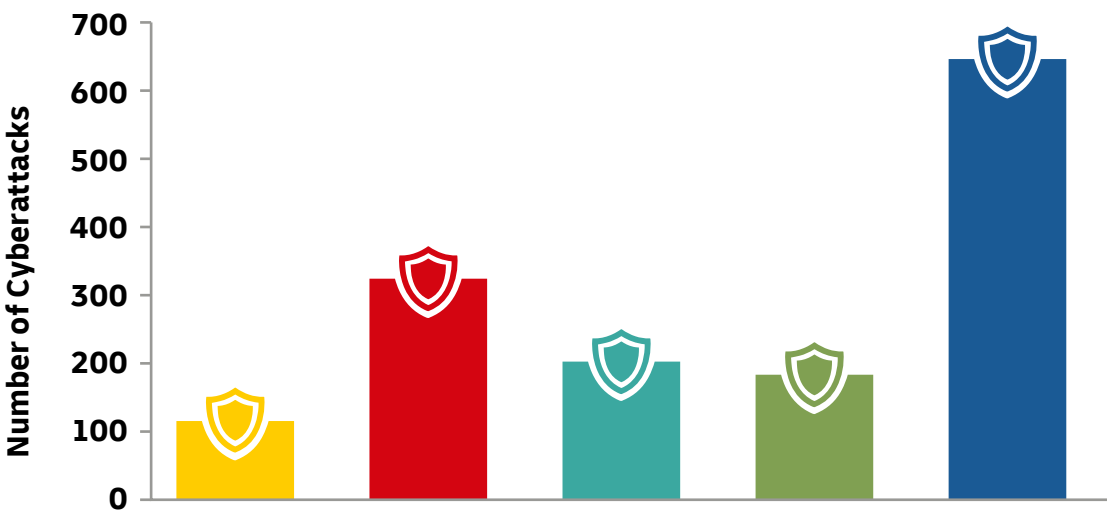
IS YOUR SUPPLY CHAIN **ECOSYSTEM CYBERSECURE?**

A continuously evolving technology landscape – and the new risks that come with it – has brought cybersecurity to the forefront. No longer the scope of the IT organization alone but a crucial priority for supply chain leaders and enablers of trust for regulators, end consumers, and society at large. But your supply chain can only be as strong as its weakest link.

2023 recorded the highest level of cyberattacks in the past **five years**



202% year-over-year increase

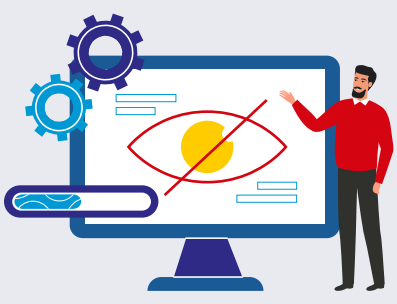
Source: 2024 Risk Report Everstream Analytics[1]

These cyberattacks affect all players across the supply chain – companies, suppliers and logistics providers. But it's the partner ecosystem that represents the highest vulnerability.

98% of organizations have a relationship with at least one third party that has experienced a breach in the last two years.[2]

67% of breaches were reported by a benign third party or by the attackers themselves – with only 33% discovered by the organization's own security teams or tools.[3]

With the extent of cyberattacks across the supply chain, collaboration is one of the most crucial priorities with the partner ecosystem because today



54% of organizations have insufficient visibility into the vulnerabilities of their supply chain.[4]

The consequences for organizations facing cyberattacks and data breaches are staggering. According to one IBM Security report:

277 days is the average time it takes to identify and contain a data breach.[5]

US$ 4.45 million is the average total cost of a data breach in 2023 – a 2.3% increase from 2022.[6]

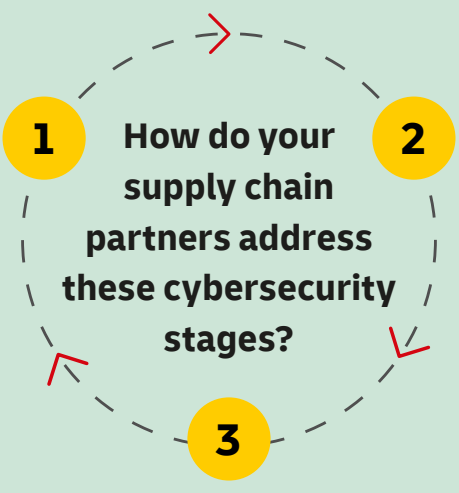
But the most significant impact of cyberattacks across your supply chain is reputational – and the lost business it represents.

90% of consumers say trust is the biggest deciding factor when choosing a brand[7] - and this trust can be easy to break. Recent research has found that 37% of consumers have switched brands to protect their privacy.[8]

So what can you do about this? Look for supply chain partners with the appropriate governance structures, guidelines, procedures and tools to safeguard your business and all its data.

PREVENT

- Compliance with existing regulations and certifications
- Procedures around testing and scanning of system vulnerabilities
- Assessments by reputable external security ratings agencies



RECOVER

- Robust IT infrastructure – people, technology, facilities
- Disaster recovery organization and systems
- Business continuity management approach

ADAPT

- Adopt a collaborative ecosystem approach
- Governance and change management approach
- Security technology investment including defensive AI

DISCOVER HOW WE DELIVER SUSTAINABLE CYBERSECURITY FOR YOUR SUPPLY CHAIN

Contact our supply chain experts **here** ›

or visit our **website** ›

[1] https://www.everstream.ai/special-reports/2024-supply-chain-annual-risk-report/
[2] https://www.weforum.org/publications/global-cybersecurity-outlook-2024/
[3] https://www.ibm.com/reports/data-breach
[4] https://www.weforum.org/publications/global-cybersecurity-outlook-2024/
[5] https://www.ibm.com/reports/data-breach
[6] https://www.ibm.com/reports/data-breach
[7] https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/business-trends-2024
[8] https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/seven-bets/experience