NetImpact Strategies

Mitigating the Risks Hidden in Your Software Supply Chain

NetImpact Strategies, Inc.

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

Introduction

Cyber - Supply Chain Risk Management (C-SCRM) has been in the news due to the number of high-profile cases impacting commercial and federal organizations. According to a study by Argon Security, in 2021 software supply chain attacks grew by more than 300% compared with 2020 with over 64% of organizations reporting that they were impacted by a software supply chain attack.

The increasing frequency and gravity of these supply chain attacks highlight the vulnerability of organizations to cyber threats that originate from third-party vendors and partners.

Additionally, the increased use of open-source software, the complexity of software supply chains, and the interdependency of components impact an organization's ability to assess and manage risk.

Notable Software Supply Chain Attacks

- In December 2020, over 100 private sector entities, 9 Federal agencies, and 18,000 customers are impacted by a supply chain attack on SolarWinds Orion, a platform that manages IT infrastructure.
- In 2020 the Microsoft Exchange Server reported four zero-day vulnerabilities.
- In late 2021, the Alibaba Cloud Security Team discovered the Log4Shell vulnerability affecting thousands of commercial and Federal applications using Java libraries.
- In 2021, hackers used ransomware to compromise Colonial Pipeline's IT systems and forced the company to shut down its entire pipeline for several days.

Cyber Supply Chain Risk Identification and Assessment

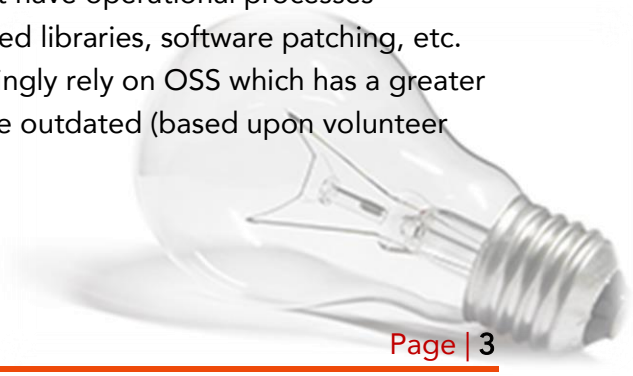
Software Supply Chain Attacks can occur during any stage of the software development lifecycle with the intention of gaining unauthorized access, conducting espionage, or facilitating sabotage. These attacks can range from simple tactics like disguising malware as legitimate software, to more advanced techniques like infiltrating and modifying the source code of genuine programs. To achieve their objectives, attackers may exploit various tools, dependencies, shared libraries, and third-party code, and even compromise the personnel and infrastructure of developers and distributors.

Identifying risks to your agency's systems entails mapping the complex relationships and interdependencies of software, components, IT assets, infrastructure, suppliers, and third-party vendors as well as understanding the policies and processes inherent in your system lifecycle. Risk identification and assessment must be consistently and continuously performed throughout this lifecycle:

- **Software Acquisition**: The processes and policies for managing software or systems acquisitions, understanding the complex software, vendor, and third-party relationships as part of Software Bill of Materials (SBOMs).
- **Software Development**: The processes and policies governing not only the agency's software development practices but the vendor's or supplier's practices, use/reliance on open-source artifacts, third-party tools, libraries, code snippets, packages, and other software resources or assets.
- **Implementation and Operations and Maintenance**: The operational processes and policies for testing, deploying, and upgrading artifacts in development, test, and production environments.
- **Retirement**: The processes and policies that ensure the identification of software, support components, libraries, environments, and other assets are decommissioned.

As these risks span multiple organizations and divisions it is critical that consistent monitoring and management as well as handoffs between organizations and phases is in place to manage risks such as:

- **Incomplete or not readily understood SBOMs**: SBOMs that do not include complete details (version, build, etc.) of libraries and components from all vendors, as well as resource locations, licensing, and support information of third-party and open-source software required for systems, can introduce risk. Additionally, acquisition teams may not have the domain or subject matter expertise to review SBOM details.
- **Open-Source Software (OSS) Vulnerabilities**: In a recent study, 32% of organizations placed "implicit trust" in open-source repositories without delivery of security or integrity of software delivered; however, recent studies show that supply chain attacks on open-source software increased 650% in 2021 without a full understanding of OSS vulnerabilities and practices for updates/upgrades, organizations can introduce risk by relying on OSS.
- **Operational Support Gaps**: Organizations may not have operational processes supporting rapid update cycles, leading to outdated libraries, software patching, etc. Exacerbating this risk is that organizations increasingly rely on OSS which has a greater chance that some libraries used in the software are outdated (based upon volunteer build and code/security hygiene).

