?
- In the case of equipment, when the unit is first powered up, is it in the expected state? Do logs show unexpected events? Does it indicate the expected version(s)? The expected state should be noted for a new vendor or product and those expectations be made part of incoming inspection.
- If the shipment includes software media, is it packaged as expected?

Delivery and Storage

- Secure Facilities and Staff
  - Restricted access to receiving and warehouse facilities is among the best controls for maintaining the integrity of the equipment prior to installation to the BES.
    - Based on risk, additional measures may be warranted, such as secure cages and video monitoring.
  - In addition to security measures taken when hiring receiving and warehouse staff,
    - assess and implement training and awareness required for each position.

Incident Management

- Consider establishing processes to be followed if
  - a shipment is received damaged or in a condition that suggests tampering, or if a shipment is lost.
  - Procedures for logging incident management activities, handling of evidence, communication and escalation should be documented and clearly communicated to management and other applicable personnel, and those procedures should be followed when an incident occurs.
- Where appropriate, post-incident analysis should be conducted in coordination with the vendor and the carrier. Detailed guidance on information security incident management can be found in ISO / IEC 27035 and NIST SP 800-161.

ISO/IEC 27035 – Security incident management

Working with your Vendor

- Establish confidence in each vendor's policies and procedures for supply chain security during the initial qualification stage, including transportation service providers.
- Know your preferred vendors' processes for handling shipments that appear to have been tampered with or damaged.
- Provide clear and timely communication regarding enhanced security requirements for any given shipment.

Conclusion

- Cargo theft, lost or damaged equipment, and malicious tampering are unfortunate realities in today's world; however, an increasing focus on security in-transit presents a number of choices for mitigating the risk of receiving compromised equipment.
- 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.

Summary

- Assessing Risk and Cost-Benefit
- Transportation Decisions
  - Enhanced Packaging
  - Tracking versus Chain-of-Custody
- Delivery and Storage
  - Incoming Inspection
  - Secure Facilities and Staff
- Incident Management
- Working with your Vendor

Questions and Answers