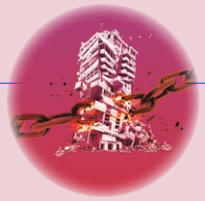

TOKIO MARINE HCC

The invisible risk: cyber security in the supply chain

The digital supply chain has become one of the most critical risk vectors for organisations. A single compromised link can trigger catastrophic consequences on a global scale, affecting thousands of companies through cascading effects. At Tokio Marine HCC, as an insurance company specialising in cyber security, we identify these incidents as systemic threats with the potential to generate high-impact cumulative losses. This article analyses the causes, propagation dynamics and key recommendations to strengthen supply chain security, highlighting the urgency to act before the next major incident.

ISAAC GUASCH

In an increasingly interconnected world, organisations no longer face cyber threats alone. To a large extent, their security depends on the robustness and reliability of their digital ecosystem: software vendors, cloud platforms, integrators, managed services and third parties that are part of their supply chain.

The problem is that these links are often the weakest point. The SolarWinds attack in 2020, the Kaseya incident in 2021 or, more recently, the CrowdStrike software update flaw in 2024 are emblematic examples of how a single breach can quickly escalate and affect thousands of organisations worldwide. These events not only cause operational disruptions, but also massive financial losses, reputational damage, legal consequences and, in some cases, can lead to physical consequences for individuals.

Attackers are very well aware of this cascading effect. It must be understood that cybercriminal groups are structured and operate like any other organisation, and that their sole purpose is to make money, as profitably as possible. This ecosystem of interconnectedness between parties provides them with a dream scenario: optimising their operations and efforts by attacking one victim that can compromise thousands of other victims at the same time. For them, it is a masterstroke.

From an insurance perspective, at Tokio Marine HCC, we classify such scenarios as accumulation of risk, or systemic risk. Unlike an isolated cyber incident, which impacts a single entity, a supply chain failure can unleash a chain reaction with exponential consequences. For an insurer, this represents one of the most complex scenarios to model and mitigate, as a single vector can simultaneously trigger multiple policies across different sectors and geographies, resulting in multi-million-dollar payouts.

Moreover, the challenge of assessing these scenarios is compounded by opacity in third-party visibility. Many organisations do not have a clear inventory of their critical suppliers and second or third tier dependencies. This "iceberg effect" leaves the organisation exposed to unknown vulnerabilities, which are impossible to protect if not identified in advance.

Proactive third-party risk management strategy

It is therefore imperative that security managers adopt a proactive third-party risk management strategy. Some key recommendations include:

- Assess and rank suppliers according to their criticality and risk exposure.
- Include cybersecurity clauses in contracts, such as incident reporting and regular security testing.
- Require transparency in security practices and encourage audits or certifications where possible.
- Continuously monitor the supplier ecosystem, including reputational analysis and changes to the attack surface.
- Encourage collaboration between IT, legal and procurement to integrate security into the supplier lifecycle.

In conclusion, cyber security is no longer just an internal issue, but a collective exercise in trust, verification and resilience. Faced with an increasingly sophisticated threat landscape, investing in supply chain security is not optional: it is a strategic necessity. For insurers like Tokio Marine HCC, understanding and anticipating these types of risks will be key to protecting our clients in a future where interdependence is the only certainty. ■

ISAAC GUASCH
Cyber Security Leader
TOKIO MARINE HCC

*Published in Spanish in **Revista SIC** #165 on June 4th 2025*