CSCMP hottopics

JUNE | 2023

Securing the Supply Chain: Best Practices for Mitigating Cybersecurity Risks

By Carsten Sorensen, CEO, LynnCo

Understanding Today's Supply Chain Cybersecurity Challenges 1

Supply Chain Security Best Practices 2

Multi-Factor Authentication 2

Regular Vulnerability Assessments 2

Incident Response Plans 2

Disaster Recovery & Business Continuity Planning 3

A Look into the Future: Cybersecurity & The Supply Chain 3

CSCMP

Educating and Connecting the World's Supply Chain Professionals.™

The supply chain is a critical component of any business—the supply chain chaos of the pandemic has made that clear. The ability to keep goods and services flowing to customers is essential to maintaining operations and staying competitive. However, the rise in supply chain cyber attacks has added a new layer of risk to the already complex supply chain ecosystem. As more organizations rely on technology to manage their supply chain operations, the potential for cyber attacks increases.

In 2022 alone, the number of supply chain attacks was 40% higher than malware-based attacks. **Supply chain attacks targeted 1,743 entities and impacted over 10 million people.** Meanwhile, there were 70 malware attacks that touched approximately 4.3 million people.[1] These numbers indicate the severity and prevalence of supply chain cyber attacks, and the need for organizations to take measures to protect themselves.

All this is not to scare you away from implementing crucial technologies to better manage your supply chain. Instead, we are placing a spotlight on the best practices, trends, and technologies organizations can utilize to reduce cybersecurity risks and ensure the security and resilience of their supply chains. But first, it is important to comprehend the cyber threats to supply chains that are prevalent today.

UNDERSTANDING TODAY'S SUPPLY CHAIN CYBERSECURITY CHALLENGES

Today, there are various types of cyber threats supply chains face and the potential impact of a successful attack can be detrimental—both financially and reputationally. A successful cyber attack can damage the reputation of an organization, erode customer trust, and **result in significant financial losses**. It can also lead to regulatory fines, legal penalties, and other compliance issues.

Here is what we know about supply chain cyber attacks as the industry stands today:

- The top three supply chain cyber risks include malware attacks, security breaches, and data leaks and losses
- Cyber attacks on supply chains have recently increased by 51%[2]
- 82% of Chief Information Officers believe their organizations are vulnerable to cyberattacks specifically targeting supply chains[2]
- 40% of cyber threats are occurring within supply chains[2]
- 44% of organizations plan to increase their budget on supply chain cybersecurity in 2023[2]
- Only 32% of supply chain management leaders feel "very confident" in their ability to respond quickly and effectively to a cyber attack[2]

The impact of a successful cyber attack on the supply chain can be devastating. It can disrupt the flow of goods and services, cause financial losses, damage the reputation of the affected organization, and even affect national security. Even the U.S. recently announced a new national cybersecurity policy to proactively combat cyber attacks on supply chains: "The US will work with its allies and partners to counter cyberthreats and create reliable and trustworthy supply chains for information and communications technology."[3] [2]

[1] *Help Net Security (January 2023) "Supply chain attacks caused more data compromises than malware" Help Net Security. Retrieved from:* ***https://www.helpnetsecurity.com/2023/01/26/data-compromises-2022/***

Today, there are various types of cyber threats supply chains face and the potential impact of a successful attack can be detrimental—both financially and reputationally.

SUPPLY CHAIN SECURITY BEST PRACTICES

To mitigate cybersecurity risks in the supply chain, organizations should follow industry best practices and implement measures, such as:

- Multi-factor authentication
- Regular vulnerability assessments
- Incident response plan
- Disaster Recovery and Business Continuity planning

MULTI-FACTOR AUTHENTICATION

Multi-factor authentication (MFA) is an authentication method that requires users to verify their identity with at least two or more pieces of evidence in order to access software systems. To illustrate, the initial verification process might involve using a strong password. Meanwhile, the second verification step might necessitate the system sending a code to your phone that you would subsequently need to enter into the system to prove your identity is valid. Overall, MFA is an effective way to prevent unauthorized access to proprietary systems, networks, and data by doubling down on the authentication process.

REGULAR VULNERABILITY ASSESSMENTS

Additionally, vulnerability assessments, also referred to as "penetration tests," are key components of effective supply chain cybersecurity programs. These assessments can help identify and address weaknesses in the supply chain before they can be exploited by threat actors. By conducting regular vulnerability assessments—ideally on a quarterly basis—supply chain managers can:

- Identify and mitigate risks before they turn into major security incidents
- Proactively protect the reputation and financial stability of the organization
- Keep supply chain processes and systems in compliance with industry and government regulations
- Protect intellectual property and prevent the loss of confidential or sensitive information

Overall, vulnerability assessments are essential for maintaining the security and integrity of supply chains and should be standard practice for all organizations involved in supply chain management.

INCIDENT RESPONSE PLANS

Incident response plans can help organizations respond quickly and effectively in the event of a cyber attack. Essentially, these plans detail what an organization and various stakeholders in the business must do in the event of a security breach or incident. It's vital for supply chain teams to develop an incident response plan to address any cybersecurity threats that may affect the organization's supply chain.

