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

Over the years, supply chain networks have been fiercely driven by technology and most supply chains are now fully digitally enabled. Additionally, as a response to the coronavirus pandemic, organizations of all sizes and across all 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 such 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. The technology that makes supply chains faster and more efficient also poses a threat to their cybersecurity. However, despite this, a vast majority of organizations haven’t evaluated how such interruptions could negatively affect them or their supply chain and how to mitigate that risk. 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.

AHT INSURANCE
A BALDWIN RISK PARTNER

A LOOK INTO SUPPLY CHAIN ATTACKS

Historically, supply chain attacks have been cyberattacks 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 all companies in the supply chain because, more than ever before, suppliers and service providers are more digitized.

In recent years, the networked interconnectivity of production equipment to critical systems such as purchasing, sales, accounting, and other internal networks, has enabled these attacks to seize hold of various production lines in both food and non-food industries. This leaves many organizations down for weeks at a time and their clients scrambling to find alternatives for their own customer demands. Even if production equipment is on an internal network system, if it is connected to another system that speaks to the outside world (even through email), attackers have used those ports to gain access to the production system itself to hold for ransom. These systems sometimes even run on older and unsupported software, such as Windows 98, or are manually tweaked through internal IT departments for their unique functions that can lead to further vulnerability.

Even organizations that feel they have a strong cybersecurity posture are still vulnerable to the most unpredictable of sources—employees. Business email compromise and successful phishing scams that result in the deployment of ransomware or malware are among some of the most common causes of loss for organizations. With the simple click of an email, one employee can cause an entire organization's production system to be seized.

Many Chief Information Security Officers are also concerned about the surge of software supply chain attacks in recent months. A software supply chain system attack is when an attacker injects malicious code into an application to infect all app users. They can do this because most modern software involves many off-the-shelf-components, such as open-source code, code from software vendors, or third-party APIs, and these separate sources of code or applications are what create vulnerability within various software applications. 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 key here is knowing that the threat to an organization is very real and the risk to their operations goes beyond their own organization to everyone in the supply chain itself.

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.**

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.

66%

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

60%

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

Attacks on the supply chain 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 at least one vulnerability amongst the various organizations in your supply chain. 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. And let's not forget the meatpacking giant, JBS, whose production shutdown rattled the beef market.

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. One way is for organizations to collaborate internally with their operations, IT, sales, legal, procurement, and finance departments to better understand the financial impact to the company should a cyber event occur, both internally and externally. This collaborative approach helps all areas of an organization understand the financial return on investment for upgrading their cyber security posture and identifying potential weaknesses within their key supplier relationships. 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.

Content written in collaboration with Brian King, Advisor with AHT Insurance.
brian.king@ahtins.com | 206.336.2963

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.