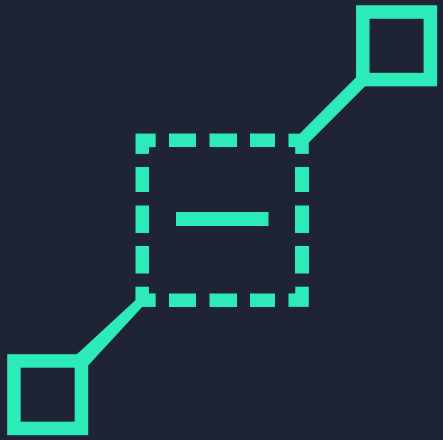
RiskXchange

SECURING THE SUPPLY CHAIN

Understand and mitigate
the supply chain
security risk of today’s
modern enterprises

You’re only as secure as the weakest link in your digital supply chain

Supply chain security is a real issue for enterprises in today’s connected digital economies



Supply chain security is crucial in today’s digital age. Not only can vulnerabilities be inherent or introduced and exploited at any point in the supply chain but they can also cause widespread disruption and damage to your organisation.

As traditional supply chains are transformed into more flexible, digital, connected, and customer-centred networks, the number of external links an organisation maintains grows exponentially. With that comes greater risks and vulnerabilities.

Larger, more flexible supply chain networks provide hackers with an extensive attack surface to target. They create more points of vulnerabilities in the flow of physical products and digital components within the supply chain. This not only emphasises the importance of powerful cyber security but also of protecting your organisation at every level.

The COVID-19 pandemic has seen many companies around the world shift to online infrastructure, pushing more of the supply chain online and onto the cloud. Organisations now have to work that much harder to ensure the physical and digital security of their products and services.

Organisations worldwide are doubling down on digitisation to increase their agility and responsiveness and be better prepared to deal with the impacts of the pandemic and its aftermath. The pandemic has not only pushed consumers online but has also seen a higher number of cyber incidents at the same time.

As companies expand their online and cloud-based operations, they expose themselves to an exponential increase in vulnerabilities. Additionally, organisations are turning to cheaper or alternative suppliers who may not have had their cybersecurity posture thoroughly vetted, exposing the entire organisation to new avenues of attack.

Greater needs creates greater risks

As organisations expand their operations, supply chains grow and with it so do the risks

In order to meet both business and consumer needs, enterprises have made their supply chains more flexible, integrating third-party vendors in super-quick time and, sometimes, without proper checks.

In many cases, organisations have allowed suppliers to connect directly into enterprise systems to speed up data sharing. Not only does it open a company's attack surface at the point of entry but increases the risks that come with the vendor's integrated supply chain.

It's not only the security of your own organisation to contend with but also ensuring that any organisation you partner with has the same level of care and security as yours. Third-party vendors, including cloud providers, facilities vendors, benefits providers, IT service providers, legal counsel, office suppliers, and more, all have the potential to cause significant damage to your organisation if their cybersecurity defences are not up to par.

According to Deloitte, more than 40% of cyberattacks are now believed to originate in entities within the extended supply chain or by external parties exploiting security vulnerabilities within that supply chain.

Companies now have to react quickly to secure the supply chain, explore alternative suppliers and expand the use of digital collaboration technologies. Changes that would normally take years to implement are now being compressed into a matter of weeks, leaving many security vulnerabilities unchecked.

This rapid diversification and digitalisation of supply chains is a necessary response to the pandemic, but it also increases security risks.

Understanding global cyber threats

Just as modern supply chains extend right around the world, so do the threats. Malicious actors are not bound by geography and can target any point in the supply chain, at any time

Key facts

1. Compromising geopolitics.

Cybercriminals are taking advantage of geopolitical difficulties to launch phishing lures, malware targeting, and disinformation campaigns. The global disruption caused by COVID-19 present significant opportunities for these activities, but it is just one of many vulnerabilities to watch out for.

2. Cybercriminals adapt

Conventional cybercrime and financially motivated attacks continue to pose a significant threat. But criminal networks are growing in maturity and resilience – they're finding weak points, bypassing network defences and then selling this access to other groups. They're also shifting their tactics to reduce the risk of detection, working in close-knit syndicates, increasing the precision of targeting, and taking advantage of their familiarity with local environments.

