Supply Chain Risk Management (SCRM)

Supply Chain Risk Management (SCRM) is the process of identifying, assessing, and neutralizing risks associated with the global and distributed nature of product and service supply chains.

The globalization of the U.S. economy presents unique and complex challenges when applying SCRM methodologies to safeguard the U.S. Government (USG) supply chain from emerging threats and vulnerabilities. The presence and influence of foreign governments, poor manufacturing and/or development practices, counterfeit products, tampering, theft, malicious software, etc., are examples of supply chain risks that must be mitigated. Federal agencies, government contractors, suppliers, and integrators use varied and non-standardized practices, making it difficult to consistently evaluate, measure, and neutralize threats to the USG supply chain.

Federal agencies should develop a SCRM strategy that accounts for known and emerging threats, vulnerabilities, and organizational impacts. Federal agency supply chains are as unique as the individual agencies they support. No one SCRM strategy can be universally applied across the federal government, but federal agencies should follow the established National Institute of Standards and Technology SCRM standards as a foundation of their own strategy. SCRM will require USG agencies to establish a coordinated team approach to assess supply chain risk and actions necessary to mitigate the risk to an acceptable level. The backbone of the team should consist of a diverse group of professional disciplines with expertise in supply chain risk management, security, procurement, contract and administrative law, audit and finance, and facilities management. SCRM should leverage a variety of resources, including open source commercial products, to build a risk assessment baseline that includes a potential vendor's legal history, financial solvency, tax history, and corporate relationships. Initial research should be combined with a detailed risk assessment focused on counterintelligence threats. The guide below provides detailed risk assessment questions to review during the SCRM process.

Recommendations for Developing a Supply Chain Risk Assessment

An effective risk assessment begins with that agency's understanding of its supply chain and its vulnerabilities. Risk assessments are mechanisms to research, identify, and assess the security, integrity, quality, and resilience of the procured products and services.

Providers of Products and Services

Identify the location of a service provider. If in a foreign country, identify potential relationships between the foreign government and the provider (suppliers, vendors, etc.). Identify the foreign country's laws or policies which enable it to request sensitive business information from the provider. Request the names, addresses, and role of foreign individuals associated with, or who have access to the provider.

- Where is the provider headquartered, and where are their manufacturing and service facilities located (i.e., United States or a foreign country)?
- Does the provider have relationship with a foreign government?
    - To what extent is the provider foreign government-owned?

    - Does the provider receive subsidies or preferential treatment from a foreign government?

Identify if the provider employs foreign nationals. Determine who sponsors the visas, the length of time each individual is allowed to stay, and the importance of the technical skills or capabilities of each foreign national and whether a foreign country (with particular focus on the employee's home country) has expressed a need for similarly skilled workers and consider the impact of foreign nationals knowledge of USG use the product or service. Foreign governments may seek to exploit provider vulnerabilities via their intelligence services.

- How well do providers vet employees?
    - Do they have non-U.S. personnel?
    - Do they perform background checks or previous employment verification?
        - Consider disqualifying requirements such as criminal records, and falsifying or over stating previous employment or skill level.
    - Does the provider have any known connections to foreign intelligence services?

Review open source information (and classified where applicable) regarding a provider's history of intellectual property theft. Identify what was compromised or stolen, when, and if possible, by whom. Consider the potential impact to USG national security. Also consider foreign countries' national security interests as they relate to the United States and the compromised product or service. If the history of intellectual property theft is unknown, request information relating how suppliers or vendors safeguard their intellectual property.

- Do providers have a history of or been accused of intellectual property theft?
- Have providers been a victim of intellectual property theft?
    - Did an employee improperly share sensitive information or provide access to a facility?
    - Was there a computer network intrusion?
- How do providers protect their internal computer networks?
- Has the provider been a victim of a computer network intrusion?

Identify and review the provider's processes and procedures to verify the quality of its products or third-party products and services. Consider the impact to the USG if a compromised product is acquired and integrated to USG systems and facilities.

- How is the quality of product verified?
- What mechanisms are in place to ensure products meet requirements?
- Does the agency have an inspection process in place to review materials and/or services?

