

## Cybersecurity in Supply Chain

*Matthew N. O. Sadiku*

*Department of Electrical & Computer Engineering, Prairie View A&M University,  
Prairie View, TX USA*

*Uwakwe C. Chukwu*

*Department of Engineering Technology, South Carolina State University, Orangeburg, SC, USA*

*Janet O. Sadiku*

*Juliana King University, Houston, TX, USA*

**Abstract:** A supply chain is all the processes that enable the flow of goods and services between multiple entities to end customers. Key entities of a supply chain include partners, vendors, suppliers, and service providers that have direct or indirect influence on the production and delivery of your end product or service. If just one part gets compromised, the entire system is at risk. Every company is exposed to internal and external risks stemming from supply chain disruptions. Cyber criminals and other threat actors have been targeting supply chains more actively in recent years. The consequences of such an attack can be severe, operationally, financially, and reputationally. This paper introduces readers to supply chain cybersecurity.

**Keywords:** supply chain, cyber attacks, cyber threats, cybersecurity in supply chain, supply chain risk management.

### INTRODUCTION

Supply chains are the networks between a company and the suppliers it relies on to distribute the company's products or services. In today's complex and tightly interconnected world, it is hard to deliver a product or service without a supply chain. Just like a human body consists of different organs and systems, a supply chain comprises different companies, activities, people, resources, and information [1].

Supply chain networks have been driven by technology for decades. Ironically, the same technologies that make supply chains faster and more effective also threaten their cybersecurity. For example, the adoption of advanced technologies, such as blockchain for assuring data integrity, drones for remote deliveries and robots for warehouse operations, have improved the efficiency in logistics processes and global supply chain. The digital transformation that is enabling the supply chain sector to deal better with a disruptive norm is providing cybercriminals with opportunities to infiltrate companies.

The three most common risks affecting supply chain industry are data leaks, breaches, and malware attacks. Employees, hackers, malicious competitors, and managers can leak sensitive data and personal information. Security breaches often occur when a hacker or malicious user infiltrates an operating system/network without permission. Data breaches are one of the most serious cybersecurity threats faced by organizations. Malware attacks can happen through ransomware that locks a computer until the business pays a ransom [2]. Figure 1 shows how cyberattack on a vendor causes supply chain failure [3].

Published under an exclusive license by open access journals under Volume: 3 Issue: 6 in Jun-2023

Copyright (c) 2023 Author (s). This is an open-access article distributed under the terms of Creative Commons Attribution License (CC BY). To view a copy of this license, visit <https://creativecommons.org/licenses/by/4.0/>

## OVERVIEW ON CYBERSECURITY

Cybersecurity refers to a set of technologies and practices designed to protect networks and information from damage or unauthorized access. It is vital because governments, companies, and military organizations collect, process, and store a lot of data. As shown in Figure 2, cybersecurity involves multiple issues related to people, process, and technology [4].

A typical cyber attack is an attempt by adversaries or cybercriminals to gain access to and modify their target's computer system or network. Cyber attacks are becoming more frequent, sophisticated, dangerous, and destructive. They are threatening the operation of businesses, banks, companies, and government networks. They vary from illegal crime of individual citizen (hacking) to actions of groups (terrorists) [5].

The cybersecurity is a dynamic, interdisciplinary field involving information systems, computer science, and criminology. The security objectives have been availability, authentication, confidentiality, nonrepudiation, and integrity. A security incident is an act that threatens the confidentiality, integrity, or availability of information assets and systems [6].

- *Availability*: This refers to availability of information and ensuring that authorized parties can access the information when needed. Attacks targeting availability of service generally leads to denial of service.
- *Authenticity*: This ensures that the identity of an individual user or system is the identity claimed. This usually involves using username and password to validate the identity of the user. It may also take the form of what you have such as a driver's license, an RSA token, or a smart card.
- *Integrity*: Data integrity means information is authentic and complete. This assures that data, devices, and processes are free from tampering. Data should be free from injection, deletion, or corruption. When integrity is targeted, nonrepudiation is also affected.
- *Confidentiality*: Confidentiality ensures that measures are taken to prevent sensitive information from reaching the wrong persons. Data secrecy is important especially for privacy-sensitive data such as user personal information and meter readings.
- *Nonrepudiation*: This is an assurance of the responsibility to an action. The source should not be able to deny having sent a message, while the destination should not deny having received it. This security objective is essential for accountability and liability.