3. Expanding motives for ransomware

Ransomware attacks on corporations are becoming more than just financial. Ideological and political factors are now in play as well. Organisations must be able to prepare, prevent, detect, and contain these attacks, accepting if the motives are not financial, ransom payments may not rectify the situation.

4. Improved ecosystem hygiene is pushing threats up the supply chain.

As enterprises improve their own security, malicious actors are turning their attention to their suppliers. Organisations must look to expand their visibility over this increased threat profile, integrating cyberthreat intelligence into mergers & acquisitions and incorporating vendor and factory testing into their processes. Conducting security testing for products and services from the supply chain should be prioritized based on risk analysis from cyber threat intelligence in correlation with internal vulnerability analyses.

5. Vulnerabilities in cloud infrastructure demand costly solutions.

The vulnerabilities and threats associated with migrating to the cloud are ever-evolving. It is important to consider all risks and challenges linked to cloud adoption specific to the company’s systems, mission and data. An organisation that uses cloud service providers (CSP) or adopts cloud technologies without becoming fully informed of the risks involved exposes itself to a myriad of financial, commercial, legal, technical, and compliance risks.

The solution? Make security a core part of the entire supply chain.

In order to manage growing threats, organisations must adopt security principles across the entire supply chain. This includes making cybersecurity a priority not just within the core enterprise, but across all connected organisations as well. This includes developing traceability solutions for improved visibility across your network.

Tighter security ensures a more secure enterprise and a secure supply chain. Not only does it help secure sensitive data and reduce the attack surface, but it is extremely important for brand perception as well. Businesses, today, need to ensure the security of products across their entire supply network.

No industry is exempt. While the obvious targets remain (such as financial, consumer goods, pharmaceuticals and industrial products), other sectors also face increased risks.

Take the automotive industry, for example. Connected vehicles could become lethal weapons if successfully hacked and misdirected. The implications for sectors like aerospace and defence are equally grave.

Regulatory implications are also important. For sectors like telecommunications, critical infrastructure, aerospace, and defence, ensuring supply chain security and transparency is key.

Regulatory requirements like the Cybersecurity Maturity Model Certification (CMMC) and NIST SP 800- 171 are put in place to combat growing cyber threats across supply chains, making cybersecurity a foundational requirement for government acquisition of commercial products and services.

Five practical steps to get ahead

1. Create a dedicated programme.

Establish a central programme to incorporate cross-business coordination and coherence to supply chain security decisions.

2. Gain greater visibility throughout the network.

Bring data and analysis together from across the whole network, including external parties.

3. Understand threats and weaknesses.

Bring all the data together and expose previously hidden threats and supply chain vulnerabilities.

4. Put the right solutions in place.

Commit the resources needed to sustain supply chain security in a constantly evolving threat landscape.

5. Maintain and monitor.

Implement a range of supply chain security solutions that support automated, intelligent threat detection and continuous monitoring.

How RiskXchange can help

RiskXchange is one of the firms leading the fight against cybercrime, coming up with novel solutions to everyday problems experienced at the hands of hackers. We are a respected provider of cybersecurity ratings and can assess third-party risk factors to protect your business inside and out.

With full visibility over your eco-system's entire attack surface in near real-time, you can monitor and mitigate risks regularly to prevent unnecessary exposures. Our passive data collection methods are effective and have no impact on your network performance. Using data-driven insights to prevent breaches is the best way to reduce an attack surface and prevent cyberattacks.

About RiskXchange

RiskXchange empowers organisations with a powerful AI-assisted, automated, centralised 360-degree cybersecurity risk rating management approach. We generate objective and quantitative reporting on a company's cyber security risk and performance, which helps organisations with evolving business requirements conduct business securely in today's open and collaborative digital world.

RiskXchange is an information security technology company, which helps companies of all sizes fight the threat of cyber threats by providing instant risk ratings for any company across the globe. RiskXchange was founded and is led by recognised experts within the security industry, who have held leading roles in companies such as IBM Security.

Find out more here.