Marsh

Building Resilience Within Digital Supply Chains

Artificial intelligence, the Internet of Things, edge computing. Technology is continually evolving, creating a range of new capabilities for people and businesses and revolutionising the way we get products and services from one place to another.

Organisations around the world are investing heavily in technologies that turn linear supply chains into more efficient integrated digital supply networks. Retailers, for example, are using advanced algorithms to anticipate product demand and creating digitally enhanced experiences in stores to better serve customers. Smart factories are using technology — such as digital thread-enabled product design, collaborative robot (cobot) supported assembly, and sensor and AI-driven predictive maintenance — to increase the efficiency of the entire manufacturing process.

The complexity of the technical environment makes it increasingly difficult for business leaders to fully understand the risk to their organisation. Some organisations have a good grasp of digital supply chain vulnerabilities linked to the software and technology vendors that supply digital tools and are taking actions to address associated risks in selecting and monitoring vendors.

However, as organisations modernise and digitise their processes, they are often digitising physical assets and processes that were not understood as digital, introducing hardware and software without a full understanding of the associated exposure to cyber risk.

Organisational silos lead to risk blind spots

The additional complexity brought about by increased digitisation, together with a fast-evolving threat landscape, is making organisations increasingly vulnerable to costly cyber-attacks. As risks evolve, organisations may require new mitigation strategies. However, many businesses are still struggling to understand their own multifaceted digital supply chains, not to mention the myriad vendor relationships that support their operations and also contribute to increased complexity.

Despite their essential nature, supply chains — including today's digitally centric ones — are still largely managed within functional silos. For example:

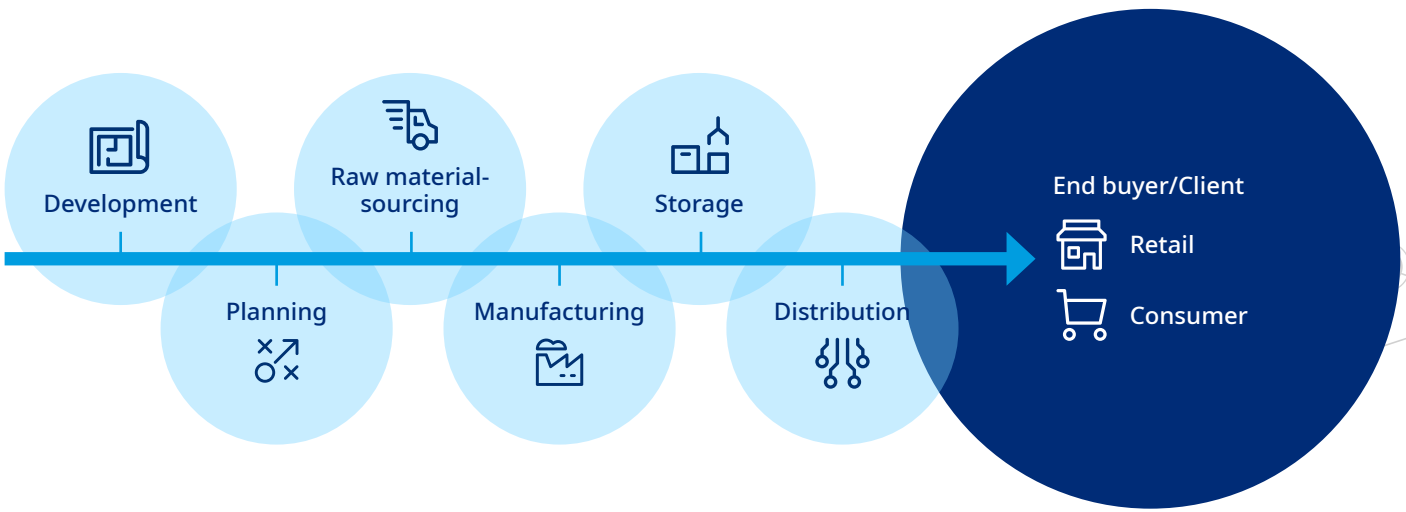
- Information technology (IT) and operational technology (OT) have historically been managed by different departments, and some organisations may still operate in silos.
  But as more operational devices are connected to the internet, they are becoming prone to cyber threats and require increased protection.
- Many digitisation efforts, such as manufacturing or supply chain planning, are run within functional departments. Disparate implementation teams may lack full visibility into end points and systems that are connected, leading to gaps in security protocol effectiveness.
- As the digital transformation accelerates and new cyber threats emerge, security and operations teams are challenged to manage alerts across thousands of devices and keep pace with communicating updates and managing new vulnerabilities.

