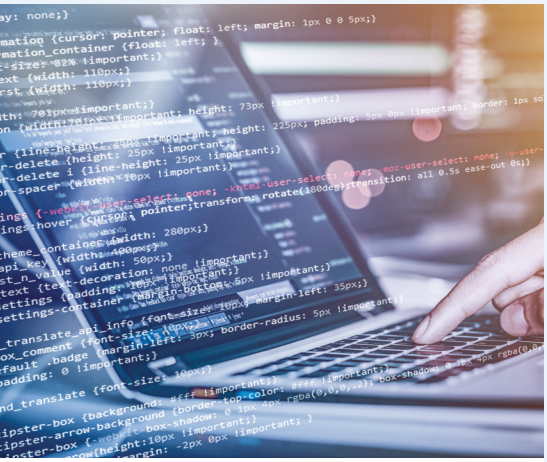
Exploiting Weaknesses in the Supply Chain: The Gateway to Cyber Attacks

An examination of exploitable vulnerabilities in the supply chain, along with risk mitigation best practices.

Gallagher

Insurance | Risk Management | Consulting



Contents

Section 1: Risk landscape 4

Risk #1: Supply chain software and technology infrastructure – Credentials theft, software and firmware tampering 4

Risk #2: Third-party vendor platforms – Integration vulnerabilities with open source, API and third-party library applications 4

Risk #3: The physical supply chain 6

Risk #4: Risk management and supply chains 6

Risk #5: Security of sensitive data – Criminal data breaches 6

Section 2: Risk analysis 7

Risk #1: The system is only as strong as the weakest link 7

Risk #2: Protecting the supply chain is a shared responsibility 7

Risk #3: Proactive approach to yield better outcomes 7

Risk #4: Traditional security tools and practices fall short 7

Section 3: Leverage the future 8

Headlines:

The increasing emphasis of organizations on fortifying internal cyber infrastructure has led to a surge in threat actors directing their attention towards the vulnerabilities existing within the broader supply chain components.

- 2021 research undertaken by the European Union Agency for Cybersecurity found that in 66% of supply chain attacks, suppliers either did not know or failed to report how their systems were breached.[1]
- Ransomware, one of the fastest-growing cybercrime vectors, is predicted to affect a business, consumer, or device every two seconds by 2031 and cost its victims nearly USD$265 billion annually.[2]
- Nearly half of all recent attacks employed "island hopping," wherein attackers exploit cyber security vulnerabilities present in the systems of vendors or smaller partners to infiltrate the ultimate target.
- In 2022, data breaches cost businesses an average of $4.35 million, up from $4.24 million in 2021.[3]
- The key to resisting cyber attacks is a proactive approach to driving up the adoption of cyber security best practices through all levels of the supply chain rather than spending resources purely on damage limitation.

Section 1: Risk landscape

Context

As digitalization continues to shape the 21st century business landscape, organizations are becoming increasingly reliant on complex supply chains and shared technology platforms. While this integration enables data-led decision-making and operating efficiency, it also presents a set of attached risks, most notably cyberattacks. Threat actors recognize the potential for exploiting vulnerabilities in shared technology platforms to gain unauthorized access, disrupt operations, steal confidential information, or inject malicious code.

Risk #1: Supply chain software and technology infrastructure – Credentials theft, software and firmware tampering

Supply chain software and technology infrastructure play a pivotal role in facilitating seamless vendor-customer engagement. Order processing software, inventory management software, shipping organization software, warehouse management software, and sourcing and procurement software are some of the major classifications of software employed for supply chain operations.

Software platform integration between supply chain participants often contains commercially sensitive information such as customer data, financial information, and intellectual property. Cyber attacks targeting points of vulnerability within software applications, operating systems, or network infrastructure enable a threat actor to gain access to confidential information.

Credential theft has emerged as a prevalent threat in recent times. Exploiters employ various strategies, such as **phishing, social engineering,** and **malware,** to steal user credentials and obtain unauthorized access to networks and databases. Compromised credentials enable attackers to masquerade as legitimate owners, bypass security measures, and navigate the different tiers of the supply chain.

The SolarWinds incident of 2020, in which SolarWinds' Orion software was compromised, remains one of the most significant cybersecurity breaches in recent history. The shareholder lawsuit that followed alleged that the company operated with weak security practices, including passwords such as *solarwinds123.*

Attackers can surreptitiously infiltrate supply chains by tampering with the software and firmware. An example is the method known as "**typosquatting**," where they are able to trick developers into downloading a malicious package by creating lookalikes of legitimate software packages. The 2021 IconBurst attack saw the icon-package typosquatted module downloaded over 17,000 times before it was removed from npm, a public collection of open-source code for the JavaScript community.

