

5 Tips to help mitigate supply chain cybersecurity risks

Supply chain cyberattacks can significantly disrupt an organization's operations and damage its reputation. Understand these five supply chain cybersecurity risks and follow these best practices to help protect your business.

Recognize supply chain threat landscape

Thinking "it won't happen to us" can be detrimental. Understand the cyberthreats posed by different parts of the supply chain, including hardware, software, lifecycles of your products, and your vendors.



Create multifaceted supply chain security strategy

The flow of assets, data and software creates vulnerabilities at several points in the supply chain. Collaborate with IT security and risk management leaders on a joint supply chain cybersecurity risk management approach for the business.



Vet suppliers' security and risk management practices

Suppliers and other vendors can introduce cybersecurity risks to your business. Establish a formal vendor risk management program that includes conducting a risk assessment of each supplier before onboarding.



Manage remote work endpoint risk

With more employees working remotely – including your suppliers' employees – there are exponentially more endpoints that hackers can exploit. Educate employees, improve the security of their mobile devices, and consider implementing network monitoring where appropriate.



Address smart product security

The internet of things (IoT) and the digitization of supply chains opens up new attack vectors across the organization. IT, procurement, product development teams and other departments need to work together to create a holistic approach to mitigating cybersecurity risk.

