Picture credit: AdobeStock

THE WEAKEST LINK

Sam Peters *shows how businesses can fortify defences amid spiralling supply chain attacks*

The commercial world as we know it revolves around supply chains. In today's interconnected and highly digitised trading environment, supply chains represent a complex web of interlinked relationships which enable the movement of goods and services between providers and their customers. These webs are becoming increasingly more complex and critical. The pandemic, for example, brought to light just how reliant economic stability and business growth are on the uninterrupted flow of products, and just how vulnerable economies can be to snags in the supply chain, no matter how far away they might be.

Supply chains are also more reliant on IT systems than ever before. As businesses continue to digitally transform their operations, their use of various software-based solutions will grow in kind. From cloud-based inventory management and automated ordering processes to real-time tracking and analytics, the modern supply chain is deeply intertwined with complex digital ecosystems, creating new efficiencies, but also expanding the potential attack surface for cyber criminals. This presents a major challenge for enterprises and the cyber security profession responsible for protecting them.

Cyber criminals understand the critical nature of supply chains and are exploiting the interdependencies between companies and their digital ecosystems, targeting the weakest links in an organisation's extended network. By infiltrating or compromising less secure elements, attackers can potentially gain access to multiple organisations, making these threats challenging to defend against.

Several high-profile incidents have thrust supply chain vulnerabilities into the spotlight. The Okta breach in early 2022, for instance, saw hackers compromising a third-party contractor's systems to access the identity and access management firm's customer support data. Similarly, the MOVEit breach in 2023 exploited a zero-day vulnerability in widely used file transfer software, leading to unauthorised access and data theft from numerous organisations globally. These incidents point us toward a conclusion that can no longer be ignored – today, an organisation's security is only as strong as the weakest link in its network of suppliers and partners.

To gauge the true extent of the supply chain attack threat, ISMS.online recently conducted a comprehensive survey of 1,526 security professionals across the UK, USA and Australia. The resulting 'State of Information Security' report paints a concerning picture, particularly for UK businesses. During the past year, almost eight in 10 (79 percent) UK businesses experienced security incidents stemming from their supply chain or third-party vendors, marking a dramatic 22 percent increase compared with the previous year's finding and highlighting the rapidly escalating nature of this threat.

In addition, some 41 percent of UK respondents told us that partner data was the most compromised type of information – this not only points towards the vulnerability of shared data within supply chains but also underscores the persistent risks posed by suppliers and third-party vendors.

During the past year 79 percent of UK businesses have experienced security incidents stemming from their supply chain or third-party vendors

BUSINESSES NEED TO RECOGNISE EFFECTIVE DEFENCE REQUIRES A COLLABORATIVE EFFORT

These figures do not simply reflect the fact that supply chains are more reliant on IT systems. There are several other factors at play. For instance, the interconnected nature of supply chains means that a single weak link can potentially compromise numerous organisations. Attackers are increasingly targeting smaller, less secure vendors or suppliers as a means of gaining access to larger, more protected companies. This 'island-hopping' technique allows cyber criminals to exploit the trust relationships between businesses in the supply chain.

Furthermore, the global nature of many supply chains adds another layer of complexity to security efforts. Different countries operate varying cyber security standards and regulations, making it challenging to maintain consistent security practices across the entire supply chain. This disparity can create vulnerabilities that savvy attackers are quick to exploit. And attackers are indeed becoming savvier.

Today's cyber criminals are employing advanced techniques such as AI-powered attacks and exploiting zero-day vulnerabilities to breach supply chain defences, helping them to extract greater rewards. ISMS.online's research found that 70 percent of UK businesses have received fines for data breaches in excess of £100,000 in the last 12 months, with the average fine amount increasing by 3.5 percent in just one year to £258,000.

The case for reviewing, reassessing and strengthening cyber security strategies is therefore clear. Supply chain resilience must be embedded as a key focus, and several important areas can be prioritised by businesses to ensure this happens. Here, we outline eight steps that all organisations can take.

MORE ROBUST VETTING PRACTICES

The first line of defence against supply chain attacks lies in rigorous security vetting processes for partners and suppliers. This involves conducting thorough due diligence, assessing the security posture and cyber security measures of potential partners and reviewing their history of security incidents and responses.

Companies should also evaluate compliance with relevant regulations and standards, such as ISO 27001, for information security management. Crucially, this vetting process should not be limited to just a one-time event, but an ongoing effort with regular reassessments and continuous monitoring of partners' security practices.

