Insight Overview

masonadvisory

Part 3 of 3 - Safeguarding supply chains: the imperative of cybersecurity

In the last of this three-part article series, we look at how today's rapidly changing digital landscape, with its increased spotlight on global supply chains, has ushered in a new surge of cyber-attacks. We delve into the key cybersecurity concerns facing supply chains and outline effective strategies to address them.

Industry	Services
Logistics & Distribution	Cyber
Retail & FMCG	Service Management

Safeguarding supply chains: the imperative of cybersecurity

Recent events from Brexit, the COVID-19 pandemic, semiconductor shortage, the Suez Canal blockage and extreme geopolitical tensions have dominated news cycles. Unsurprisingly, this volatile landscape is keeping industry professionals awake at night. At the core of all these events has been the growing realisation of the importance of, and our dependence on, supply chains and the vulnerabilities within them that can be exploited. This intensified focus has seen cyber-attacks soar, with malicious actors specifically targeting various parts of the supply chains that are so crucial to all manner of industries and organisations – from port operations to software supply chains, transportation networks, and manufacturing facilities.

Successful cyber-attacks can have devastating consequences for organisations and the global economy. Addressing technology vulnerabilities and implementing heightened security measures are imperative to ensure the resilience of supply chains. We only have to consider a few high-profile examples to appreciate how devastating the consequences of such attacks can be:

- In 2022, Toyota was forced to close down 14 plants after a cyber-attack on one of its suppliers prevented the firm from procuring necessary production parts.
- The now notorious 2021 Colonial Pipeline attack infiltrated computer systems, encrypted their data, and rendered it inaccessible, causing widespread fuel shortages and panic buying.
- The 2021 SolarWinds attack, targeted the software supply chain, compromising updates and leading to unauthorised access to numerous networks, including government agencies and major corporations.
- In 2017, shipping giant Maersk experienced a crippling attack resulting from a compromised software update. Financial losses were reported as around $300 million. Chaotic scenes ensued, with reports of thousands of trucks turned away from terminals across the globe.

Such incidents are stark reminders of the vulnerabilities present in today's supply chain ecosystem. In Mason Advisory's experience, it is imperative for any business involved in, or dependent on, supply chains to act now to build their cyber resilience.

Did you know that, in response to heightened national cyber security concerns, an Executive Order issued in 2021 mandated the National Institute for Standards and Technology (NIST) in the USA to publish specific guidance on software supply chain security? The National Cyber Security Centre (NCSC) in the UK has also published guidance on effectively securing supply chains in response to the increased level of attacks. What's more, according to a Business Continuity Institute (BCI) report, cyber attacks and data breaches are perceived as the top threat to supply chains over the next five years.

So, what are the key trends organisations should be aware of?

Third-party and supplier risk

An alarming trend revealed by recent research, including The European Union Agency for Cybersecurity (ENISA), shows that attackers increasingly target under-resourced suppliers with weaker defences, exploiting these factors to then compromise larger organisations within the supply chain. They use suppliers to gain unauthorised access to the broader network and critical systems, leading to sensitive data breaches or significant service disruption to customers.

Meanwhile, as organisations embrace advanced technologies like AI and external cloud-based composable applications, they expand their 'digital' supply chain. However, with this comes additional partners and increasingly complex security risks.

Data breaches and theft

The exchange of sensitive data and intellectual property (IP) among stakeholders is crucial for efficiency across any supply chain. Cyber-attacks can target these valuable assets, aiming to steal confidential information or disrupt operations. Research by cybersecurity company BlueVoyant surveyed more than 2000 C-Suite leaders, finding that 82% of organisations suffered a data breach in the past 12 months due to cybersecurity weaknesses in the supply chain.

According to Computer Weekly, a cyber-attack on the systems of airline IT services specialist Sita, first reported in 2021, impacted Air India by exposing the personal data of 4.5 million people who flew on the airline.

More recently, in 2023, BA, Boots and the BBC were just some of the companies affected by the MOVEit attack. The software is used by Zellis, a payroll provider, and Microsoft has linked the attack to a known extortion group.

These attacks are not uncommon, although the size and scale of the impacts fluctuate from smaller repercussions to entire organisational failures. Organisations must ask themselves: "Do we have the cyber resilience in place to survive a malicious attack on our data?" If the answer is "no", then this is a business-critical vulnerability that must be addressed now.