Everybody is at risk for a cyber attack. Cyber attacks vary from illegal crime of individual citizen (hacking) to actions of groups (terrorists). The following are typical examples of cyber attacks or threats [7]:

- *Malware*: This is a malicious software or code that includes traditional computer viruses, computer worms, and Trojan horse programs. Malware can infiltrate your network through the Internet, downloads, attachments, email, social media, and other platforms. Spyware is a type of malware that collects information without the victim's knowledge.
- *Phishing*: Criminals trick victims into handing over their personal information such as online passwords, social security number, and credit card numbers.
- *Denial-of-Service Attacks*: These are designed to make a network resource unavailable to its intended users. These can prevent the user from accessing email, websites, online accounts or other services.

- *Social Engineering Attacks*: A cyber criminal attempts to trick users to disclose sensitive information. A social engineer aims to convince a user through impersonation to disclose secrets such as passwords, card numbers, or social security number.
- *Man-In-the-Middle Attack*: This is a cyber attack where a malicious attacker secretly inserts him/herself into a conversation between two parties who believe they are directly communicating with each other. A common example of man-in-the-middle attacks is eavesdropping. The goal of such an attack is to steal personal information.

These and other cyber attacks are shown in Figure 3 [8].

Cybersecurity involves reducing the risk of cyber attacks. Cyber risks should be managed proactively by the management. Cybersecurity technologies such as firewalls are widely available [9]. Cybersecurity is the joint responsibility of all relevant stakeholders including government, business, infrastructure owners, and users. Cybersecurity experts have shown that passwords are highly vulnerable to cyber threats, compromising personal data, credit card records, and even social security numbers. Governments and international organizations play a key role in cybersecurity issues. Securing the cyberspace is of high priority to the US Department of Homeland Security (DHS). Vendors that offer mobile security solutions include Zimperium, MobileIron Skycure, Lookout, and Wandera. As shown in Figure 4, industries that rely on supply chains include fast-moving, consumer goods, IT, manufacturing, healthcare, agriculture, and retail [1]. These industries should be aware of supply chain risks. The supply chain risks faced by organizations are shown in Figure 5 [1].

### CYBERSECURITY FOR SUPPLY CHAIN

A supply chain attack occurs when someone infiltrates your system through an outside partner or provider with access to your systems and data. Foreign adversaries, nation-state actors, hackers, and criminals seeking to steal, compromise or alter, and destroy sensitive information can target suppliers at all tiers of the supply chain. Supply chain attacks have never been higher due to new types of attacks, growing public awareness of the threats, and increased oversight from regulators. The problem is getting worse, with businesses relying more and more on outside providers.

Managing cyber supply chain risks requires ensuring the integrity, security, and resilience of the supply chain and its products and services. Cybersecurity should be an integral part of the risk management strategy of any supply chain. One cannot take for granted that the software that they use or purchase is secure.

Best practices for supply chain security include [10]:

- Log and track shipments. Use automated notifications for the sender and receiver.
- Use locks and tamper-evident seals during shipping.
- Inspect factories and warehouses.
- Require background checks on employees.
- Use accredited or certified suppliers.
- Perform security strategy assessments with local laws and governance policies in mind.
- Perform penetration and vulnerability testing on partners with which you share data.
- Authenticate all data transmission and identify requestors.
- Use permissions or role-based access to data.
- Require minimum cybersecurity or specific best practice baselines of vendors and resellers.