Consider the provider's current financial state and their capability to meet requirements with current and increased demand. Review the financial background of a provider and consider the impact to the USG should the provider no longer be capable of fulfilling requirements.

- Is the provider financially stable?
- Is the provider subsidized by a foreign government?
    - Will they remain viable if the funding is reduced?
    - Are their stipulations with regard to government funding?

Distribution and Transportation

Review how products are transported from the provider to the USG. Identify the addresses of transshipment points and storage facilities. Identify individuals or government personnel who could have access to each location, and identify carriers' names and addresses of personnel who may have contact with products during shipment. Review the mode and route of transportation, the country's capability to interfere with the transportation of goods through its border patrol and customs services, and the physical security environment of transshipment and storage facilities. Consider the impact to the USG should products or service be compromised while in transport.

- How are products transported from the producer, manufacturer or service provider to the USG?
    - Are they transported overseas?
    - What are the transshipment points?
    - Will it be warehoused during transportation, if so, where?
    - Who owns or has access to those properties?
    - What transportation carriers would be used for transport?

Installation, Integration, and Maintenance

Review and evaluate how products and services are installed and maintained over time. Identify names and address of individuals who may have remote access to equipment before or after it is installed and those who may or need direct access to equipment in USG space. If foreign nationals have access, identify names of individuals and the degree and range of information each has access to. Consider the impact to national security or consequences if sensitive information, personnel, or facilitates are compromised.

- How are products and services incorporated or installed into existing systems and protocols?
- Who has access to sensitive business information, customers, or facilities?

Disposal and Retirement

Determine what electronic equipment should be cleaned or otherwise wiped of sensitive information prior to disposal or retirement. Identify the names of individuals responsible for removing sensitive data from hard drives, and those responsible for the physical removal of equipment from USG property. Determine what happens to the equipment after disposal or retirement. Identify if it is refurbished or resold, and the names and addresses of companies who could purchase or otherwise acquire such equipment.

- What level of scrutiny does the agency need to ensure sensitive data is not improperly disclosed when retiring or destroying equipment?
- What happens to disposed equipment?
    - Is it refurbished and resold?

Neutralize Risks to the USG Supply Chain

USG procurement personnel shall aggregate the research regarding threats, vulnerabilities, and their impact. Recommend actions necessary to neutralize risks to an acceptable level. These recommendations should comply with federal acquisitions regulations as well existing federal department or agency policies procedures.

Common Mitigation Techniques

- USG should have regular communication and maintain a collaborative relationship with its providers.
- USG should request onsite audits of product development, manufacturing facilities, and physical and cyber security standards of its providers.
- USG should request providers to establish and maintain visitor logs.
- USG should request advanced notice of change in provider's ownership or product development.
- USG should encourage providers to have a certified legal authority review contracts and agreements to ensure protection of intellectual property, processes, or other sensitive material.

Additional Information:

Department of Commerce
National Institute of Standards and Technology
SP 800-161 Supply Chain Risk Management Practices for Federal Information Systems
http://scrm.nist.gov

Office of the Director of National intelligence
Intelligence Community Directive 731
http://dni.gov

Defense Security Service
National Industrial Security Program
http://www.dss.mil/isp/index.html

Federal Bureau of Investigation
http://fbi.gov

Joint Duty Assignments:

The FBI is establishing joint duty assignment opportunities to better liaison and share SCRM related intelligence with interested agencies. Interested participants should contact the FBI at (202) 324-2376.

Informational Sessions:

The FBI is an active member of the Office of the Director of National Intelligence's (ODNI) National Counterintelligence and Security Center (NCSC) Supply Chain Directorate. NCSC's mission is to lead and support the counterintelligence and security activities of the U.S. Government, the U.S. Intelligence Community, and U.S. private sector entities that are at risk of intelligence collection, penetration or attack by foreign and other adversaries. In support of its mission, NCSC develops and implements unifying intelligence strategies across functional areas, including supply chain risk management. NCSC will provide SCRM informational sessions for interested government agencies upon request. The informational sessions will provide agencies an opportunity to learn more about SCRM mitigation techniques, share SCRM mitigation techniques, and network with key SCRM personnel. To schedule an information session or learn more about the NCSC's Working Group, please contact (202) 324-1735.

February 2016