National Counterintelligence and Security Center
Supply Chain Directorate

Supply Chain Risk Management
Best Practices

Introduction: The U.S. is under systematic assault by Foreign Intelligence Entities[1] (FIEs) who have augmented traditional intelligence operations with nontraditional methods, including economic espionage, supply chain exploitation, and the use of students, scientists, and corporate employees, to collect both classified and unclassified information. The scale of this effort has put entire industries at risk.

Specifically, the globalization of supply chains presents a major attack vector, characterized by a complex web of contracts and subcontracts for component parts, services, and manufacturing. FIEs use this complexity to obfuscate efforts to penetrate sensitive research and development programs, steal vast amounts of personally identifiable information (PII) and intellectual property (IP), and insert malware into critical components. Supply chain exploitation, especially when executed in concert with cyber intrusions, malicious insiders, and economic espionage, threatens the integrity of key U.S. economic, critical infrastructure, and research/development sectors. The following "best practices" provide options to address this threat.

Governance and Administrative Actions

Establish Internal Policies and Processes

- Develop internal company policies and processes that implement Supply Chain Risk Management (SCRM).
- Identify and document roles and responsibilities across the enterprise.
- Create a Capability Maturity Model (CMM) for the SCRM program.
- Delineate decision making authority and escalation process.
- Ensure that SCRM is part of the organization's annual enterprise risk assessment process.

This will address cross-organizational understanding of roles, policies, and processes, as well as establish metrics for the CMM.

Identify a Supply Chain Risk Manager

- Select an executive accountable for SCRM within the organization.
- Chair SCRM executive board meetings.
- Develop and implement SCRM program for the organization.

[1] (U) Foreign intelligence entity refers to any known or suspected foreign state or non-state organization or person that conducts intelligence activities to acquire U.S. information, block or impair U.S. intelligence collection, influence U.S. policy, or disrupt U.S. systems and programs.

- Participate in organization's Executive Risk Management function.

The SCRM executive board must include senior leaders from across the organization (e.g. logistics, information technology, acquisition, security, human resources, legal, etc.) in order for the SCRM program to be successful. Representation from across the enterprise will ensure that senior leaders are stakeholders in the supply chain program.

Enhance Contract Language for Supply Chain Security

Ensure contract language with key suppliers includes:

- Metrics for supply chain security along with cost, schedule, and performance.
- An audit capability for key suppliers' supply chain processes.
- Ability to verify compliance with applicable laws, regulations, and industry standards.
- Implementation of SCRM requirements into contractual language with third party vendors.

These steps will allow better insight and thus better oversight of any potential risks to your supply chain. Further, in the event there is a security breach at a third party organization, these contractual enhancements will allow for a more expedient and effective response to minimize the damage from such a breach.

Education, Training, and Awareness Actions

Training

- Ensure that everyone within the organization -- from the SCRM professionals to stakeholders of the SCRM processes (such as line and program managers) -- receive training on SCRM awareness and practices.
- Ensure SCRM professionals are offered SCRM-related training, such as acquisition, cyber security, etc.
- Update training annually to address evolving information regarding SCRM threats and defenses.

Training is an essential element in helping to ensure employees are aware and able to support SCRM within the organization.

Certifications

- Pursue professional certifications.
- Maintain Continuing Professional Education (CPE).

Certifications help ensure that the breadth of the supply chain process is understood. Knowledge is generally required in multiple areas of the certification subject and usually requires CPE credits to stay current.

Information Sharing

- Participate in information sharing venues.
- Attend conferences and SCRM forums.

Participation in information sharing venues with other companies, SCRM associations, and government SCRM forums can help one keep abreast of the latest threat reports, best practices, and lessons learned from specific organizations.

Mitigation Actions

Identify Critical Assets and Services

- Identify those assets and services most critical to the organization.
- Determine the risk tolerance and tradeoffs regarding protecting those critical assets and services.
- Develop contingency plans to restore critical assets and services.

The SCRM executive board and stakeholders should determine which assets and services are most critical to the organization's mission. These determinations can inform the business impact analysis.

Conduct SCRM Assessments

- Audit the SCRM processes.
- Document audit results, clarify findings, and incorporate lessons learned into the SCRM processes and CMM.
- Perform ad hoc SCRM assessments and exercises to validate processes.
- Encourage continuous improvement in SCRM processes.

Performing SCRM assessments as part of the organization's annual enterprise risk assessment process will ensure there is a comprehensive look at threats, vulnerabilities, and risks, and that information is captured for critical assets/services.

Exercise Due Diligence on Suppliers

- Conduct research and due diligence on suppliers prior to doing business with them.
- Build an understanding of suppliers' security practices.
- Procure components from authorized sellers, whenever possible.
- Change the paradigm from focusing primarily on lowest cost to focusing on best value.
- Reward employees for executing robust due diligence in acquisitions.

Incentivize staff for the discovery of "best value" vendors rather than rewarding staff for finding the lowest cost provider (the current practice in most cases). This new paradigm evaluates prospective vendors with respect to supply chain risks against performance and costs. Exercising due diligence will not only increase the integrity of the organization, it will also reduce the supply chain risks to the organization and customers.

Perform Damage Containment and Strengthen Defenses

When damage from a compromise occurs:

- Determine the breadth and depth of the compromise.

- Contain the compromise.
- Assess damage caused by compromise.
- Develop and share lessons learned with other SCRM stakeholders within the organization.
- Use the lessons learned to help advance the CMM.

Containing and assessing the damage will help ensure that it does not spread and will help minimize impact to the overall mission of the organization.