- Use licensed third-party auditors to certify potential partners.
- Train employees to be alert to changes and inconsistencies.
- Regularly audit open source and vendor source code.
- Restrict third-party programs' access and permissions.
- Use network level scanning, behavioral analysis and intrusion detection to identify potential breaches.
- Have a response plan in place for quickly acting on discovered threats.
- Consult governmental guidelines and regulations appropriate for your region.

## PROTECTING SUPPLY CHAIN

Cybersecurity and the IT department are the lifeblood of any company that wants to prevent, mitigate, and eliminate malware attacks, breaches, leaks, and infections. For cybersecurity, prevention is always better than cure. By planning for every contingency and seeking out future vulnerabilities, companies can inoculate themselves against would-be cyberattacks and viruses. To strengthen your supply chain security and be less vulnerable to potential threats, embrace the following best practices.

- *Establish a Proactive Program:* The best way to respond to a cyber attack is to prevent it from happening in the first place. Companies can build cybersecurity awareness into their supply chains. They should take a proactive approach to securing their supply chains against cyber attacks. Companies can ensure that every link of the supply chain is protected from cyber threats. This requires implementing a comprehensive cybersecurity awareness solution across the company. One of the most persistent trends in cybersecurity is the role of human beings in keeping organizations safe. They play a major role in incidents and breaches alike [11].
- *Malicious Insider Activity:* The entire supply chain, including your organization, may suffer from malicious insiders, who may be employees purposefully seeking to compromise your critical data and systems. Your employees, suppliers, and other supply chain entities may make accidental errors that put the supply chain at risk. In some cases, your employees and supply chain members can unintentionally cause data leaks, breaches, and supply chain damages or disruptions. Malicious insiders might steal valuable data like intellectual property or sensitive information on your finances, clients, and marketing strategies [1].
- *Limited Access:* In order to protect your important data and systems from malicious activity, do not blindly trust your supply chain. Limit your suppliers' privileged access to critical assets. You can apply the principle of least privilege, which means limiting employees' access to your organization's critical assets to only what is needed to perform regular duties [1]. An important element of a supply chain risk management program is applying a risk rating to all suppliers. Focus your supplier pool by pre-qualifying suppliers that meet your risk management criteria.
- *Continuous Monitoring:* This is a necessary practice because your business partners can and do – change their processes all the time. It is necessary to continuously monitor for changes in your own business, your supply chain network, and changes in regulations. Continuous monitoring can limit potential cyberattacks and data breaches [12]. Cybersecurity is not a one time process. It needs undivided attention and active measures to prevent threats.
- *Staying Vigilant:* Organizations should always be vigilant to look out for new cyber risks. The best way to be vigilant is to establish a management process to review supply chain cyber risks on a continuous basis and keep working to enhance the supply chain process [13].

## **BENEFITS**

The benefits of supply chains come at the price of cybersecurity risks posed to each supply chain entity. Supply chain security is a part of supply chain management that helps to ensure the security of the supply from threats like theft, counterfeiting, cyberattacks, and natural disasters. It focuses on the risk management of external suppliers, vendors, logistics, and transportation. It primarily involves minimizing risks from using software developed by another organization, and securing organizational data accessed by another organization in your supply chain. Its goal is to identify, analyze, and mitigate the risks inherent in working with other organizations as part of a supply chain.

Other benefits of supply chain security include the following [14]:

- Improved Security
- Better Compliance
- Increase in Efficiency
- Enhanced Reputation
- Improved Risk Management

## **CHALLENGES**

Cybersecurity is a topic that is fraught with complexity and confusion. Research shows that organizations have an inflated sense of their supply chain's cybersecurity. While companies implement a global supply chain management strategy in order to boost their competitive advantage, many of the benefits that come along with supply chains can also increase an organization's risk of quality, safety, business continuity, reputation, and cybersecurity. Because supply chains may involve many different organizations, there is no single set of established supply chain security guidelines or best practices. No single set of best practices can cover every situation.

Your organization's participation in the supply chain inevitably creates risk for your organization. Whether it is legal, compliance, financial, strategic, or reputational risk – the supply chain introduces your business to numerous potential disruptions to data, finances, or business operations at some point.