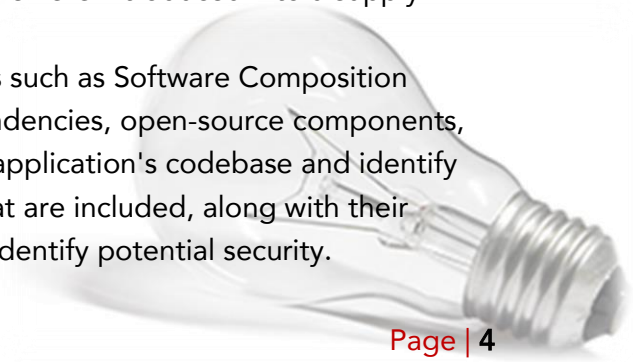


- **Lack of Strict Software Development Controls**: These controls should be implemented at both the customer and vendor organizations to ensure that new risks are not introduced at any level in the supply chain.
- **Software and System Complexity and Lack of Transparency**: Incomplete SBOMs can initiate a risk; however, the inability to document component and asset interdependencies as well as data flows and integration at a detail level add increased supply chain risk.

Risk Mitigation and Response

Securing the software supply chain requires the implementation of controls and security best practices throughout the lifecycle, mapping, monitoring, and managing risks, employing scenario-based response training, and maintenance of a comprehensive catalog of potential vulnerabilities and risks encompassing software, vendors, OSS, and components. Organizations should consider the following strategies:

- **Contract Negotiations and Acquisition Reviews**: Using contract terms to reinforce software supply chain security by including language requiring secure development practices, supply chain transparency (for third-party components, libraries, etc.), independent, third-party software reviews, and timely vendors notification of any security breaches or vulnerabilities as well as prompt patching. Strengthening acquisition reviews by ensuring subject and domain expertise, detailed requirements, complete SBOMs with all details as well as any strategies for secure maintenance for components and libraries.
- **Standards and Compliance**: Implementing guidelines and controls from standards such as NIST SP800-161 enables organization to achieve a baseline of effect controls for their software supply chain. Managing compliance and conducting reviews of supply chain controls in concert with the flow-down of NIST SP800-53 cybersecurity controls provides insight into potential software supply chain vulnerabilities.
- **Supply Chain Transparency and Traceability**: Requiring detailed mapping of the software component interdependencies, information flow, and other assets and components to include the supplier, third-party vendor, ownership/affiliations, and source provides a better picture of the software supply chain ecosystem and enables organizations to pinpoint weaknesses and vulnerabilities. Enabling organizations to make decisions based on the source, quality, security and integrity of components (to include underlying components) provides a greater understanding of the risks introduced into a supply chain and identify informed risk strategies.
- **Software Transparency and Traceability**: Using tools such as Software Composition Analysis (SCA) Tools to identify software interdependencies, open-source components, libraries used in the software. These tools scan the application's codebase and identify the open-source libraries and other components that are included, along with their version numbers and other relevant information to identify potential security.



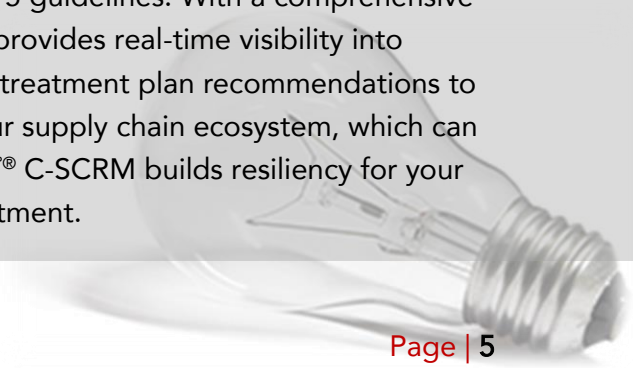
- **Heightened Risk Response and Follow-On**: Incident response plans should encompass multiple scenarios and target the organization's ability to identify, contain and eradicate attacks by rapidly identifying system interdependencies. Response drills should focus not just on disaster recovery or contingency operations, but the response readiness for containing software or component attacks. Additionally, in the event of a supply chain incident, the incident response team should provide details of the component and software vulnerability to the acquisition team. This approach enables software acquisition teams to better monitor the security posture of the software vendors, identify vulnerabilities, and provide alerts and reports.
- **Lifecycle Risk Management and Continuous Monitoring and Review**: Software supply chain risks are dynamic, becoming heightened at different phases. It is important to continuously monitor, document and share software supply chain risks throughout the lifecycle, enabling organizations to address new and emerging threats. Risks and vulnerability intelligence should be shared across multiple divisions and potentially external partners and other organizations.

Conclusion

Managing software supply chain risk is an ongoing process that requires organizations to take a comprehensive approach to risk management. Using tools ranging from contract language and requirements, comprehensive secure development policies and practices, and improved software and system traceability and transparency can assist organizations in building a catalog of potential vulnerabilities and mitigation approaches, understanding their risk exposure, preparing for potential risks or risk scenarios, and becoming more resilient.

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 their 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.