ISTARI Perspectives

Stopping the domino effect: Cyber resilience in the supply chain

Mark Malecki
Robert Hannigan

06 • 2022

Cyber attackers increasingly focus on penetrating complex supply chains. To build resilience, companies can start by getting three things right.

Supply chains have become one of the biggest fault lines for global business. Battered by geopolitical trade tensions, pandemics, inflation, and extreme weather events, any company can now, on average, expect operational disruptions to cost the loss of nearly half of a year's profits over the course of a decade, according to estimates from McKinsey.[1] Alongside these physical and financial vulnerabilities, cyber attacks are becoming an increasing threat to supply chains. Most large organisations rely on a network of third parties, and the forces of digitalisation have led to deep levels of interconnectivity. The benefits - efficiency, cost and visibility - are clear when times are good. But a cyber breach in any third party can quickly escalate in unpredictable ways.

The problem is not new; it has been nearly a decade since the infamous breach of Target via a refrigeration, heating and air conditioning service vendor.[2] But it is a problem that is growing. After all, this is an era in which a high-tech toilet is hackable.[3]

Recently ISTARI asked a room of chief information security officers (CISOs) about their experience with the potential domino effect that arises from supply chain cyber risk. Almost half had experienced a cyberattack that originated from their supply chain, and three quarters responded that their company's supply chain had been indirectly disrupted or impacted by a cyberattack on one of their suppliers.

The supply chain 'risk trinity'

Organisations need to defend themselves against three types of supply chain cyber risk. The first category is when a core supplier suffers its own cyberattack, preventing it from delivering essential products and services. The cyberattack on shipping giant Maersk in 2017 that disrupted global supply chains is one such example.[4]

The second occurs when an organisation suffers a breach due to a vulnerability in a supply chain partner, where an attacker moves laterally from a supplier's network into the organisation itself. That occurred in the cyberattack on software company Kaseya, where attackers gained access to over 1,000 companies, using Kaseya as a stepping stone.[5]

The third case is when an organisation suffers a breach because of a vulnerability embedded in a third-party product used in its own operation. The 2021 Log4j vulnerability, a weakness in an obscure but ubiquitous piece of software used to record computer system activity, is a case in point.[6]

What companies get wrong about supply chain risk

Organisations frequently struggle to implement effective supply chain cyber risk management programmes. One reason is governance; there tends not to be a single owner of an organisation's supply chain but multiple stakeholders across departments like procurement, operations, technology, finance, legal and security. Supply chain risk management does not have an obvious 'home'.

A second reason is visibility. Assessing risk requires asking difficult questions of current suppliers, which might create friction. Organisations might have limited visibility into legacy risks if past partners were onboarded without the kind of rigorous cyber assessment that today's more complex environment requires.

A third is scale and complexity. Larger organisations will typically have thousands of third and fourth parties in their ecosystem. Getting a handle on cyber risk is an intimidating task. Organisations could focus on their biggest suppliers, but that bears no relation to risk exposure. A very small provider of a critical, cyber-exposed piece of software might be far more deserving of scrutiny than a major equipment vendor. It is often the 'long tail' of smaller suppliers with modest budgets and less mature cybersecurity provisions that harbour the next attack.

Then come inadequate third-party risk management programmes; many enterprises have them, but they are often box-ticking exercises. Survey-based reviews, for instance, take a long time to gather and rely on honest responses. More comprehensive approaches, such as requiring evidence or periodical audits, are costly and slow. There may also be little follow-up in remediation to ensure an identified risk has been tackled. When we asked the

CISOs in our room, the majority admitted to only assessing third-party risk with suppliers once, when they were onboarded. This is problematic because cyber threats and network vulnerabilities are inherently dynamic and constantly evolving.

Finally: budget. Budgets often limit the scope of how many suppliers an organisation can assess. This means that some high-risk suppliers are omitted from the assessment because of financial constraints. The right approach should be to understand how many high-risk suppliers need reviewing and then set the appropriate budget.

Three steps to building cyber-resilient supply chains

To scale appropriately and keep pace with cyber risks across the categories identified (operational disruption, data breaches from a hacked supplier, or a direct vulnerability due to a third-party product), enterprises need to shift their approach.

1) *Set clear ownership.* It is essential to have an 'owner' of third-party cyber risk management programmes. Multiple stakeholders need to be consulted, but a single individual or team should be incentivised to assess and reduce supply chain risk - and then given the resources they need.

2) *Assess and prioritise suppliers.* Prioritise suppliers in terms of risk exposure based on factors like what products or services they provide, what data they have access to, what regulatory requirements apply and whether they have direct connectivity to systems. Identifying which suppliers are mission-critical may well lead to pursuing dual or multi-sourcing in order to reduce the risk of a significant operational disruption. Organisations must also conduct an internal discovery process to understand what third-party products exist in their environment, how they are composed and what aspects of the business they support.

3) *Fix the past – and anticipate the future.* Companies must examine whether current contractual clauses are fit for purpose for the risk or regulatory environment. They also need to seek partners to help them anticipate future risk by onboarding specialist continuous third-party risk management services. Those provide real-time risk identification and ensure third parties are not just notified of risks but supported with guidance on how to remediate them properly. Through in-house or outsourced capabilities, organisations can continuously monitor the external attack surface of all companies in their supply chain so they can act quickly when new vulnerabilities emerge.

After decades of deepening globalisation, supply chains are now one of the biggest risks organisations face in both the physical and digital domains. To operate successfully in the 21st-century cyber landscape, every company must properly assess the threats and then implement the right structures, policies and partnerships to ensure a proactive supply chain cyber-resilience strategy.

About the Authors

Mark Malecki is the Chief Technology Officer at ISTARI. He has worked in cybersecurity for over 20 years. Before joining ISTARI, Mark held the position of CISO at McKinsey, where he also supported client engagements relating to cybersecurity matters. He has also held the position of CISO at QuantumBlack, a McKinsey owned company, and at Dunnhumby, running their global security programme. Mark graduated from the University of Royal Holloway with a Masters in Secure Electronic Commerce and a BSc in Psychology.

Robert Hannigan is the Chairman of International Business at BlueVoyant and an advisor to a number of governments and international companies. He was a British civil servant who previously served as the director of the signals intelligence and cryptography agency, the Government Communications Headquarters (GCHQ), and established the UK's National Cyber Security Centre (NCSC). Since 2021, he is the Warden of Wadham College, Oxford University.

References

[1] Alicke, K., Luchtenberg, D. Supply-chain resilience: Is there a holy grail? McKinsey. https://www.mckinsey.com/business-functions/operations/our-insights/supply-chain-resilience-is-there-a-holy-grail

[2] Srinivasan, S., Paine, L., & Goyal, N. (2019). Cyber breach at Target. Harvard Business School Case Studies. https://www.hbs.edu/faculty/Pages/item.aspx?num=51339

[3] Quigley, J.T. (2013). Cyber-Attack in the Bathroom: Japanese Toilet Can Be Hacked. The Diplomat. https://thediplomat.com/2013/08/cyber-attack-in-the-bathroom-japanese-toilet-can-be-hacked/

[4] Greenberg, A. (2019). The untold story of NotPetya, the most devastating cyberattack in history. Wired.com. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

[5] Newman, L.H. (2021). How REvil Ransomware Took Out Thousands of Business at Once. Wired.com. https://www.wired.com/story/revil-ransomware-supply-chain-technique/

[6] Newman, L.H. (2021). The Log4J Vulnerability Will Haunt the Internet for Years. Wired.com. https://www.wired.com/story/log4j-log4shell/