Cybercriminals know that IoT and IIoT security is not at its finest and this makes it easier for them to be target for a cyberattack. Supply chain attacks may take months to succeed. In many instances, such an attack may even go undetected for a long time. An enterprise could be vulnerable to a supply chain attack even when its own defenses are quite good [15].

## **CONCLUSION**

As the world becomes more tightly interconnected, organizations increasingly rely on extended supply chains to conduct business. Organizations that do not adequately manage their supply chain risks are more likely to fall victim to a cyberattack. Cyber risk is an increasingly important risk that supply chains introduce to organizations. In order to manage cyber risk smartly, companies need to keep the security of their supply chains a priority. Cybersecurity is near the top of the list of priorities of most CIOs. If you are a supply chain leader, you should know where your business is on the risk spectrum and now is the time to make cyber resilience a core priority [16].

Supply chains are getting more global and complex than ever, so are the associated risks. Cyber risk is part of the new business reality today. Organizations that are proactive in adopting security measures will be better positioned to manage the risks associated with their supply chain. Cybersecurity threats do not have to be an inevitable fate that organizations must face. More information about cybersecurity in supply chain can be found in the books in [17-30] and the following related periodicals:

- *Journal of Cybersecurity*
- *Cyber Security Journal*
- *Security Magazine*

## REFERENCES

1. “Major supply chain cybersecurity concerns and 7 best practices to address them,” July 2022, <https://www.ekransystem.com/en/blog/supply-chain-security>
2. “Cybersecurity risks to consider in supply chain management,” <https://www.cybersaint.io/blog/cybersecurity-in-supply-chain-management-risks-to-consider>
3. “Six degrees of separation: Cyber risk across global supply chains,” August 2017, <https://www.nortonrosefulbright.com/en-us/knowledge/publications/dfa3603c/six-degrees-of-separation-cyber-risk-across-global-supply-chains>
4. “Eliminating the complexity in cybersecurity with artificial intelligence,” <https://www.wipro.com/cybersecurity/eliminating-the-complexity-in-cybersecurity-with-artificial-intelligence/>
5. M. N. O. Sadiku, S. Alam, S. M. Musa, and C. M. Akujuobi, “A primer on cybersecurity,” *International Journal of Advances in Scientific Research and Engineering*, vol. 3, no. 8, Sept. 2017, pp. 71-74.
6. M. N. O. Sadiku, M. Tembely, and S. M. Musa, “Smart grid cybersecurity,” *Journal of Multidisciplinary Engineering Science and Technology*, vol. 3, no. 9, September 2016, pp.5574-5576.
7. “FCC Small Biz Cyber Planning Guide,” <https://transition.fcc.gov/cyber/cyberplanner.pdf>
8. “The 8 most common cybersecurity attacks to be aware of,” <https://edafio.com/blog/the-8-most-common-cybersecurity-attacks-to-be-aware-of/>
9. Y. Zhang, “Cybersecurity and reliability of electric power grids in an interdependent cyber-physical environment,” *Doctoral Dissertation*, University of Toledo, 2015.
10. “Supply chain security,” <https://www.techtarget.com/searcherp/definition/supply-chain-security>
11. S. McAlmont, “Why cybersecurity has never been more important for the supply chain sector” October 2022, <https://www.supplychainbrain.com/blogs/1-think-tank/post/35798-why-cybersecurity-has-never-been-more-important-for-the-supply-chain-sector>
12. “Cybersecurity risks in supply chain management,” June 2022, <https://reciprocity.com/blog/cybersecurity-risks-in-supply-chain-management/>
13. “Cyber security risks in supply chain management – Part 2,” March 2015, <https://resources.infosecinstitute.com/topic/cyber-security-risks-in-supply-chain-management-part-2/>
14. “Building a secure future: Strategies for managing cybersecurity in the supply chain,” March 2023, <https://www.ssl2buy.com/cybersecurity/cybersecurity-supply-chain-risk-management>
15. “Understanding the increase in supply chain security attacks,” July 2021, <https://www.enisa.europa.eu/news/enisa-news/understanding-the-increase-in-supply-chain-security-attacks>

