BEST STRATEGIES TO MANAGE YOUR SUPPLY CHAIN RISKS

Your relationships with suppliers and vendors are important for business growth. Yet, they can leave you vulnerable to supply chain cyber attacks. Such attacks exploit the supply chain's weaknesses to infiltrate your systems and cause harm.

To avoid becoming a superspreader to other systems and organisations, businesses need to address vulnerabilities in their suppliers' and vendors' environments as well as their own. This is ever more crucial due to the rise of supply chain disruptions impacting businesses across various industries and sizes.

Identify risks in your supply chain hardware and software
Suffering an attack through your hardware or software can significantly affect your organisation. So, ensure that you scan and track all hardware and software to find potential threats, especially those from third-party providers that could carry more risk.

Screen external vendors carefully
External and third-party providers must go through a rigorous vetting procedure before you choose anyone to partner with. You may even need to expand your verification further if they have additional partners. It's crucial to plan out your vetting procedure before you initiate a partnership with any vendor.

Restrict access and permission for third-party programs
You can separate and limit access to specific vendors within specific departments. With a segmented network, you can contain the risks within a particular field even if your network is compromised. That way, it doesn't affect the entire chain.

Enact a comprehensive cyber defence strategy
Cyberattacks are becoming more sophisticated every day, and no business is immune. Just taking a proactive approach to preventing supply chain risks is not enough. You also need a robust incident response plan.

Outline working agreements clearly
When partnering with third-party vendors, develop a thorough agreement of their roles to protect your company's cybersecurity. Both parties must be clear about their expectations and adhere to security best practices.

Review and audit vendors regularly
Vendor screening shouldn't be limited to onboarding. They can create supply chain issues at any time, with or without their knowledge. Auditing vendors can help mitigate product quality or safety issues resulting from their quality control processes. An organisation can also measure the performance of a vendor using this approach.

Create an incident response strategy
It's crucial to have a plan that covers every step of dealing with any incidents that may arise. It should encompass readiness, response and recovery from technical and business perspectives.

Partner with an IT service provider
You might need an IT service provider who can offer you an integrated solution for vulnerability and patch management in real time. The solution would mitigate supply chain risks and build a strong cybersecurity posture for your organisation.

Larger supply chains have higher risks, making assessment and mitigation even more complicated. But you can quickly and effectively address a supply chain attack by having the necessary people, processes and technology in place.

CONTACT US TO SECURE **YOUR SUPPLY CHAIN TODAY**

KALARA® t: 01293265777 e: hello@kalara.co.uk