Five steps to fortify your supply-chain cyber-security resilience

March 2025

Daniela Nietz

As reliance on interconnected supply chains increases, cyber-security risks tied to external relationships are surging. These risks are often overlooked and can cause severe operational disruptions and significant financial losses for your business.

A strong cyber-security strategy allows you to tackle these challenges head-on. By embedding security across the entire supply chain, you can build trust, enhance resilience and gain a competitive edge in the process. The key is ensuring all stakeholders are equipped to handle cyber threats effectively.

1. Recognise what you are up against

Cyber criminals will actively exploit vulnerabilities introduced by gaps in the supply chain, from vendor to partner to third party. Understanding where these risks lie is the first step to protect your business from potential security failures.

Practical steps you can take

- **Study your supply chain:** take the time to look at your entire supply chain, from upstream suppliers to downstream customers. You should focus on understanding how data flows between these areas, assess their security measures, and determine which connections pose the highest risk to your supply chain.
- **Examine the potentially risky scenarios:** be prepared for even minor security gaps in your supply chain. For example, if an email from a supplier you trust becomes compromised, you will need to have appropriate frameworks in place to deal with this effectively.
- **Assess indirect risks:** investigate how a security failure in one part of your supply chain could create a ripple effect throughout your business.

By following these steps, you will not only be able to take a more proactive stance on cyber security across your supply chain, but also actively mitigate risks before they escalate.

2. Keep up to date with regulations

Cyber-security legislation is changing fast. As the Cyber Resilience Act (CRA) comes into force, you and your team must stay on top of new regulations to ensure compliance and meet mandatory cyber-security standards across your supply chain.

Practical steps you can take

- **Monitor and report:** stay one step ahead of potential attacks by monitoring your digital products continuously. Any exploited vulnerabilities should be reported by the manufacturer to the Computer Security Incident Response Team (CSIRT) and the European Union Agency for Cybersecurity (ENISA).

- **Assess risk of a product's lifecycle:** it is important to make assessments at every stage of the product's lifecycle so you can minimise threats to your supply chain from the outset.
- **Ensure your vendors are compliant:** if cyber-security risks are to be mitigated effectively, you will need to ensure your vendors abide by legislation and implement key security measures.

CRA compliance should be an essential part of your cyber-security strategy. Not only will it help you to build a robust and secure supply chain, but it will also ensure you protect your reputation.

3. Take control of supplier risk

A risk management approach is your foundation for staying ahead of cyber threats in your supply chain. It is about identifying vulnerabilities before they become crises, ensuring your resources are focused where they matter most. Instead of reacting to threats, you take charge – strengthening supplier security, safeguarding operations, and maintaining compliance with confidence.

Practical steps you can take

- **Identify high-priority suppliers:** protect your assets by evaluating suppliers based on their role in your operations, the type of data they handle, and their exposure to cyber threats.
- **Segment suppliers by risk level:** to enhance your cyber-security measures for suppliers, categorise vendors into high-, medium- and low-risk groups to identify where to focus your attention.
- **Allocate resources effectively:** dedicate security investments and monitoring efforts to high-risk suppliers, while maintaining oversight of lower-risk vendors. This will help to enhance operational resilience.

A proactive approach is essential here. Regular assessments of your suppliers will keep your strategy agile in the face of evolving threats and ensure you are in a stronger position to respond to emerging risks.

4. Uncover the weak links

One important aspect of your strategy is to make sure your security measures align with your expectations. Regular audits and assessments uncover vulnerabilities before they become serious threats, helping you to stay ahead of risks and avoid compliance violations.

Practical steps you can take

- **Schedule regular audits:** keeping a close eye on your suppliers means that you can be prepared for any risks that might arise. The regularity of these is determined by your risk levels, but a good baseline could be:
  - high-risk suppliers should undergo in-depth security reviews quarterly or bi-annually
  - medium- and low-risk suppliers can be assessed annually or every 18–24 months.
- **Assess cyber-security posture:** use security questionnaires, vulnerability scans and compliance checks to evaluate supplier security readiness.
- **Refine security measures:** use audit insights to enhance security expectations, adjust risk assessments and work collaboratively with suppliers to strengthen their cyber-security posture.
- **Evaluate new partnership risks:** ensure vendors meet strict cyber-security standards by assessing their compliance, risk history, data handling and third-party dependencies, while contracts should mandate security requirements, incident reporting, audit rights and clear exit strategies to safeguard your supply chain.

This helps you build a resilient, future-ready business that can navigate evolving threats with confidence.

5. Strengthen your defences

Taking a dynamic stance on mitigation empowers your business to operate with agility and confidence. Instead of scrambling to contain cyber incidents, you will have the right structures in place to prevent disruptions before they happen. By strengthening supplier relationships, refining response strategies and continuously improving security measures, you can ensure your supply chain remains resilient. This will allow your business to focus on growth, innovation and long-term success.

Practical steps you can take

- **Strengthen supplier contracts:** set clear security expectations, define response obligations and enforce accountability, with penalties for non-compliance.
- **Conduct regular incident response drills:** simulate cyber attacks with suppliers to improve crisis response and build resilience.
- **Continuously optimise:** learn from real-world incidents and audit findings to enhance security protocols and stay on top of new threats.

Embedding resilience into your supply chain will give you a strategic advantage that ensures your business continues to thrive.

As supply-chain cyber attacks continue to rise, businesses can no longer afford to be reactive. The risks are real, the impact is severe, and the time to act is now. A proactive approach – one that embeds security across your entire supply network – will not only protect your operations but also strengthen trust with partners and customers. By taking decisive steps today, you can turn cyber resilience into a competitive advantage, ensuring your business stays ahead of evolving threats.