16. S. Ashcroft, "Top 10: Supply chain cybersecurity vulnerabilities," October 2022, <https://supplychaindigital.com/digital-supply-chain/top-10-supply-chain-cybersecurity-vulnerabilities>
17. F. Liu et al., *Science of Cyber Security*. Springer, 2018.
18. U.S. Department of Commerce, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations: National Institute of Standards and Technology*. Independently published, 2022.
19. S. Carnovale and S. Yenyurt (eds.), *Cyber Security and Supply Chain Management: Risks, Challenges, and Solutions (Trends, Challenges, and Solutions in Contemporary Supply Chain Management, 1)*. World Scientific Pub Co Inc., 2021.
20. J. Manners-Bell, *Supply Chain Risk Management: How to Design and Manage Resilient Supply Chains*. Kogan Page, 3rd edition, 2020.
21. K. M. Koepsel, *The Aerospace Supply Chain and Cyber Security: Challenges Ahead*. SAE International, 2018.
22. N. Polemi, *Port Cybersecurity: Securing Critical Information Infrastructures and Supply Chains*. Elsevier Science, 2017.
23. E. Osborn, *Learning Supply Chain Cybersecurity*. Germany, LinkedIn.com, 2019.
24. T. A. Cook, *Managing Global Supply Chains: Compliance, Security, and Dealing with Terrorism*. Taylor & Francis, 2008.
25. T. Kieras, J. Farooq, and Q. Zhu, *IoT Supply Chain Security Risk Analysis and Mitigation: Modeling, Computations, and Software Tools*. Springer, 2022.
26. B. Halak, *Hardware Supply Chain Security: Threat Modelling, Emerging Attacks and Countermeasures*. Springer, 2021.
27. K. Sigler, D. Shoemaker, and A. Kohnke, *Supply Chain Risk Management: Applying Secure Acquisition Principles to Ensure a Trusted Technology Product*. Boca Raton, FL: CRC Press, 2017.
28. Australian National Audit Office, *Management of Cyber Security Supply Chain Risks: Auditor-General Report No.9 2022-23*. Australian National Audit Office, 2022.
29. A. G. Arway, *Supply Chain Security: A Comprehensive Approach*. Taylor & Francis, 2013.
30. K. M. Koepsel, *Supply Chain Vulnerabilities Impacting Commercial Aviation*. SAE International, 2020.

## ABOUT THE AUTHORS

**Matthew N. O. Sadiku** is a professor emeritus in the Department of Electrical and Computer Engineering at Prairie View A&M University, Prairie View, Texas. He is the author of several books and papers. His areas of research interest include computational electromagnetics and computer networks. He is a life fellow of IEEE.

**Uwakwe C. Chukwu** is an associate professor in the Department of Industrial & Electrical Engineering Technology of South Carolina State University. He has published several books and papers. His research interests are power systems, smart grid, V2G, energy scavenging, renewable energies, and microgrids.

**Janet O. Sadiku** holds bachelor degree in Nursing Science in 1980 at the University of Ife, now known as Obafemi Awolowo University, Nigeria and Master’s degree from Juliana King University, Houston, TX in December 2022. She has worked as a nurse, educator, and church minister in Nigeria, United Kingdom, Canada, and United States. She is a co-author of some papers and books.

