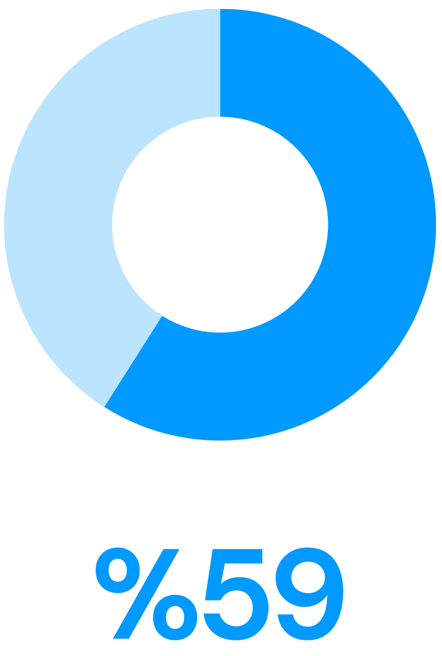
bugbounter

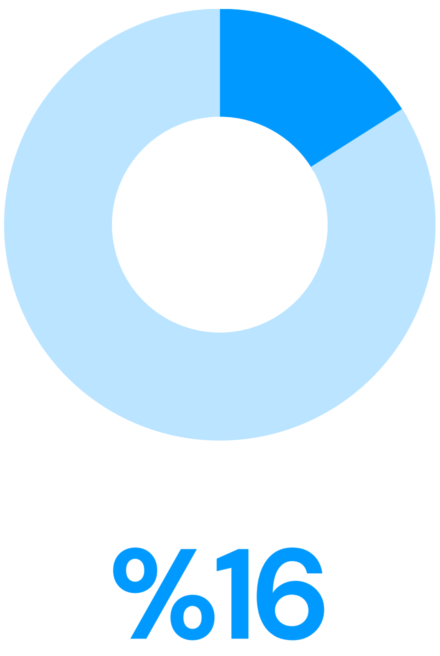
# Cybersecurity in Supply Chain

May 2023

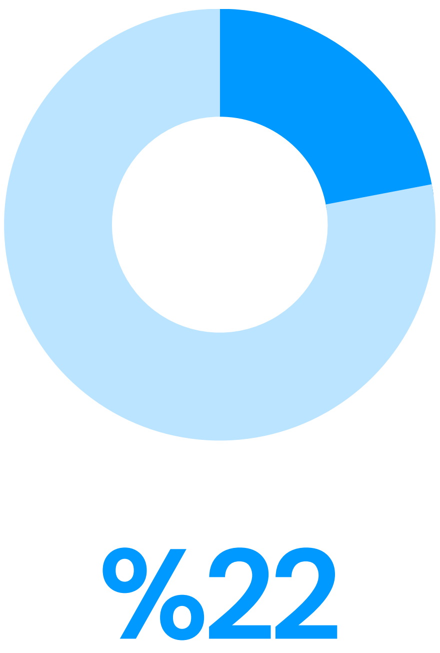
Organizations and their supply chain partners are becoming more interconnected every day, and thus, cybersecurity threats via supply chain partners deeply affect the contracted companies. Even though businesses protect themselves with the most advanced security methods, it is crucial that their suppliers and partners have similar levels of security. Therefore, companies need to consider the potential for cyberattacks via the supply chain to effectively protect their sensitive data.



**According to the Data Risk in the Third-Party Ecosystem study by the Ponemon Institute**, 59% of companies are affected through their suppliers involved in cyberattacks.



On the other hand, only 16%of companies successfully eliminate potential risks via these business partners.



Furthermore, 22% of respondents were unaware if their collaborating suppliers had experienced a data breach in the past 12 months.

A supply chain attack signifies a breach via a contracted company such as a business partner or supplier. While it may seem initially challenging to control other stakeholders, there are ways to achieve this and thoroughly protect the company.

## Here are some methods to consider:

**Testing providers before beginning any business relationship is at the top of the list.**

Companies can request security tests from their suppliers at this stage. Through various audits, they can determine the answers to questions like, "What security tools are they using" "Which access policy do they prefer" "Do they update their patches promptly" Companies can also have the supplier tested by a trusted business partner using methods like penetration testing. Additionally, they can require their suppliers to publish a Vulnerability Disclosure Program (VDP) or run bug bounty for 24/7 check.

