SUPPLY CHAIN MANAGEMENT REVIEW

Cybersecurity as a major supply chain risk domain

The digitization and interconnectedness of business is increasing the risk of cyberattacks, regardless of the level of security employed

Seongkyoon Jeong · August 5, 2024 ·

Editor's Note: *This is the first in a series on Cybersecurity in Supply Chains by SK Jeong, a University of Tennessee professor and digital supply chain researcher experienced in detecting vulnerabilities in software systems and economic impact of cyberattacks. He explores why cybersecurity matters to supply chain managers and what fundamental strategies managers should take. You can find the original post on the University of Tennessee Global Supply Chain Institute's blog, where supply chain professionals can find essential reading from leading researchers and scholars on the latest trends and topics relevant to global supply chain management.*

With the digitalization of business, cyberattacks have become a top risk. These attacks occur more frequently and cause significant losses in business value. Recognizing the severity of the risk they're exposed to, leading companies have enhanced their cybersecurity measures. However, building a so-called security fortress does not prevent cyberattacks entirely. Instead of directly attacking well-protected target companies, cyber-attackers will often exploit suppliers with weaker protections to gain access and harm their primary targets.

Related content

Leadership development for supply chain leaders

Five critical challenges facing supply chain planning talent and leadership development

11 core competencies critical for today's supply chain planners

Five organizational action areas for developing supply chain talent

A prominent example of a supply chain cyberattack is the 2020 SolarWinds incident. SolarWinds offers Orion software, an IT

infrastructure tool used to monitor, analyze, and manage corporate IT systems. State-sponsored hackers infiltrated the software, inserting malicious code into a scheduled update. Customers, including U.S. federal agencies, state and local governments, and major corporations, were compromised when they executed the update. This breach affected around 18,000 SolarWinds customers.

For over a decade, scholars like me have documented the rising pattern of cyberattacks channeled through the supply base. What we began observing in the early 2010s accelerated with the COVID-19 pandemic. As the world moved online, the rapid and necessary adoption of digital tools, active use of digital services, and improved digital connectivity with suppliers increased business productivity but also induced more cyberattacks through the supply chain.

Importance of integrating cybersecurity into supply management

A primary reason the supply chain is leveraged for cyberattacks is suppliers' weak cybersecurity levels. Despite the rising risk, suppliers—often smaller companies—do not have sufficient measures to protect themselves against attacks. With fewer operational resources and limited capabilities, they're left exposed. Even when made aware of the importance of cybersecurity, suppliers place more emphasis on key operational performance measures like speed and cost than cybersecurity-related measures. This inclination within supply management is akin to other emerging issues in the discipline (e.g., sustainability in the supply base).

Supply management thus plays an essential role in securing against cyberattacks. Cybersecurity must be integrated into the supplier selection process, and continuous supplier development in cybersecurity is necessary. After all, in today's digitally connected environment, companies can remain vulnerable to cyberattacks originating from their supply chains regardless of their own defense level. In that regard, supply managers must take a leadership role in cybersecurity, orchestrating their supply chains in the same way they do when facing other key business issues.

Understanding the digital supply chain for cybersecurity

Like physical products, most software products are not built by a single supplier. They consist of multiple modules, potentially made of sublevel modules, forming "software supply chains." Companies embedded in software supply chains face challenges akin to those in conventional supply chains. While recent studies consistently reveal that a significant portion of software modules rely on vulnerable components within their supply chains, it is difficult to map what constitutes a software supply chain below the first-tier

supplier/module and how a software supply chain evolves over time. This challenge becomes more serious when hackers exploit vulnerabilities in a low-tier supplier/module in software supply chains.

In 2021, for example, Log4J, an obscure but widely used software that records computer system activities, was exploited through a security vulnerability that allowed malicious attackers to infiltrate the system without using valid passwords. Digital goods, by nature, can be readily and instantaneously accessed from the outside. As new vulnerabilities are disclosed, hackers may exploit them before they are resolved. Software products using vulnerable modules in their supply chains remain at risk of cyberattacks unless these issues are addressed.

Recent developments and best practices

In response to the rising risk of cyberattacks, government agencies and industry organizations have developed frameworks that supply chain managers should adopt.