Risks associated with Internet of Things (IoT)

IoT devices significantly expand vulnerabilities within the supply chain ecosystem. According to the EC Council, advanced manufacturing systems in factories may lack adequate security protections, and security may not be built into IoT architectures by design. Moreover, as automation continues to play an important role in improving IoT services, threat actors can leverage automation capabilities to launch more sophisticated attacks on IoT devices.

In 2020, Ripple20 flaws were discovered in a widely used IoT software library called Treck, allowing attackers to remotely execute code, gain unauthorised access, and potentially take control of un-secured IoT devices, including medical equipment, industrial systems, and more.

To mitigate and combat the adverse effects of this evolving threat landscape, organisations must proactively adopt technology-driven security measures to safeguard their enterprises and external supply chains.

There are, however, many stories where the supply chain organisation has successfully defended itself against attacks. This is no small feat! Success is largely achieved through a true understanding of vulnerabilities, consistent improvements, and shared knowledge across industry organisations. Mason Advisory helps many clients to tackle this complex area, by focusing efforts across these key considerations:

Managing the partner ecosystem

The NCSC has emphasised how crucial it is to know **who** your suppliers are, **what** they provide and **how** they provide it, to help you anticipate and manage the cyber security risks that may threaten your organisation.

Implementing rigorous due diligence processes, conducting regular audits, and establishing clear contractual obligations are all essential tactics here. Continuous monitoring and communication are also vital to ensure compliance and address any potential vulnerabilities promptly.

Implementing the right frameworks and controls

Embedding robust technology frameworks and controls enables organisations to effectively address security challenges by promoting proactive risk management, improving incident response capabilities, and ensuring compliance with industry standards and regulations.

When considering the right frameworks and controls to put in place, it is important to:

- Understand the risks and associated impact severity in the specific context of your organisation and industry, ensuring that the highest priorities are addressed.
- Align frameworks to your business objectives and ensure that security is universally considered as a business imperative, not just a technology one.
- Regularly evaluate and update. Security threats are constantly evolving, so the organisational response must do the same.

Operational resilience and business continuity reviews

These reviews provide the necessary expertise and approaches to assess, mitigate, and respond effectively to cyber threats within supply chains. By incorporating these measures, organisations strengthen their overall cybersecurity position by:

- Identifying potential entry points, helping to prioritise and strengthen necessary preventative steps.
- Measuring impacts by identifying critical functions and processes and the multitude of dependencies that exist within operations.
- Forming response plans to ensure that steps can be rapidly activated to manage threats and accelerate recovery.

Industry and organisational knowledge sharing

The importance of understanding your organisation, customers, and threat actors cannot be underplayed. If someone is targeting your supply chain, you can be sure that you will not be the only target. There is huge potential to collectively build cyber resilience by appropriately sharing cross-industry knowledge – for example, simulation activities or cyber security investment strategies. They key to this is ensuring that the entire supply chain is enabling the minimum standard your organisation requires, and that any additional insight generates appropriate action. It is also vital to invest the time to understand the different actors here, through specialist forum insights, data-analysis and understanding the 1% variation (the most comprehensive level of insight to drive the business).

As cyber threat actors and tactics become more sophisticated, and global supply chains become increasingly complex, organisations must take a proactive approach to enhancing resilience. The integrity and stability of the global economy depends on the end-to-end understanding of cybersecurity within internal and external supply chain partners. And, of course, business continuity depends on it too.

Start by reflecting on your ability to respond to and mitigate attacks, and by recognising that robust cybersecurity measures are an absolute necessity today, as well as tomorrow.

Remember, treating cybersecurity as a business issue, not just a technological concern, is vital in ensuring the long-term viability of your supply chain.

Author

Sammy Allanson
SME industry lead
contact@masonadvisory.com

Katie Stanton
SME industry lead
contact@masonadvisory.com

About Mason Advisory

Mason Advisory has offices in Manchester and London and employs over 100 staff, with plans to continue its expansion. We enable organisations to deliver value through digital & technology transformation, solving complex business challenges, and helping clients set strategy through the intelligent use of IT resources including architecture, cyber, operating model and organisational design, service management, and sourcing. We operate in sectors such as financial services and insurance, legal and law, government, health and social care, emergency services, retail, FMCG, logistics and distribution, transport, and not-for-profit.

Contact us

To get in touch, please email contact@masonadvisory.com or call +44 333 301 0093

www.masonadvisory.com

MANCHESTER
Landmark
St Peter's Square
1 Oxford Street
Manchester
M1 4PB

LONDON
Bush House
North West Wing
Aldwych
London
WC2B 4PJ