NetImpact Strategies

Assessing Vendors for Cyber-Supply Chain Risk

A Field Guide for Federal Procurement Professionals

NetImpact Strategies, Inc.

7600 Leesburg Pike, West Building, Suite 140, Falls Church, VA 22043
(703) 559-3280 | www.netimpactstrategies.com

Introduction

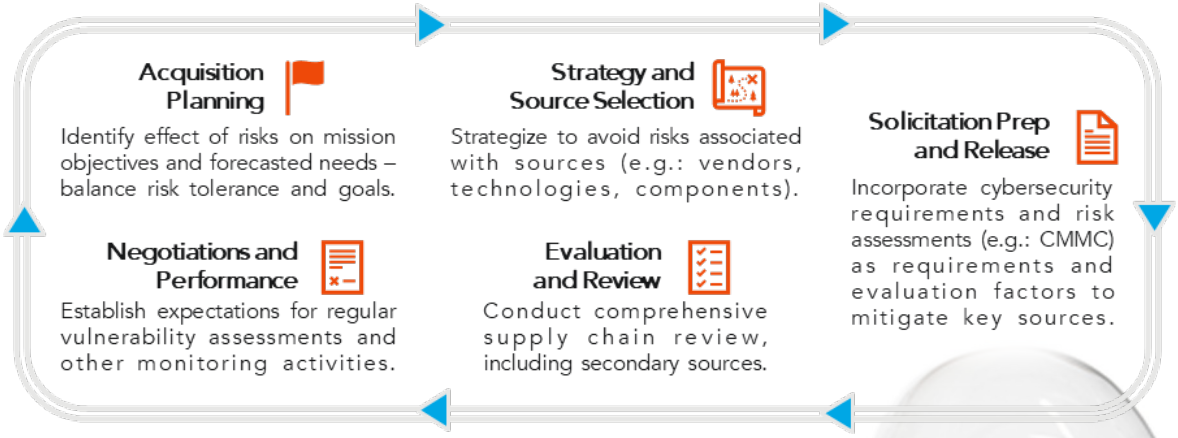
Vendors are an integral part of the federal procurement process, providing goods and services that are essential to government operations. However, these vendors also present significant cybersecurity risks as they may introduce vulnerabilities into the government's supply chain. To mitigate this risk, federal procurement professionals must assess the cyber-supply chain risk within the vendor ecosystem. Acquisition professionals play a critical role in implementing Cyber-Supply Chain Risk Management (C-SCRM). They are responsible for ensuring that cybersecurity is integrated into the procurement process and that the vendor meets security requirements to reduce the risk of cyber-attacks and ensure the integrity and security of the supply chain. This field guide highlights some key challenges and offers practical solutions to building cyber-supply chain risk mitigation from an acquisition perspective.

Understanding Cyber-Supply Chain Risk

A cyber-supply chain refers to the interconnected web of suppliers, manufacturers, and service providers responsible for creating and delivering products or services. In this context, cyber-supply chain risk refers to the potential for vulnerabilities in the chain that may result in a cyber incident, such as unauthorized access, data breaches, or the disruption of critical services.

Cyber-Supply Chain Risk Sources

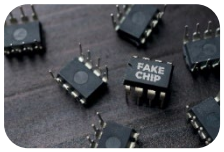
Risk sources are the various points within a supply chain where vulnerabilities and threats related to cybersecurity can originate. Identifying the risk source is an essential first step in risk management and mitigation for the federal procurement process because it reveals potential weak links whether additional attention needs to be applied as procurement specialists formulate acquisition strategies. Gaining insights into risk sources empowers the procurement team to make informed decisions regarding acquisition process, risk tolerance, vendor selection, and the implementation of appropriate security measures as acquisition progresses.



By proactively identifying and addressing these risk sources, the federal procurement process becomes a powerful mitigation force to significantly reduce the likelihood of supply chain disruptions, minimize cyber-attack severity, and lay the foundation for a healthy and resilient supply chain ecosystem.

Key Cyber-Supply Chain Risk Sources.

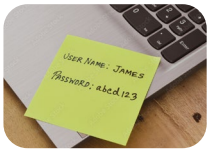
Identifying and mitigating these risk sources is crucial to ensuring the security and integrity of the overall supply chain ecosystem.



Hardware and Software Components

Compromised parts, including counterfeit products, jeopardize performance, security, and customer trust.

Malicious actors may introduce malware into a vendor's products and its smaller components or deliver counterfeit components entirely, compromising the integrity and security of an organization's infrastructure.



Vendor System Vulnerabilities

Lax or insufficient security measures open doors for other cyber threats and create indirect attack opportunities that ultimately affect mission infrastructure.

Leveraging a vendor's vulnerabilities, malicious actors and unwitting insiders can expose an organization to cyber threats. With these exploitations, data leaks, stolen sensitive IPs, and data loss may occur, jeopardizing the vendor and the entire supply chain.

Data Leaks

Unauthorized or accidental disclosure of protected information is one of the most significant risks.