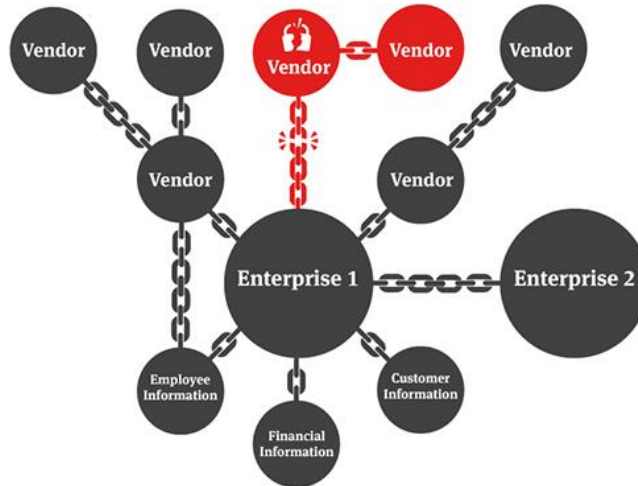


Figure 1 How cyberattack on a vendor causes supply chain failure [3].

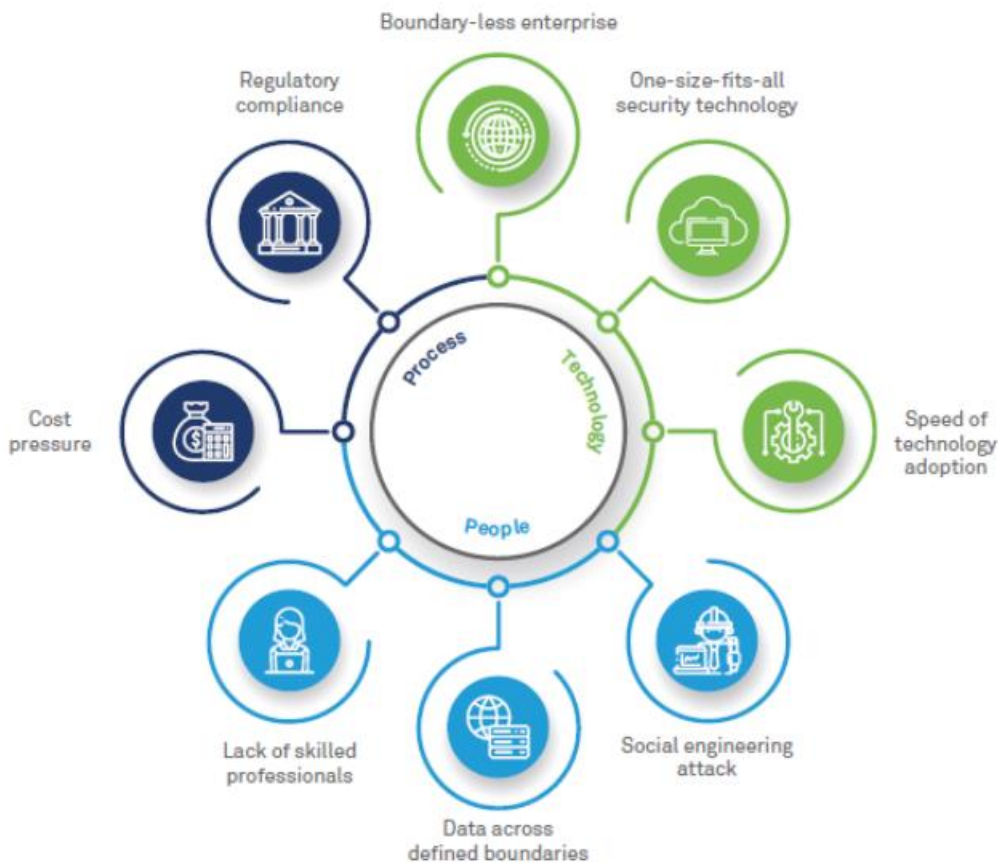


Figure 2 Cybersecurity involves multiple issues related to people, process, and technology [4].



