Cyber-Supply Chain Risk Management Best Practices

Interview Questions

- What is the organization's structure for managing supply chain risk? What roles are involved in risk management decisions?
- What are the key business drivers for allocating resources for cyber supply chain risk management?
- Where does the organization see benefits from effective cyber supply chain risk management?
- How does the organization identify supply chain threats, vulnerabilities and overall risks?
    - How are these risks prioritized or measured?
    - What does the organization consider to be major supply chain risks? (examples: quality or products (received or produced), supply chain resiliency, third-party cybersecurity, counterfeits)
- What requirements does the organization put in contracts and service agreements, e.g., security, quality, integrity, etc.? Can provide examples?
    - How does the organization monitor compliance with contractual requirements? How often?
- Has the organization ever felt a need to help a supplier improve their cybersecurity/supply chain practices?
- How does the organization vet or manage third-party suppliers/vendors?
    - Is the organization's cybersecurity considered? Evaluated?
    - If a questionnaire is used, is it a standardized questionnaire, or internally developed? Why?
    - If an audit is required, how are auditors chosen? - do they have cybersecurity expertise?
    - Are suppliers vetted differently depending on what they provide, their size, or some other reason?
    - What kinds of information are collected about suppliers?
- What methods does the organization use to protect their supply chain? (Especially from cybersecurity-related threats)
    - How does the organization assure quality and integrity of products/software they receive?
    - How does the organization track the provenance of a product?
    - How does the organization prevent tampering of products in the supply chain?
    - What methods for protecting supply chains have been most effective?
    - What key metrics does the organization track for cyber supply chain risk management? Is there an executive dashboard to capture and share those metrics?
    - With whom are those metrics shared?
- What standards or guidelines has the organization implemented to assure the quality, integrity, physical and cybersecurity of products?

- Is supply chain risk included in cybersecurity policy? Is cybersecurity included in supply chain management policy?
- Does the organization have a plan to manage cybersecurity-related supply chain incidents?
- What makes implementing cyber-supply chain risk management difficult?
- What tools/techniques has the organization found most valuable in managing their supply chain risk?
- What resources would the organization suggest useful to organizations less mature in managing their supply chain risks?