Similar to traditional Bill of Materials practice, the Software Bill of Materials (SBOM) details the required software modules for a product. This helps organizations understand the components within their software, allowing for better tracking of potential vulnerabilities and responsive mediation of emerging issues in the software supply chain.

There is also a government-level movement toward creating standardized frameworks for managing supply chain cybersecurity. For example, the National Institute of Standards and Technology (NIST) released a Cybersecurity Supply Chain Risk Management framework, which underscores the issue's importance and provides a systematic approach to helping companies consider factors involved in supply chain cybersecurity.

Beyond technical tools, managerial attention to potential cybersecurity concerns is crucial. Cyberattack strategies evolve as hackers and defenders interact, meaning no permanent solutions can exist. Collective and responsive actions across organizational boundaries can mitigate the impact of potential cybersecurity risks. For instance, despite the severity of the log4j vulnerability, many companies and communities were proactive in addressing the issue collectively, effectively minimizing the ramifications.

In the next post, we will explore recent supply chain cyberattack cases and what lessons we can learn from them.

About the Global Supply Chain Institute

The University of Tennessee's Global Supply Chain Institute (GSCI) is the preeminent hub for supply chain thought leadership and talent development. The pinnacle of GSCI's efforts is UT's Supply

Chain Forum, which brings together more than 80 of the world's most innovative and impactful companies twice a year to learn, network, and recruit the country's top supply chain talent.

SC MR

(Photo: Getty Images)

Similar to traditional Bill of Materials practice, the Software Bill of Materials details the required software modules for a product, helping organizations understand the components within their software and better track vulnerabilities.

More Cyber Security

- Analyzing the supply chain risks behind the top data breaches in 2024
- Regulations are forcing organizations to address software supply chain security
- The 3 types of cyberattacks affecting global supply chains
- Cybersecurity as a major supply chain risk domain
- Maintaining Cybersecurity in a Growing Digital Supply Chain

> More Cyber Security

What's Related in Cyber Security

It's Time to Get Real About Cybersecurity

On this episode, Steven A. Melnyk discusses why cybersecurity needs to be at the top of every supply chain manager's to do list.

Listen in

Explore

> Explore Software & Technology

Topics

- News
- Software & Technology
- Artificial Intelligence
- Cloud
- Software
- Education
- Cyber Security
- Cyberattacks
- Digitization
- Supply Chain Security

Software & Technology News

- 6 Questions With … Christian Floerkemeier
- How Reddy Ice Transforms Data to Drive End-to-End Automation and Agility
- Gartner survey reveals AI, ESG and geopolitics top supply chain influences
- Managing supply chains in times of uncertainty: The emergence of digital twin technologies
- Stop buying technology. Start purchasing a problem-solving solution
- Applying lessons learned from healthcare drone logistics to other supply chains

> More Software & Technology

Latest Software & Technology Resources

Talking Supply Chain: How J&J's Luis Roman views digital transformations

As vice president of Johnson & Johnson's MedTech Supply Chain, Luis Roman has a front-row seat to the digital transformation of supply…

Listen in

- Talking Supply Chain: Explaining Agentic AI
- Talking Supply Chain: Will Visibility-as-a-Service enable full supply chain transparency?

> More resources

Editors' Picks

U.S. tariffs create urgent need for supply chain agility

Trump's aggressive tariffs and the ongoing possibility of even greater…

DEI is dead; long live DEI (but you don't have to love it)

DEI, as a term, is effectively dead —there is too much negative

baggage…

Building resilience

Tariffs have been added to traditional disruptions such as climate and…

Tariffs, taxes and trade: The impact of Trump's reelection on the supply chain

From promises of new tariffs, lower taxes, and trade deal renegotiations, the…

Podcast: Talking Supply Chain: How J&J's Luis Roman views digital transformations

Webinar: How Reddy Ice Transforms Data to Drive End-to-End Automation and Agility

News: Where do your delivery boxes end up? Optimizing the lifecycle of last-mile packaging

News: 6 Questions With … Christian Floerkemeier

Artificial Intelligence: 6 Questions With … Christian Floerkemeier

NextGen Supply Chain Conference: It's time to stay focused

Research: Supply chain salaries, job satisfaction on the rise

Research: Supply Chain's Top Trends for 2024 Require Talent Investment for Success

› Explore more