# Mitigating complex cyber threats in supply chain security requires a holistic approach



In response to an increasingly sophisticated landscape of cyber threats targeting supply chains, organisations are adopting comprehensive strategies to mitigate risks arising from upstream software, hardware, and vendor relationships. Adversaries are infiltrating trusted supply channels—whether through malicious updates in continuous integration/continuous deployment (CI/CD) pipelines, rogue dependencies concealed in open-source code, or tampered hardware components—to bypass traditional defences and compromise downstream targets.

Colin Fraser, Director at i-confidential, emphasised the growing significance of third-party security in this context, stating, "As more supply-chain attacks surface, third-party security is becoming essential for all businesses. Organizations must vet their suppliers, ensuring they practice good cyber security hygiene, while also working to limit exposure when attacks do occur on their partners." Despite rising national security concerns and governmental restrictions, Chinese military-linked companies remain deeply integrated within the US digital supply chain. These entities continue to supply critical digital infrastructure, potentially exposing US businesses and key industries to cybersecurity threats.

The expansive range of vulnerabilities requires Chief Information Security Officers (CISOs) to broaden their security scope beyond their internal boundaries. A major shift is underway from conducting one-time vendor assessments to implementing continuous monitoring of third-party risks. This real-time surveillance helps organisations identify supplier vulnerabilities, exposures, and atypical behaviour dynamically, enhancing defensive readiness.

Another notable evolution is the progression of Software Bill of Materials (SBOMs) from mere compliance documents to crucial operational tools. SBOMs now allow security teams to quickly pinpoint exposure when new zero-day vulnerabilities emerge. This development aligns with regulatory initiatives such as the US Executive Order on Improving the Nation’s Cybersecurity and the National Institute of Standards and Technology’s Secure Software Development Framework (SSDF), which advocate for transparency and mandate the adoption of SBOMs across various sectors.

Similarly, the European Union has introduced regulations like the Digital Operational Resilience Act (DORA) and the Network and Information Systems Directive (NIS2), aimed at reinforcing supply chain security and holding businesses accountable for their cybersecurity practices.

Artificial intelligence (AI) is playing dual roles in this evolving arena—both as a threat and as a defensive asset. AI is increasingly utilised to scale threat detection, leveraging predictive capabilities to identify potential compromises before they materialise, especially in code and package repositories. Zero trust security principles extend beyond internal networks to encompass vendor systems, enforcing stringent identity verification, device posture assessments, and behaviour-based access controls throughout the extended enterprise.

However, adversaries are also exploiting generative AI technologies to craft highly convincing phishing and impersonation attacks. Such attacks specifically target procurement processes, vendor communications, and executive communications. A survey conducted by Logility among 500 global supply chain leaders found that 97% are already using some form of generative AI, yet only one-third employ tools tailored to supply chain functions. Additionally, 43% expressed concerns about data privacy in these AI applications, and 40% reported distrust in the AI-generated responses.

CISOs are simultaneously contending with a resurgence of hardware-level threats. Reports of tampered devices and compromised firmware have raised alarms, particularly in critical infrastructure and environments requiring high-security assurance.

Real-time supply chain visibility is becoming a critical requirement, facilitated by innovations such as Internet of Things (IoT) telemetry and blockchain-based traceability. These technologies provide defenders with enhanced visibility across vast, global supplier networks. For example, BMW has implemented blockchain technology to ensure the traceability of components and raw materials throughout its multi-stage international supply chains, reinforcing transparency and guarding against tampering.

Nate Warfield, Director of Threat Research and Intelligence at Eclypsium, highlighted the complexity of supply chain security: "Supply chain security is a relatively new concept that organizations may have put on the back burner due to the relentless barrage of vulnerabilities, zero-day exploit campaigns, ransomware, and the challenges of working in both a COVID and post-COVID world. Understanding the need for a supply chain strategy and prioritising it is the biggest challenge, and the problem is complex. It will require collaboration across executive, development, security, and legal teams, and the strategy will vary based on the organization and its business model."

Combating supply chain attacks necessitates more than technical controls. It demands a strategic, systemic transformation whereby CISOs extend visibility, validate trust on a continuous basis, and strengthen every layer—from code to hardware, and from vendor to endpoint. This holistic approach aims to harden defences against an evolving and expanding threat landscape in supply chain cybersecurity.

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://www.reuters.com/world/us/complaints-about-ransomware-attacks-us-infrastructure-rise-9-fbi-says-2025-04-23/> - This article discusses the rise in ransomware attacks on U.S. critical infrastructure, highlighting the increasing sophistication of cyber threats targeting supply chains.
2. <https://www.ft.com/content/a430819f-7a8e-4d5d-b21d-bd32bf1f5fba> - This piece covers the U.S. government's efforts to enhance cybersecurity at ports in response to potential threats from Chinese hackers, emphasizing the need for robust third-party security measures.
3. <https://www.esentire.com/how-we-do-it/use-cases/third-party-cyber-risk> - eSentire's page outlines strategies for managing third-party cyber risks, including continuous monitoring and due diligence, aligning with the article's emphasis on proactive third-party risk management.
4. <https://www.rsaconference.com/library/blog/third-party-vendors-the-weak-link-in-supply-chain-security> - This blog post discusses the vulnerabilities introduced by third-party vendors in supply chain security, supporting the article's point about the need for continuous monitoring of third-party risks.
5. <https://www.techtarget.com/searchsecurity/tip/How-to-manage-third-party-risk-in-the-supply-chain> - This guide provides insights into managing third-party risks, including performing risk assessments and verifying partners' controls, which supports the article's discussion on the importance of third-party security.
6. <https://www.pmmi.org/blog/third-party-risk-how-do-you-secure-your-supply-chain> - This blog emphasizes the importance of auditing vendors and implementing contractual safeguards to secure the supply chain, aligning with the article's focus on strengthening defenses against supply chain cyber threats.
7. <https://news.google.com/rss/articles/CBMifEFVX3lxTE9xS0pOZ1ZtbUlSMHZzb0huZFBmbVhRUlktUmRmZVNQWmVtNzZqS3pKMW5JSzAtRm5CZ0dyb0hweEFVdloxWXNTS3ZfZ2x1VlZTTFhCaEJCNXA3MnBoamtQRnB0eTc5b2swZVNJS2YyRzk4UnZRTm1JZUQ0ZFo?oc=5&hl=en-US&gl=US&ceid=US:en> - Please view link - unable to able to access data