Global Supply Chains and Cyber Security: Specialists are meeting Current Challenges with Modern IT Infrastructure

Published in a similar form in magazine 'dispo', Austria's leading trade magazine for logistics, on 28 July 2025

Authors:

- *Stefan Riese, Department Manager Customer Service, q.beyond logineer GmbH*
- *Felix Wagner, Supply Chain Consultant, q.beyond logineer GmbH*

Global logistics companies are currently facing enormous challenges. Trade route and supply chain networks are at risk. Cyber attacks are becoming increasingly likely. Individual stop-gap measures are not enough to future-proof organisations. The key requirement is an integrated, resilient IT infrastructure.

Under threat: Supply chains, the heart of logistics

Supply bottlenecks, long response times, unstable partnerships, disruptions or operational failures: supply chain complexity is constantly increasing. Root causes are raw material shortages, ongoing and expanding geopolitical tensions and increasing regulatory pressure. Logistics companies that rely on traditional, rigid approaches are struggling to keep pace with these ever-accelerating developments.

The consequences of delayed shipments or congested ports impact not only individual links in the chain but have a systemic effect. A delayed container can bring entire production lines to a standstill. Differing regulatory requirements between countries hamper the smooth flow of goods, while exchange rate fluctuations or sudden export bans create additional uncertainty. These factors can be compounded by environmental factors such as water shortages, resulting in reduced capacity, as in the case of the Panama Canal. If, in the face of such varied uncertainties, supply chain management lacks flexibility and transparency, competitive disadvantages arise.

Digitalisation – between light and shadow

High expectations of adaptability, response speed, transparency and efficiency prompt many managers to turn to digitalisation – and with good reason. Digital platforms for transport management are becoming a key control tool, bringing together transport data, material flows and communication processes in a single system. This creates an interconnected depiction of reality that both provides information and enables, real-time response. Companies benefit from more accurate forecasts, intelligent route planning and automated communication – for example, with partners, freight forwarders or customs authorities. Bottlenecks can be identified early on, alternatives can be more quickly examined and more targeted responses can be initiated.

Here a word of caution: If implemented too hastily and without careful consideration, digitalisation significant-ly increases vuerability vis-a-vis cybercriminals. In the context of globally networked supply chains, the security of digital processes must therefore be a top priority – as also reflected in guidelines and legislation. In order to establish a stable and resilient digital security strategy, logistics companies must comply, among other things, with the EU's NIS2 directive. This requires critical infrastructure operators to continuously assess potential risks, implement appropriate cyber security measures and ensure that partners and service providers also comply with security standards.

Laying the foundations – with resilient IT infrastructure

Those opting for various individual measures will usually miss the goal of achieving secure and efficient supply chain management. True cyber security and resilient supply chains depend on an integrated concept – or, more precisely, on the underlying IT infrastruc-ture. Whether it's real-time data flow, access from locations around the world or the uninterrupted operation of cloud-based applications – this can only be achieved if the digital basis is stable and grows with the business. Companies that take business continuity seriously do not view infrastructure as an afterthought, but as an integral part of their strategy.

Basically, their individual infrastructure must be able to keep pace globally. Cloud-based systems, uniform interfaces and secure, scalable IT structures ensure that all participants – regardless of location or end device – have access to the same, real-time data. Thus, digitalisation is not an isolated measure but the structural foundation of resilient supply networks.

Interconnected work thanks to digital workspace

One element that is indispensable in any global logistics company is the digital workplace. It offers not only tools, but also structures that enable remote working, process reliability, data sovereignty and compliance. From secure authenticcation to role-based access to systems and documents, a digital workspace must be created that is available, stable and protected at all times. With it, managers supply the basic

prerequisite for a resilient and highly secure logistics network. For a business with international locations, an efficient IT infrastructure in conjunction with digital workspace is therefore indispensable. However, it is important not to opt for standard solutions. Concepts that take individual requirements into account are distinctly preferable. This is more reliably realized with IT experts who also have industry-specific know-how – as is the case with the team at q.beyond logineer GmbH. In making their selection, logistics companies should keep five advantages in mind:

1. Are solutions scalable, enabling a response to current developments?
2. Does the program offer planning reliability and cost control?
3. Can a high system availability be guaranteed?
4. Can IT systems and digital workspaces be used worldwide?
5. Is 24/7 support available if necessary?

Farsighted Logistics

Logistics companies are currently facing a huge variety of challenges – above all, the move towards resilient supply chains and maximum cyber security. Companies often resort to individual software solutions without keeping the big picture in mind. However, modern software solutions can only deliver their full potential if the underlying infrastructure is resilient. Without it, any digital transformation remains a fragile construct. That is why it is worth ensuring a stable IT infrastructure first, so that cyber security and supply chain management can subsequently be implemented efficiently.

***Stefan Riese** has been supporting q.beyond logineer GmbH as Department Manager Customer Service since 2021. Thanks to his many years of experience, he knows which training courses promote cyber security awareness in different logistics companies.*

***Felix Wagner** joined q.beyond logineer GmbH in October at its new location in Charlotte, North Carolina. During his time as a Supply Chain Consultant, he has worked on numerous projects addressing the challenges of the logistics industry with regard to the supply chain and always finds the right solutions for customers.*

Do you have any questions for logineer? Or would you like a consultation?

Write to us and tell us about your requirements if you are looking for a committed partner to help you tackle the requirements of the future with digitalisation. We are ready for the challenge. Please contact us!
https://www.logineer.com/en/contact