External and internal attackers exploit software, hardware, or personnel vulnerabilities to release and obtain information. A data leak can result in the loss of sensitive data, including intellectual property, confidential information, and personally identifiable information (PII). This can lead to significant reputational damage, destruction or corruption of databases, exposure of individuals and businesses, theft of intellectual property and identities, financial loss (including compensating victims), and regulatory implications.

Malware Attacks

Bad actors deploy malicious software to infiltrate an organization's information systems and cause damage.

Malware can be introduced into an organization's supply chain through various means and can take the form as viruses, worms, ransomware, or spyware. They are designed to disrupt operations, steal information, gain unauthorized access, or even control the system. Timeliness of detection play a critical role as the compromise can lead to significant financial losses, reputational damage, and the undermining of critical infrastructure and remediation effectiveness worsens with delays.

Component Reuses

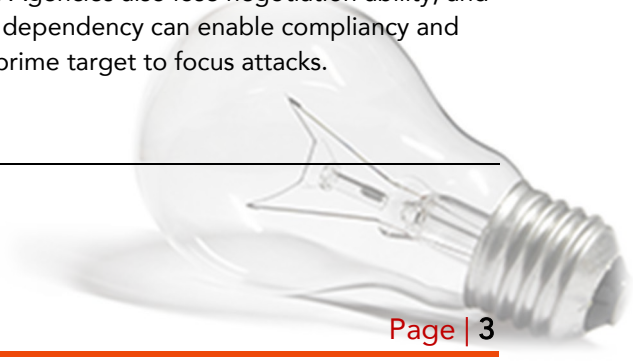
Reusing components and not evaluating the vulnerability of reused components amplifies and compounds risks.

As vulnerable components are reused, they become a common exploitation point and widen the attack surface for malicious actors. Attackers exploiting these vulnerabilities can launch widespread attacks that may now affect a large number of systems and require an enterprise-wide, coordinated effort to address. The origin issue scales and degrades the overall security posture.

Vendor Homogeneity

A lack of vendor or geographical diversity creates a single point of failure where events have a cascading effect.

The dependency and reliance on a small and homogenous vendor portfolio mean mission-critical software and services have reliance on a single point of failure, which means delays and attacks affecting the vendor can severely disrupt and shut down mission operations. Agencies also lose negotiation ability, and this known dependency can enable compliancy and become a prime target to focus attacks.



Mitigating Cyber-Supply Chain Risk: An Acquisition Perspective

Mitigating cyber supply chain risks is of paramount importance for procurement specialists as their work upfront affects the security and integrity of the agency's supply chain ecosystem and the long-term sustainability and reliability of the goods and services procured. As the threat landscape continues to evolve and cyberattacks become more sophisticated, it is crucial for procurement professionals to adopt proactive strategies and measures to safeguard their procurement processes and mitigate potential vulnerabilities. The recommendations and best practices below are practical risk mitigation within the federal procurement process.

- **Ensure all SOWs, RFPs, and RFQs include security requirements to include supply chain risk management**:
  Federal procurement professionals must ensure that all acquisition documents, including Statements of Work (SOWs), Requests for Proposals (RFPs), and Requests for Quotes (RFQs), include security requirements that cover supply chain risk management. These requirements should be well-defined and should cover all aspects of the supply chain, including hardware, software, and services. The requirements should also include specific cybersecurity controls and policies that vendors must comply with. Procurement professionals should ensure that vendors understand these requirements and can demonstrate compliance during the vendor assessment process. Requiring validated controls through certifications like Cybersecurity Maturity Model Certification (CMMC) and ISO 27001 as part of solicitation Go-No-Go criteria indicates good cyber hygiene. These certifications provide guidelines for critical security policies, practices, and processes to include controls for supply chain risk management as they mandate organizations to implement controls to mitigate identified risks and continuously monitor and review their risk management processes' effectiveness. Requesting vendor's documents or providing a Supply Chain Risk Management Plan based on NIST 800-161 enables acquisitions teams to understand better the prioritization of cybersecurity and the flow down of these controls and practices to subcontractors.
- **Ensure that vendors document their Supply Chain Risk Management Plan**:
  As part of the vendor assessment process, procurement professionals must ensure that vendors document their Supply Chain Risk Management (SCRM) plan. This plan should include details on the vendor's approach to managing cyber-risks and the flow-down of their SCRM policies and procedures to vendors. The plan should also outline the specific cybersecurity controls and policies the vendor has implemented to mitigate risks.
- **Develop a rigorous vendor assessment process**:
  Procurement professionals must develop a rigorous vendor assessment process to identify and assess supply chain risks. This process should include identifying the geographical location of the vendor, company ownership, past cyber incidents, and vendor concentration. The assessment process should also include evaluating the vendor's policies and procedures for managing supply chain risks, including their incident

response procedures and business continuity plans. The assessment process should also review the vendor's contracts, memorandum of understanding, approach to information sharing throughout the supply chain, and service level agreements to ensure they align with the government's cybersecurity requirements. In addition, the assessment process must ensure that the vendor has secure development policies and practices, access policies, and incident response and communication procedures. Procurement professionals should require documentation of these policies and procedures as part of the proposal submission as an appendix to the Technical Volume.

