Make supply chain security your competitive advantage

Supply chain and third-party suppliers account for 55% of security breaches[1] – and each breach has reached an average high cost of $4.46 million[2]. Risk factors such as a remote workforce, multi-tier supply chains, complex security regulations, and digital supply chains all contribute to compromising the integrity of supply chain security architectures (Figure 1). With 62% of attacks exploiting customers[3], it is now more important than ever to take the necessary steps in securing your organization's supply chain.

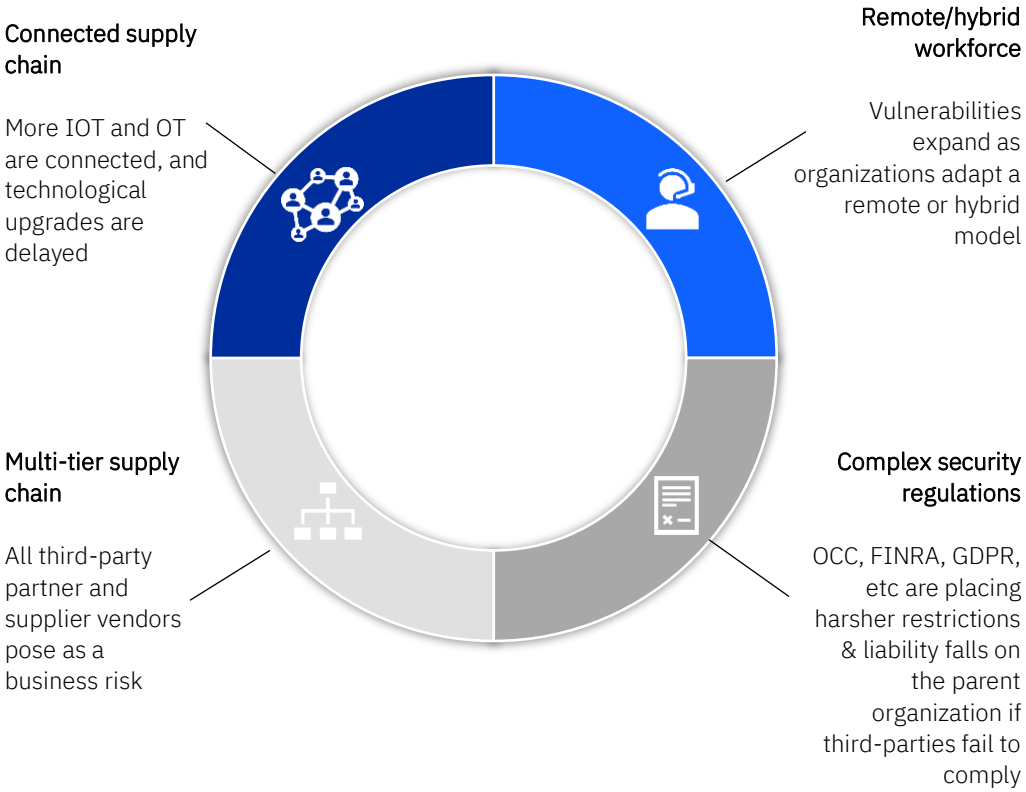

Figure 1. Key trends driving increased supply chain risks

Protect and secure your business with Supply Chain Cyber Risk Management

- **Comprehensive risk identification and management** to establish a core governance structure and a risk aware culture by defining a supplier management program
- **Secure the digital supply chain** by consistently assessing and categorizing third party software in the supply chain environment to define security control effectiveness
- **Drive efficiency with automation** by building a threat informed security program and requiring proper training for software development
- **Build operational resilience** to protect data and assets by adopting quantitative risk analyses and collaborating with supplier to improve cybersecurity practices

Supply chain and third-party suppliers account for

55% of security breaches.

Securing the supply chain comes with challenges

Key challenges can arise when trying to compose a comprehensive plan on how to rebuild the trust of customers and secure your supply chain. Identifying inherent risks in such a complex ecosystem of a multi-tier supply chain structure can be extremely challenging since visibility and threat intelligence is often limited. In addition, modernization of infrastructure and applications is critical but must be tailored to the specific security needs of each organization's supply chain data, customer information, manufacturing, and cloud technology. Without these technological modernizations, your company can be susceptible to OT/IOT attacks resulting in a loss of integrity and operational resilience.

