


Cyberattacks on the Rise & Threatening the Links in Your Supply Chain



Over the years, supply chain networks have been fiercely driven by technology. And as a response to the coronavirus pandemic, organizations of all sizes and across industries accelerated their digital transformation to adapt to the operational needs of remote workforces and customer expectations in a physically distanced world.

This fast-growing technology transformation brought a significantly increased occurrence of cyberattacks, with supply chain networks being particularly vulnerable to attacks.

Globally, supply chains are under immense and unprecedented amounts of pressure from many different directions, which is why they are a prime target for malicious actors. Additionally, the technology that makes supply chains faster and more efficient also poses a threat to their cybersecurity. Because technology and supply chain are so intertwined, discussions about supply chain recovery need to include cybersecurity and risk management with a focus on mitigating supply chain attacks.



A LOOK INTO SUPPLY CHAIN ATTACKS

Supply chain attacks are a type of cyberattack that target trusted third-party vendors with access to systems and data that offer vital services or software to the supply chain. This has dramatically changed the attack surface for companies because, more than ever before, suppliers and service providers are touching sensitive data. Supply chain attacks have historically been referred to as attacks against trusted relationships.

However, software supply chain attacks are becoming a greater concern. A software supply chain attack occurs when an attacker injects malicious code into an application to infect all app users. **Software supply chains are very vulnerable because most modern software involves many off-the-shelf-components, such as open-source code, code from software vendors, or third-party APIs.** According to a 2021 study by GitHub, the average software project has 203 dependencies. If an application includes any compromised dependencies, every business that downloads the app then becomes compromised.

THE STATS

84%

In 2021, CrowdStrike surveyed 2,220 IT decision-makers, and 84% responded that software supply chain attacks could become one of the **biggest threats to their organizations within the next three years.**

66%

An estimated 66% of supply chain breaches are a **result of supplier or third-party vulnerabilities.**

36%

The 2021 CrowdStrike Global Security Attitude survey also found that only 36% of respondents vetted all new and existing suppliers for security purposes in the previous 12 months. Additionally, **45% of respondents' organizations experienced at least one software supply chain attack in 2020**, compared to 32% in 2018.

60%

Over 60% of **data breaches are caused by simple oversights**, like failing to patch software.

Supply chain attacks are becoming more common as a response to companies hardening their digital environments. As we know, there are many different points along a supply chain, and there's a good chance that there's a vulnerability somewhere along the way. When these vulnerabilities are exploited, all other parties in the chain are in harm's way. With enterprises becoming more reliant on outside providers, this problem is only likely to get worse. And no industry is safe. The oil, government, manufacturing, and financial institutions have all shown to be at risk.

Take for example the SolarWinds supply chain attack in December of 2020. This complex attack injected malicious code into a software's build cycle and infected about 18,000 customers, including government agencies and major firms protected by leading cybersecurity tools and services. The Colonial Pipeline hacking attack also made headlines by interrupting fuel supply to the southeastern United States for a week. This attack set off a chain reaction of panic buying, price hikes, and gas shortages, proving just how disruptive and tangible a supply chain cyberattack can be.

With the supply chain already in such a precarious position due to underlying economic changes and labor shortages, companies and their suppliers need to find ways to better manage the risk of supply chain attacks. **Organizations should vet the cybersecurity posture of their supply chain partners on an ongoing basis in addition to performing internal cybersecurity assessments.** Businesses suffer when they're unable to meet customer demands due to supply chain interruptions and might not be able to survive the fallout.

[Connect with your broker](#) to discuss your cybersecurity risk strategy to help protect your business and better position your business to underwriters in a hardened market.



This material has been prepared for informational purposes only. BRP Group, Inc. and its affiliates, do not provide tax, legal or accounting advice. Please consult with your own tax, legal or accounting professionals before engaging in any transaction.