K&S INSURANCE
A BALDWIN RISK PARTNER

NOT JUST A PASSING TREND – SUPPLY CHAIN CYBERSECURITY RISKS IN 2023

Last year, supply chain attacks became one of the top cybersecurity concerns for organizations. Unfortunately, that prediction has come to fruition, with cybersecurity attacks on supply chains only becoming more sophisticated and pervasive in 2023.

Cyberattacks in the supply chain specifically target the intricate web of relationships between organizations and their suppliers, vendors, and third-party service providers. They take advantage of vulnerabilities that arise due to the interconnected nature of digital supply chains, which often span across various organizations, systems, and regions. For hackers, this type of attack is appealing because through one breach, they can cast a wider net that impacts a greater number of users.

Compromising a trusted component or software within the supply chain enables attackers to infiltrate their target organization. Because many organizations trust their vendors, they might not think to check for vulnerabilities in the software or services they're purchasing. With an increasing dependence on global, interconnected digital supply chains, it's essential for businesses to comprehend the risks and consequences of a supply chain attack in order to maintain security and resilience.

BY THE NUMBERS

Impact of Supply Chain Cybersecurity Risk

In a recent study by ReversingLabs, **98%** of respondents indicated that **software supply chain issues pose a significant business risk.**

This same study found that nearly **90%** of surveyed technology professionals **detected significant risks** in their software supply chain in the last year, but only **60% felt their software supply chain defenses were up to task.**

Another study by cybersecurity provider, Sonatype, found that between 2019 and 2022, **software supply chain attacks increased 742%.**

Gartner predicts that by 2025, **45% of organizations globally will have experienced attacks** on their software supply chains.

SUPPLY CHAIN SECURITY THREATS IN 2023

1. **SOFTWARE VULNERABILITIES** – Attackers have an opportunity to inject malicious code into the software of firmware used by a vendor in the supply chain.

2. **INABILITY TO DETECT SOFTWARE TAMPERING** – Identifying software vulnerabilities requires the right tools, time, and expertise, which are resources that many organizations may not have.

3. **THREATS HIDDEN IN OPEN-SOURCE REPOSITORIES** – A growing reliance on open-source software is a significant cyber risk, since bad actors examine the code and its components to find the most effective ways to exploit them. If the open-source software code library has a vulnerability, then every company that downloads and uses that code may be compromised.

4. **VULNERABILITIES IN THE CLOUD** – More organizations are using the cloud, which is a treasure trove of data that hackers want to get their hands on. Cloud providers are an attractive target for bad actors, which is why organizations that depend on these services need to do their due diligence to contain this third-party risk.

5. **ZERO-DAY VULNERABILITIES** – A zero-day vulnerability is when an issue has been discovered but no fix is available for it. Between this time and the vendor's release of a patch, cybercriminals have an opportunity to exploit the vulnerability. And in some cases, the vendor might not identify an exploitable issue until it's too late.

6. **CREDENTIAL THEFT** – Through the use of attacks, like phishing, social engineering, or system vulnerability exploitation, attackers can steal login credentials of suppliers to gain access to your systems.

7. **DATA THEFT** – Malicious actors might breach your suppliers' systems and gain access to sensitive data related your organization's operations or its customers.

8. **PHYSICAL SUPPLY CHAIN THREATS** – Digital supply chain attacks may pose threats to the physical supply chain, like with the Colonial Pipeline incident which affected the supply of oil in the Southeast.

9. **THE AGE OF AI** – Artificial intelligence (AI) has brought tremendous changes in cybersecurity, with bad actors using it to advance their interests. For example, with the popularity of tools, such as ChatGPT, they can easily draft more realistic phishing emails.

10. **CYBER INSURANCE EXCLUSIONS** – With supply chain attacks posing a growing risk to organizations and leading to significant losses, cyber insurers are paying attention, with some carriers now beginning to ask organizations questions about third-party cybersecurity measures. Organizations that purchase cyber insurance need to monitor exclusionary language or sublimits carriers place on supply chain cyberattacks.

BOTTOM LINE

It's clear that supply chain cyberattacks pose a significant risk to organizations of all sizes and industries. When organizations understand the nature of these threats and implement adequate security measures, they can better protect themselves against the harmful consequences of a successful supply chain attack. As cyber threats continue to become more sophisticated, a proactive and comprehensive approach to managing supply chain cyber risk will play a key role in maintaining resiliency amongst our interconnected digital ecosystem.

In addition to internal assessments, organizations need to vet the cybersecurity posture of their supply chain partners on an ongoing basis. **If you need recommendations or access to resources to better understand and contain this risk, contact us today. Our team of cyber experts can help contextualize cyber supply chain risk within your overarching risk mitigation strategy and business goals.**

Contact Us

K&S INSURANCE
A BALDWIN RISK PARTNER