Risk #2: Third-party vendor platforms – Integration vulnerabilities with open source, API and third-party library applications

Global organizations, privately and publicly owned, have embraced the adoption of always-functioning, remote cloud-based systems and software that operate using open source and third-party code. Although open source ranks highly in parameters such as cost-effectiveness and flexibility, it often relies on community-driven development, where vulnerabilities can potentially go unnoticed for extended time periods. Operational risks, particularly supplier/third-party risks, are among the most concerning threats to an organization's revenue, according to 52% of Canadian firms.[4]

"When you look at a modern company, 80% of their infrastructure is outsourced, especially in the mid-corporate space. They won't have a whole network that they own and manage. One of the areas of interest for cyber insurance carriers now is the potential for third-party security failures or third-party outages.

In terms of where a company is most likely to have an incident, statistically, it's always about a person sending the wrong email. But from a network reliance perspective, they have more of their network managed by somebody else than they do themselves.

When you think about a supply chain attack, it's actually a really big risk for an insurer because there is very little to contain it. Unlike a natural catastrophe, which can be devastating and hugely costly but is still fairly localized to that particular part of the world, an attack on a major vendor is a huge issue for the capacity providers we work with."

Johnty Mongan, Head of Cyber Risk Management, Cyber Risk Management

Trust in **open-source software** implanted with malicious software can hurt organizational security. Open-source repositories such as **npm** and **PyPi** have seen a rise in malicious packages, with attacks on them having increased by 289% in the last four years.[5] Once malicious code or a backdoor is introduced into shared components, the exploiter's activity could range from spying to shutting down critical infrastructure.

Supply chain systems often require libraries to streamline development and enhance functionality. These third-party libraries are often the target of cyberattacks, which first came to light in 2014 with Heartbleed, a vulnerability in OpenSSL that eventually affected 17% of all SSL servers.[6]

Inadequately secured APIs can also serve as entry points for threat actors, leading to system downtime, data breaches, or the unauthorized disclosure of sensitive information. This could be executed in the form of injections, **XSS, MitM attacks, credential stuffing, or DDoS attacks**, leading experts to estimate API abuses to move from an infrequent to the most frequent **attack vector.**[7]

Definition of terminology: Types of API attacks

- **Injection** occurs when exploiters are able to add malicious code into a program where typical user input, such as a username or password, is expected.
- **Cross-site scripting (XSS)** is a type of injection of malicious executable scripts into the code of a webpage or application.
- **Man-in-the-middle** attacks occur when the exploiter intercepts traffic between two systems and relays messages by impersonating each other.
- **Credential stuffing** involves exploiters obtaining user credentials from one service and attempting to login to another unrelated service.
- **Distributed denial-of-service (DDoS)** makes a network system unavailable to users, typically flooding a server with internet traffic.

Risk #3: The physical supply chain

Canada is a trading nation. The country's annual merchandise exports increased by 22.5% to $779.2 billion in 2022, while the value of annual imports increased by 19.9% to $757.4 billion.[8] Disruptions in the supply chain can have profound implications for the country's economy.

The COVID-19 pandemic and the Russia-Ukraine conflict are the two major recent factors to severely compromise the global supply chain, with the conflict expected to cause a 60% drop in trade and a 50% increase in wheat prices.[9]

Another noteworthy instance of a hindrance to the physical supply chain is the 2021 **ransomware attack** on Colonial Pipeline Company,[10] which forced the largest refined oil pipeline in the US to shut down for a few days.

Cyber attacks disrupt various stages of the physical supply chain, including manufacturing, logistics, and distribution. The attackers can infiltrate critical systems, compromise the safety of goods, and potentially endanger the health and level of trust of the consumer.

Risk #4: Risk management and supply chains

Lessons from the past have ensured organizations now see risk management as a crucial strategic initiative to facilitate a smooth supply chain. It involves identifying potential risks and planning steps for risk mitigation, including avoidance, transference, resistance, and recovery, and response in the worst-case scenario.

Businesses need to adapt to manage both **known risks** (suppliers going bankrupt) and **unknown risks** (natural disasters). Companies formulate the different aspects of risk, such as impact, chance of risk materialization, and preparedness to face the risk, while building an integrated risk management framework.

PPRR (Prevention, Preparedness, Response, and Recovery) risk management template is a globally recognized risk management strategy followed by organizations. PPRR can play a pivotal role in planning business continuity.

Organizations can strengthen their risk management capabilities **with robust cybersecurity protocols, regular vulnerability assessments,** and **continuous monitoring of components** that may be potential targets for threat actors.

Risk #5: Security of sensitive data – Criminal data breaches

Exfiltration and misuse of sensitive and confidential information have always been at the heart of cyber attacks. In 2021, Quanta Computer, a Taiwanese technology manufacturer and Apple partner, was attacked by the REvil ransomware group. This left Quanta's systems locked and encrypted with sensitive data, including "large quantities of confidential drawings and gigabytes of personal data with several major brands" accessed and extracted.[11]

More recently, 3CX, whose 3CX Phone System is used by over 600,000 companies worldwide and over 12 million users daily,[12] was targeted by a North Korean hacking group. According to the information security company and their investigative partner, Mandiant, the identified software supply chain compromise is the first they were aware of, which led to an additional software supply chain compromise.