- **Ensure that all proposed vendors are identified and added to the vendor assessment**: Federal procurement professionals must ensure that all proposed vendors are identified and added to the vendor assessment process. This includes vendors that provide hardware, software, and services critical to government operations. Procurement professionals should also ensure that vendors provide sufficient details on their supply chain, including subcontractors and vendors.
- **Require risk mitigation across the complex vendor ecosystems**: Federal procurement professionals must assess not only their primary vendors but also the entire ecosystem of vendors that these primary vendors use. This complex network of vendors can make it challenging to identify and manage potential security risks effectively. Federal procurement professionals can ensure that all vendors in the supply chain comply with cybersecurity regulations and standards by requiring flow-down terms to all subcontractors and making the Prime contractor responsible for reviewing their subcontractor's cybersecurity practices, evaluating their security posture, and ensuring that all vendors they use meet the required cybersecurity standards.
- **Emphasize training and awareness to improve skills**: Training and Awareness is a critical component in mitigating cyber supply chain risk from an acquisition perspective. Procurement professionals must ensure that all stakeholders involved in the acquisition process, including program managers, contracting officers, and technical evaluators, receive appropriate training and awareness to identify supply chain risks. This training should be tailored to different levels, including foundational and advanced levels, to ensure that all stakeholders have the necessary knowledge and skills to identify and assess supply chain risks. Procurement professionals should ensure that training and awareness programs are regularly updated to reflect the latest supply chain risks and best practices. Additionally, training programs should be mandatory for all stakeholders involved in the acquisition process to ensure that everyone has a consistent understanding of cyber supply chain risk management.
- **Adopt a centralized and standardized approach to manage and monitor vendors' cybersecurity risk:** A comprehensive vendor risk management software solution should enable procurement professionals to track all vendor-related information, including vendor contracts, compliance with regulations, and vendor risk assessments. Such a solution can also help

identify and manage vendor risks effectively by tracking and management of all cybersecurity-related tasks and activities. The software solution should be able to provide real-time updates and notifications of any changes in the vendor's cybersecurity posture, cyber incidents, performance, ownership or partnership changes, or compliance status. It should also enable procurement professionals to generate reports on vendor risk and compliance metrics, providing insights into areas that require additional focus and attention.

By following these recommendations in applying supply chain vigilance and the discipline of assessing vendor risks, federal procurement professionals enhance their agency's cybersecurity resilience against cyber threats, improve the ability to protect federal data and reduce the likelihood, impact, and damage of potential supply chain disruptions.

Conclusion

In conclusion, assessing vendors for cyber-supply chain risk is challenging and requires a comprehensive approach. Federal procurement professionals must take a risk management approach, prioritize cybersecurity, and ensure transparency and compliance with cybersecurity regulations and standards. By doing so, they can mitigate potential cybersecurity risks and protect the integrity of the supply chain.

NetImpact's DX360°® C-SCRM

NetImpact's DX360°® C-SCRM is a must-have tool for any organization looking to navigate and mitigate risks in its complex supply chain. With DX360°® C-SCRM, organizations regain the power of proactivity and the ability to reveal and neutralize threats – including ones traditionally obscured by the supply chain complexities. DX360°® C-SCRM enables organizations to identify, evaluate, and assess risk factors and make informed risk management decisions to achieve outcomes-focused compliance with NIST RMF and CSF, RMF for DoD IT, CNSS 1253, FedRAMP, ISO, and COBIT 5 guidelines. With a comprehensive library of potential risks and smart dashboards, C-SCRM provides real-time visibility into supply chain operations, including software security, and treatment plan recommendations to help you identify and treat potential risks that disrupt your supply chain ecosystem, which can threaten the entirety of your enterprise functions. DX360°® C-SCRM builds resiliency for your organization with each step, from detection through treatment.

Request a Demo

Experience a live, customized demo with our experts to learn how DX360°® C-SCRM or our other DX360°® products will make your mission fulfillment goals easier and safer.

Our products are sold as Software-as-a-Service (SaaS), which means your subscription includes maintenance and upgrades, eliminating expensive capital investments in hardware and software. Additionally, our Microsoft DX360°® products effortlessly integrate into your existing tenant so it won't be bogged down by accreditation processes either.

Experience immediate outcomes for mission value with rapid implementation in as little as two (2) weeks.

demo@netimpactstrategies.com

About NetImpact Strategies Inc.

NetImpact is a NextGen digital transformation leader disrupting how technology is applied to deliver mission value. Our team understands the challenges of managing and modernizing your agency's technology. That is why we have developed a portfolio of powerful, yet easy-to-use DX360°® apps that are designed to help you tackle your mission's most pressing needs. Building on our decades of experience in developing technology that integrates seamlessly into your ecosystem, we have harnessed the power of platforms from world-class partners like Microsoft to bring you a range of products for digital transformation in Government. These trailblazing applications are high-value, ready-to-use solutions tailored to federal missions and their evolving needs. Our DX360°® suite of high-performance digital solutions drives impact by delivering agile, outcome-focused results to securely transform client operations and accelerate mission outcomes at a fraction of the cost of traditional projects.