ENHANCE INTERNAL CYBER SECURITY

While it's crucial to demand robust security measures from partners, businesses must lead by example. Bolstering internal cyber security measures and extending them to the supply chain can significantly reduce risks.

Key strategies include regular auditing of internal systems and processes, comprehensive employee training in cyber threat recognition and response, and adoption of advanced cyber security technologies like multi-factor authentication and encryption. Companies should also develop and regularly test incident response plans specific to supply chain breaches and consider implementing zero-trust architecture principles.

DEVELOP ROBUST PARTNERSHIP AGREEMENTS

Clear and stringent partnership agreements are essential in establishing cyber security expectations and responsibilities across the supply chain. These agreements should define specific security requirements and standards, mandate regular security status reports and audits, and establish clear access controls to safeguard sensitive information. They should also outline incident reporting and response procedures, and include termination or penalties provisions in case of security breaches.

ALIGN WITH KEY STANDARDS AND FRAMEWORKS

Adopting and aligning with recognised cyber security standards and frameworks can provide a structured approach to managing supply chain risks. For UK businesses, some of the most relevant standards include Cyber Essentials, a UK government-backed scheme that provides clear guidance on basic security controls to protect against common cyber threats; ISO 27001, an international standard for information security management systems that offers a systematic approach to managing sensitive company information; and the National Cyber Security Centre's (NCSC) Supply Chain Security Guidance, which provides comprehensive recommendations for managing supply chain risks, implementing robust cyber security measures and ensuring continuous monitoring and improvement.

LEVERAGE ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

Despite the challenges posed by AI-driven threats, there's a strong belief in the potential of AI and machine learning (ML) to enhance data security. Our research found that 72 percent of UK businesses agree that AI and ML will play a crucial role in improving their data security programs.

These technologies can be leveraged to enhance threat detection and response capabilities, automate security processes and analysis, identify anomalies and potential vulnerabilities in the supply chain, and improve the accuracy and speed of security decision-making.

INVEST IN EMPLOYEE EDUCATION

The human element remains a critical factor in supply chain security. Our research revealed that 47 percent of UK businesses are placing greater emphasis on employee education and awareness initiatives. Comprehensive training programs should cover recognition of phishing attempts and social engineering tactics, best practices for data handling and protection, awareness of emerging threats, and procedures for reporting suspicious activities or potential breaches.

> COMPANIES NEED TO TEST INCIDENT RESPONSE PLANS SPECIFIC TO SUPPLY CHAIN BREACHES

REGULARLY ASSESS AND UPDATE SECURITY

The threat landscape is constantly evolving and so too must an organisation's security measures and protocols. Regular assessments and updates should include periodic security audits of both internal systems and those of key suppliers, vulnerability assessments and penetration testing, review and update of security policies and procedures, and evaluation of new security technologies and their potential implementation.

FOSTER A CULTURE OF SECURITY

It is crucial to create a security-conscious culture throughout the organisation and extend it to the supply chain and various partners. There are many actions which can help to build this culture. They include making security a board-level priority, encouraging open communication about security concerns and recognising and rewarding security-conscious behaviour. Ultimately, organisations need to integrate security considerations into all business processes and decisions.

As supply chain attacks continue to rise in frequency and sophistication, UK businesses must recognise that effective defence requires a collaborative effort across entire value chains.

Indeed, no single organisation can secure the entire supply chain alone – rather, it requires ongoing cooperation, information sharing and mutual support among all stakeholders, no matter how physically disparate they may be.

What's more, as our research indicates, nearly two-fifths (38 percent) of UK businesses are set to increase their financial allocations for securing supply chain and third-party vendor connections by up to 25 percent in the coming year. This increased investment reflects a growing awareness of the critical importance of supply chain security.

While the task of securing the supply chain may seem daunting, the burden does not have to be overwhelming. With the right approach, support and tools, businesses can implement best practices and significantly enhance their resilience against supply chain attacks.

As we navigate this complex threat landscape, one thing is clear: in today's interconnected business world, supply chain security is not just an IT issue – it's a fundamental business imperative. By taking proactive steps to fortify defences and fostering a culture of security that extends throughout the supply chain, UK businesses can not only protect themselves against cyber threats, but also gain a competitive edge in an increasingly digital marketplace.

The journey towards robust supply chain security may be challenging, but with vigilance, collaboration and a commitment to best practices, UK enterprises can build up the resilience needed to thrive in the face of evolving cyber threats ●

Sam Peters is Chief Product Officer at ISMS.online.

> **With the right approach, support and tools, businesses can implement best practices and significantly enhance their resilience against supply chain attacks**

Picture credit: AdobeStock