Cyber attacks pose a significant threat to sensitive data, necessitating stringent measures. Steps such as conducting thorough background checks on supply chain partners, implementing updated encryption protocols, and enforcing strict access controls can improve the safeguards for sensitive information.

Section 2: Risk analysis

Risk #1: The system is only as strong as the weakest link

From dialogue with suppliers to customer support, each link in the supply chain represents a potential point of weakness that could be targeted by cyber attackers.

These attackers scan for the soft underbelly of the network. More often than not, they end up targeting vulnerable suppliers, who may lack necessary safeguards such as updated software to insert malicious code into the supply chain. Labeled "Island Hopping," the attack facilitates infiltrating the ultimate target's network by finding vulnerabilities in their smaller partners. The method was utilized in nearly 50% of the attacks in previous years.[13]

Ensuring secure coding practices, implementing encryption protocols, and developing transparency of all processes within the supply chain can go a long way toward recognizing vulnerabilities and creating safeguarding strategies.

Risk #2: Protecting the supply chain is a shared responsibility

In 2021, a Romanian threat researcher, Alex Birsan, was able to breach Tesla, Apple, Uber, and Microsoft data by taking advantage of dependencies that applications use to provide an integrated service to end-users. Birsan was able to transmit counterfeit but harmless data packets to prominent users by exploiting these dependencies.

This incident highlights why companies must be aware of the cloud service platforms and security tools employed by their partners, which may become gateways into the supply chain.

However, no single organization or entity can solely take over the duty of safeguarding the entire supply chain. In order to effectively traverse the supply chain life cycle, the involved parties must create an ecosystem of collaboration, cooperation, and collective efforts aimed at strengthening its integrity.

"Any type of systemic issue is of concern for insurers. Back in the early days of cyber insurance, one of the carriers we work with reported that when a cloud, which was specialized in healthcare, was hacked, they had something like 80 different clients with information hosted in that cloud. But they weren't underwriting to that. They weren't asking, 'Which cloud service do you use?' for instance. So they're paying a lot more attention to software and programs where they could end up with a large number of claims out of one incident."

Dan Lewis, VP National Management Liability Practice, CA National Specialties

Risk #3: Proactive approach to yield better outcomes

Adopting a proactive approach rather than a reactive one is crucial to effectively mitigating risks and potential incidents. A reactive approach could lead to financial and reputational damage and disruptions in business operations.

One proactive measure would be implementing an endpoint detection and response (EDR) system, which can help stop various types of supply chain attacks as the endpoint itself is protected against threats.

Heightened vigilance can be attained by encouraging supplier education, running security tests, and regularly reviewing and updating policies. By promoting a culture of security awareness at all levels, organizations can create an attentive workforce that actively contributes to ensuring the integrity of the supply chain.

Risk #4: Traditional security tools and practices fall short

Traditional security tools often focus on protecting individual endpoints or network parameters but neglect the broader perspective of the supply chain. This causes a lack of visibility and control over all components.

With security measures primarily focusing on safeguarding internal infrastructure, the same level of control and protection will not apply to external systems such as vendor and third-party applications.

The cyber threat landscape is constantly evolving, with sophisticated tactics such as zero-day attacks or advanced persistent threats (APTs) such as GhostNet.[14]

Section 3: Leverage the future

It is important to note that as new tools enter the market, exploiters begin experimenting with them to pinpoint vulnerabilities. As such, the priority should be to always stay one step ahead of them.

The future of supply chain security will depend on our ability to leverage emerging technologies such as artificial intelligence (AI) and machine learning (ML). Employing these technologies, predictive models can be created to identify anomalies or patterns indicative of potential breaches.

The **human factor** has played a role in cybersecurity breaches over the years, exposing a lack of awareness and preparedness. Of all the proactive steps, this should be the first issue to be rectified. Companies and employees have to realize there are only two ways vigilance can be culturally ingrained: **either you learn or you live and learn**.

Citations

[1] Understanding the increase in Supply Chain Security Attacks
[2] Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031
[3] Cost of a Data Breach Report 2022
[4] 2022 Global Risk Survey
[5] The state of software supply chain security report: Top takeaways for development and SOC teams
[6] Half a million widely trusted websites vulnerable to Heartbleed bug
[7] API Security: What You Need to Do to Protect Your APIs
[8] Canadian international merchandise trade: Annual review 2022
[9] The impact of Russia-Ukraine conflict on global food security
[10] The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years
[11] REvil gang tries to extort Apple, threatens to sell stolen blueprints
[12] Security Incident Update Saturday 1 April 2023
[13] Carbon Black Quarterly Incident Response Threat Report
[14] GhostNet

AJG.com **The Gallagher Way.** Since 1927.

Gallagher