Taking all these into consideration, suppliers should demonstrate their level of security, be transparent to the companies they serve, and be open to developer suggestions. Having provisions related to security and privacy (confidentiality) in contracts with suppliers and strengthening these provisions with penalties is essential.

**However, several past incidents have proved that contracts alone don't adequately protect parent companies.**

## The following questions could also be asked to the supplier at this stage:

- Is software and hardware design documented?
- Are known vulnerabilities present in the product design?
- How does the provider respond to emerging vulnerabilities? How can they fix a possible zero-day vulnerability?
- What is the performance of configuration management processes?
- At what level is malware protection and detection process?
- What security-related preventive measures are in place?
- What cyber and physical access controls are used? How are these documented and tested?
- Which types of employees are subjected to background checks? How are these documented and tested?
- How secure is the distribution process?
- Are authorized and approved distribution channels clearly documented?
- How is security maintained throughout the product's lifecycle?

## The second option is to continually monitor data access:

**Testing providers before beginning any business relationship is at the top of the list.**

The first step is to clearly define who can access what data, both within the company and on the supplier side. Companies can thus see to what extent they are connected to their stakeholders and which systems are accessible to whom.

## Thirdly, companies can train their suppliers' critical employees and ensure that their partners are improving themselves.

Cybersecurity training plays a significant role in raising awareness. Many different technologies are frequently used in daily operations, and because this results in a complex structure, it can become almost impossible to detect new risks. Risks arising from human error are as important as technology. Supply chains are becoming more complex with the involvement of more stakeholders, and the number of people using necessary technologies is increasing, but knowledge and skills are not keeping pace.

In a training organized for suppliers, companies should address common password mistakes, detecting phishing attempts, Business Email Compromise (BEC), and Vendor Email Compromise (VEC). In addition to these, teaching how to identify types of malwares, increasing vigilance against suspicious situations within the company, and sharing information on how to behave when encountering such situations is critical.

# The company needs to be protected with multi-layered cybersecurity measures.

**Testing providers before beginning any business relationship is at the top of the list.**

First and foremost, it's crucial to ensure that every device, network, and system within the organization has proper security controls in place. This includes robust firewalls, secure VPNs for remote access, regular system updates, and security patches.

Encryption should be utilized wherever possible, especially regarding data in transit or at rest. Additionally, network monitoring tools should be implemented to identify suspicious activities or patterns in real-time, enabling swift response to potential threats.
However, technical measures alone are not enough. Employee training and awareness are equally important, as the human element is often the weakest link in cybersecurity. Staff should be regularly trained on the latest cybersecurity threats and best practices, such as identifying phishing emails and using strong, unique passwords.

Furthermore, the company should adopt the principle of least privilege (PoLP), meaning that employees should only have access to the systems and data they need to perform their jobs. This can reduce the risk of insider threats and limit the potential damage if an employee's account is compromised.

Cybersecurity measures should also extend to third-party vendors and partners. Organizations should conduct thorough cybersecurity audits of these third parties and require them to adhere to the same or higher security standards.

## Finally, the implementation of a bug bounty program can be a valuable component of a robust cybersecurity strategy.

Such programs encourage independent researchers, also known as ethical hackers, to discover and report potential vulnerabilities in your systems. Through this approach, the organization can leverage the collective intelligence of the cybersecurity community to identify and fix vulnerabilities before they can be exploited by malicious actors. However, the company must remember that a bug bounty program is not a replacement for comprehensive security practices; it's an additional layer that can help to uncover blind spots.

These measures, along with a culture of cybersecurity awareness and vigilance, can help to protect the company from a wide range of threats. But it's important to remember that cybersecurity is a continuous process, not a one-time task. Threats and technologies are constantly evolving, and so must the company's cybersecurity strategy.

## Resources

- https://heimdalsecurity.com/blog/supply-chain-cyber-security/
- https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf
- https://medium.com/@KodiakRating/the-cyber-security-of-supply-chains-whos-the-real-risk-man-or-machine-ecdcc365d49d
- https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf
- https://databreachcalculator.mybluemix.net/?_ga=2.96830426.436800262.1577141175-921129177.1577141175&cm_mc_uid=18423071444915771411736&cm_mc_sid_50200000=91922601577141173609&cm_mc_sid_52640000=36284071577141173618