These organisational blind spots can lead to considerable exposures due to a lack of understanding of risks that exist outside of each department's purview.

Expanded supply chains, expanded risks

Although risk managers tend to have more visibility across the organisation, this is often not deep enough to fully identify and understand their potential supply chain risks. Changes and enhancements to the digital supply chain are frequently carried out without fully understanding how they can affect overall risk, and thus without proper risk mitigation measures.

As supply chains become more digitised and therefore more connected, new risks emerge. But fully understanding digital supply chain risk is rarely a simple process. Not only does the constantly expanding attack surface lead to new risks, but malicious cyber actors are continuously evolving their attack methods and looking for new threat vectors. In addition, new interdependencies across the surface area of the digital supply chain create vulnerabilities that can hamper transformation.



Addressing digital supply chain risks

The actions needed to identify and mitigate supply chain risks seem reasonably simple, but in fact require a strong cross-organisational dialogue and collaboration and a robust process to evaluate and measure risk in financial terms.

Incorporating complex technologies and innovative tools has always been a challenge; incorporating multiple technologies — required for effective digital supply chains — is even harder. Manufacturers, in particular, have long struggled with integrating new technology with legacy systems that lack connectivity and trap information.

Success often requires a dedicated team that has visibility across the organisation and is able to assess the dynamic cyber threat landscape associated with using new technologies, both independently and together. This team, often in collaboration with external specialists, needs to anticipate the challenges with the selection of each technology, the integration progress, and upkeep of all systems to ensure that no new vulnerabilities emerge.

This is not a one-and-done process. As technology continues to evolve and proliferate, the risk will outpace the knowledge and experience of many frontline workers. The dedicated team will need to continuously monitor new risks and evaluate the risk profile, then apply the necessary security controls.

Risk professionals have a key role

As supply chains become more complex and bad actors continue to hone their malicious strategies, it becomes even more difficult to identify threats and to quantify them. At the same time, there is a greater recognition for organisations to take a forward-thinking approach to mitigating risks, driving preparedness, and building resilience.

Tackling the new — and legacy — challenges brought by more connected supply chains requires an enterprise-wide lens that allows for a complete understanding of the technology ecosystem and a full evaluation of interconnected risks.

Risk managers will have a central role in helping organisations identify, quantify, mitigate, and respond to the risks within their supply chains. Risk professionals will need to have a clear understanding of the supply chain landscape and the threat vectors to be better able to identify emerging risks. Another crucial step is to carry out robust stress testing for a variety of scenarios to understand potential risk exposure and financial implications.

The overall complexity of digital supply chains make it increasingly difficult to know where to look to identify risk, underscoring the importance that risk professionals have visibility across the entire organisation.

Finally, cross-organisation collaboration will be crucial to understanding and tackling new risks. Risk professionals need a seat at the decision-making table with key stakeholders to drive agility and design risk management processes that improve resilience.

Marsh

CONTACT US

For more information about Cyber Risk and how Marsh can support your business, please contact your Marsh representative.

Kelly Butler
Cyber Leader – Pacific
+61 3 9603 2194
kelly.butler@marsh.com

About Marsh

Marsh is the world's leading insurance broker and risk advisor. With around 40,000 colleagues operating in more than 130 countries, Marsh serves commercial and individual clients with data-driven risk solutions and advisory services. Marsh is a business of Marsh McLennan (NYSE: MMC), the world's leading professional services firm in the areas of risk, strategy and people. With annual revenue over $18 billion, Marsh McLennan helps clients navigate an increasingly dynamic and complex environment through four market-leading businesses: Marsh, Guy Carpenter, Mercer and Oliver Wyman. Follow Marsh on Twitter @MarshGlobal; LinkedIn; Facebook; and YouTube, or subscribe to BRINK.