National Institute of Standards and Technology

Best Practices in Cyber Supply Chain Risk Management

Conference Materials

Cyber Supply Chain Best Practices

In a Nutshell: Cybersecurity in the supply chain cannot be viewed as an IT problem only. Cyber supply chain risks touch sourcing, vendor management, supply chain continuity and quality, transportation security and many other functions across the enterprise and require a coordinated effort to address.

Cyber Supply Chain Security Principles:

1. **Develop your defenses based on the principle that your systems will be breached**. When one starts from the premise that a breach is inevitable, it changes the decision matrix on next steps. The question becomes not just how to prevent a breach, but how to mitigate an attacker's ability to exploit the information they have accessed and how to recover from the breach.
2. **Cybersecurity is never just a technology problem, it's a people, processes and knowledge problem**. Breaches tend to be less about a technology failure and more about human error. IT security systems won't secure critical information and intellectual property unless employees throughout the supply chain use secure cybersecurity practices.
3. **Security is Security.** There should be no gap between physical and cybersecurity. Sometimes the bad guys exploit lapses in physical security in order to launch a cyber attack. By the same token, an attacker looking for ways into a physical location might exploit cyber vulnerabilities to get access.

Key Cyber Supply Chain Risks: Cyber supply chain risks covers a lot of territory. Some of the concerns include risks from:

- Third party service providers or vendors – from janitorial services to software engineering -- with physical or virtual access to information systems, software code, or IP.
- Poor information security practices by lower-tier suppliers.
- Compromised software or hardware purchased from suppliers.
- Software security vulnerabilities in supply chain management or supplier systems.
- Counterfeit hardware or hardware with embedded malware.
- Third party data storage or data aggregators.

Examples of Cybersecurity Questions: Companies are using the following questions to determine how risky their suppliers' cybersecurity practices are:

- Is the vendor's software / hardware design process documented? Repeatable? Measurable?
- Is the mitigation of known vulnerabilities factored into product design (through product architecture, run-time protection techniques, code review)?
- How does the vendor stay current on emerging vulnerabilities? What are vendor capabilities to address new "zero day" vulnerabilities?
- What controls are in place to manage and monitor production processes?

- How is configuration management performed? Quality assurance? How is it tested for code quality or vulnerabilities?
- What levels of malware protection and detection are performed?
- What steps are taken to “tamper proof” products? Are backdoors closed?
- What physical security measures are in place? Documented? Audited?
- What access controls, both cyber and physical re in place? How are they documented and audited?
    - How do they protect and store customer data?
    - How is the data encrypted?
    - How long is the data retained?
    - How is the data destroyed when the partnership is dissolved?
- What type of employee background checks are conducted and how frequently?
- What security practice expectations are set for upstream suppliers? How is adherence to these standards assessed?
- How secure is the distribution process?
- Have approved and authorized distribution channels been clearly documented?
- What is the component disposal risk and mitigation strategy?
- How does vendor assure security through product life-cycle?

Examples of Cyber Supply Chain Best Practices: Companies have adopted a variety of practices that help them manage their cyber supply chain risks. These practices include:

- Security requirements are included in every RFP and contract.
- Once a vendor is accepted in the formal supply chain, a security team works with them on-site to address any vulnerabilities and security gaps.
- “One strike and you’re out” policies with respect to vendor products that are either counterfeit or do not match specification.
- Component purchases are tightly controlled; component purchases from approved vendors are pre-qualified. Parts purchased from other vendors are unpacked, inspected, and x-rayed before being accepted.
- Secure Software Lifecycle Development Programs and training for all engineers in the life cycle are established.
- Source code is obtained for all purchased software.
- Software and hardware have a security handshake. Secure booting processes look for authentication codes and the system will not boot if codes are not recognized.
- Automation of manufacturing and testing regimes reduces the risk of human intervention.

- Track and trace programs establish provenance of all parts, components and systems.
- Programs capture “as built” component identity data for each assembly and automatically links the component identity data to sourcing information.
- Personnel in charge of supply chain cybersecurity partner with every team that touches any part of the product during its development lifecycle and ensures that cybersecurity is part of suppliers’ and developers’ employee experience, processes and tools.
- Legacy support for end-of-life products and platforms; assure continued supply of authorized IP and parts.
- Tight controls on access by service vendors are imposed. Access to software is limited to a very few vendors. Hardware vendors are limited to mechanical systems with no access to control systems. All vendors are authorized and escorted.