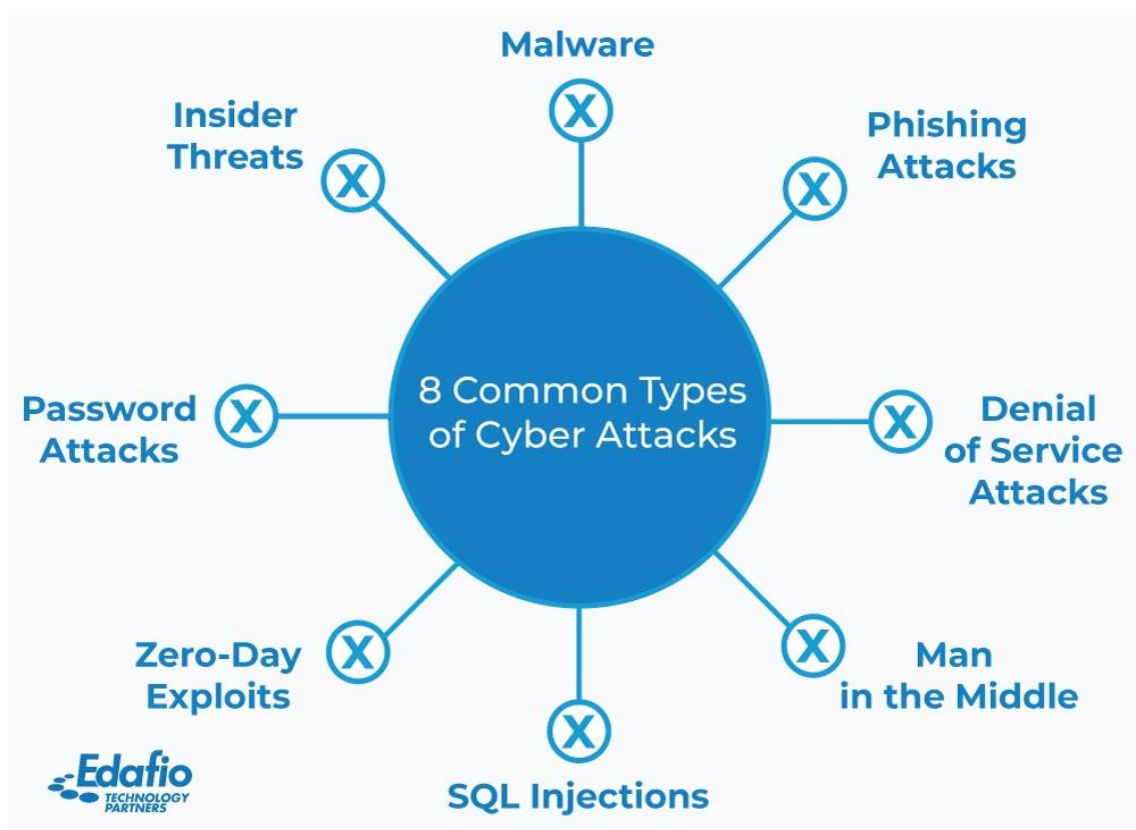


Figure 3 Common types of cyber attacks [8].

### Industries vulnerable to supply chain risks



Figure 4 Industries that rely on supply chains [1].

### Major supply chain risks


<b>Financial risks</b>	<ul style="list-style-type: none"> <li>• Revenue loss</li> <li>• Contractor bankruptcy</li> <li>• Business partner fines &amp; penalties</li> <li>• Compliance fines</li> </ul>	
<b>Reputational risks</b>	<ul style="list-style-type: none"> <li>• Loss of brand's good name</li> <li>• Reputational damage among partners</li> <li>• Loss of trust among customers and investors</li> </ul>	
<b>Legal risks</b>	<ul style="list-style-type: none"> <li>• Legal disputes with suppliers</li> <li>• Lawsuits</li> <li>• Administrative penalties</li> </ul>	
<b>Operational risks</b>	<ul style="list-style-type: none"> <li>• Interruptions of business operations</li> <li>• Supply chain disruptions</li> <li>• System breakdowns</li> </ul>	
<b>Cybersecurity risks</b>	<ul style="list-style-type: none"> <li>• Supply chain attacks</li> <li>• Malicious insider activity</li> <li>• Inadvertent threats</li> </ul>	

Figure 5 The supply chain risks faced by organizations [1].