Establish a strong foundation with a programmatic approach

How do you mitigate these risks to build a fortified security structure that aligns with your business objectives and protects your third-party supply chain ecosystem against cyber-attacks? There are a few questions to take into account when establishing a strong security program for your supply chain:

- Do you have the right governance model around strategy, new policies and procedures and change management?

How can IBM Security help?

- **Assess** current risk management functionalities to identify gaps against leading frameworks and industry standards
- **Design and Improve** an operational model, organizational governance structure, policies and procedures, and contract security requirements
- **Automate** the end-to-end vendor assessment to allow for continuous vendor monitoring
- **Manage** or co-source a functional and technical third-party risk program

- How are you going to establish processes to mitigate identified supplier risks?
- What technology will be put in place to help you drive efficiencies in the process?
- How do I know it is working?

Answering these questions helps you understand where you're at in your journey and how to strengthen your program.

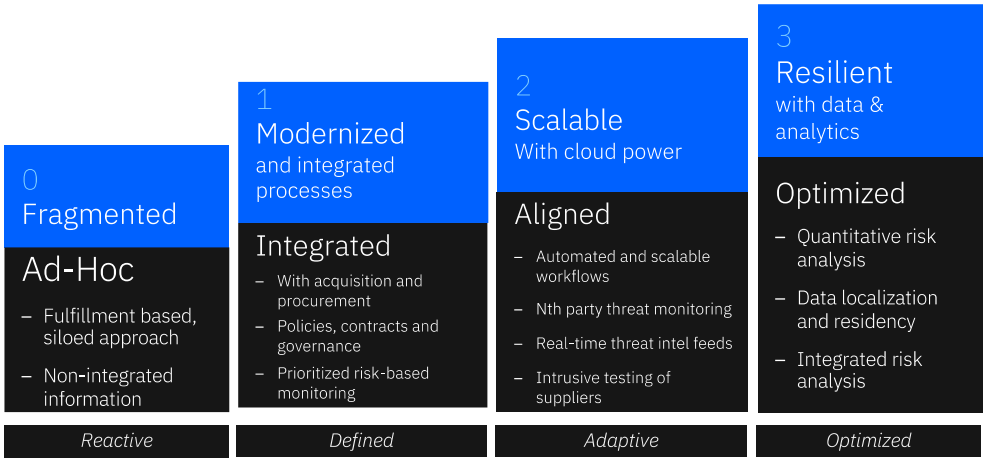

Figure 2. The four-step supply chain journey to secure your business

Journey to a secure supply chain

No matter where your organization is currently at, IBM Security can help move you forward with a four-step security journey that shifts your strategy from reactive to one that is defined, adaptive, and optimized by AI and data (see Figure 2). You can not only make supply chain security your competitive advantage but also reduce total cost of ownership by up to 70% and security opex costs by up to 40%.

Reduce total cost of ownership by up to

70%

with an optimized supply chain security strategy

Why IBM?

IBM has the breadth of expertise and skills you need to mitigate supply chain cyber risk. With end-to-end support, a large ecosystem of partners, and IBM's vast experience helping Fortune 500 clients reduce their supply chain and third-party risk, we can help you no matter where you are starting from.

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, provides security that moves with you.

IBM operates one of the broadest and deepest security research, development and delivery organizations. With more than 5500+ experts in more than 130 countries, we hold deep industry and security domain expertise deliver hundreds of advisory engagements each year, and help protect thousands of managed services clients.

We utilize a design thinking approach to bring business and security leaders together to co-create a solution tailored to your specific business needs now and as your challenges evolve.

For more information

To learn more about IBM Security Supply Chain Cyber Risk Management Services please contact your IBM representative, or visit https://www.ibm.com/services/grc

To schedule a no-cost half-day security workshop, submit a request at: https://www.ibm.com/security/resources/workshop

Sources:

1. The State of Third-Party Risk Management, 2022, Forrester
2. 2022 Cost of a Data Breach, IBM
3. https://www.enisa.europa.eu/news/enisa-news/understanding-the-increase-in-supply-chain-security-attacks