This plan should outline specific steps supply chain teams should take in response to a breach, such as:

- Identifying affected systems and investigating the breach
- Communicating with vendors and partners
- Implementing measures to contain and mitigate the damage
- Notifying customers, regulators, and other relevant parties
- Administering a post-incident review to identify possible areas of improvement

[2] *LynnCo (February 2023) "The State of the Industry: Supply Chain & Logistics in 2023" LynnCo. Retrieved from:* ***https://marketing.lynnco.com/hubfs/The%20State%20of%20the%20Industry%20Supply%20Chain%20&%20Logistics%20in%202023.pdf***

[3] *Akshay Joshi et. al (March 2023) "The US has announced its National Cybersecurity Strategy: Here's what you need to know" World Economic Forum. Retrieved from:* ***https://www.weforum.org/agenda/2023/03/us-national-cybersecurity-strategy/***

CSCMP™

Educating and Connecting the World's Supply Chain Professionals.™

Any disruption in the supply chain, whether it's due to natural disasters, cyber attacks, or any other unforeseen events, can have severe consequences on the entire network.

With a well-crafted incident response plan in place, supply chain teams can act swiftly and confidently to minimize the impact of any cyber attack on the organization and its partners.

DISASTER RECOVERY & BUSINESS CONTINUITY PLANNING

Disaster Recovery (DR) and Business Continuity (BC) planning are critical components of a resilient supply chain. Supply chains are complex networks that involve multiple entities, including suppliers, manufacturers, distributors, and retailers. Any disruption in the supply chain, whether it's due to natural disasters, cyber attacks, or any other unforeseen events, can have severe consequences on the entire network. Therefore, having a comprehensive DR/BC plan in place can help supply chain managers mitigate risks and ensure continuity of operations.

By identifying potential risks, establishing communication protocols, and developing backup plans, organizations can minimize the impact of disruptions on their supply chain and ensure that products and services are delivered to customers on time. Ultimately, DR/BC planning is an essential aspect of supply chain management that helps ensure the smooth functioning of operations, even during unexpected events.

Key Points to Consider:

- DR/BC is a team sport, not just an Information Technology event. Include the business and key partners/vendors in your planning.
- Create a tiered approach to the critical business organizations and functions
- Identify the scope of the DR/BC Plan
- Identify dependencies between business functions and critical organizations
- Determine an acceptable downtime for each tier of service
- Ensure your backups and restoration points are immutable and can't be changed once you commit them
- Assume at some point you will need to deploy DR/BC, so test it often
- Review, update, and improve your plan constantly

A LOOK INTO THE FUTURE: CYBERSECURITY & THE SUPPLY CHAIN

Here's the truth. We don't expect cyber threats to supply chains to slow down or weaken any time soon. It's quite the contrary, in fact. We expect cybersecurity attacks to become more sophisticated at breaching supply chains across the globe. That being said, we also expect that due to the rise in cyber attacks and the increase in sophistication, supply chain leaders will begin to prioritize proactive cybersecurity measures. This means supply chain cybersecurity is likely to become more proactive and focused on risk management, with organizations adopting new tools and strategies for threat detection and prevention.

Furthermore, we expect to see supply chain leaders gain a seat at the executive table, as there will be a growing collaboration between stakeholders in the supply chain, cybersecurity leadership, and business leaders to strengthen supply chain cybersecurity and build a culture of security awareness and resilience throughout the organization. To stay ahead of the threat actors, it's time to implement more robust cybersecurity measures throughout your supply chain.

LynnCo offers a wide array of services, from Managed Transportation to Supply Chain Consulting. Each of our subject matter experts can help you and your team optimize your supply chain and get on the right track to strengthen your supply chain security posture. Reach out to us at **LynnCo.com**—we'd be happy to help!

CSCMP™

Educating and Connecting the World's Supply Chain Professionals.™

About CSCMP Hot Topics

Issues of *CSCMP Hot Topics* may include early results from ongoing research being conducted for CSCMP or other organizations; new supply chain practices, thought-provoking ideas, or emerging trends; discussions of changes in the broader business and regulatory environment that may impact the supply chain and logistics field.

CSCMP™

Educating and Connecting the World's Supply Chain Professionals.™

About LynnCo

LynnCo is a global leader in supply chain analytics and operational solutions. Over 25 years, we have quietly built a leading supply chain platform of solutions and technology for high-growth companies. At LynnCo, we work collaboratively with mid-market, emerging growth companies to help improve supply chain performance. By looking deeper into their needs and challenges we are able to find the right solutions for long-term success. To learn more about LynnCo, please visit **LynnCo.com**.

About the Author: Carsten Sorensen

Carsten Sorensen, CEO of LynnCo, is a technology and finance executive with a broad background in a variety of industries and extensive European work experience. A former software engineer, Mr. Sorensen has over 25 years of experience combining technology, mergers, acquisitions and finance as well as a deep operating background to the organizations he works with. He has worked as a senior executive in fast-growing companies, both private and public, and is comfortable balancing the conflicting needs of high-growth and long-term strategy within organizations he runs. Carsten is a keen steward of a company's culture and understands its importance for long-term financial and strategic results.