Freight Forwarders Are Buying More Than Software. They Are Entrusting Control.

By Amit Maheshwari, Founder & CEO, Softlink Global

Technology buying decisions in freight forwarding have changed.

Forwarders are no longer comparing only features, pricing, implementation timelines or basic system capability. The conversation now includes automation, integrations, cloud access, AI capabilities, customer portals, ecosystem connectivity and the ability to support increasingly digital freight operations.

That shift is necessary. But it also changes the risk a forwarder accepts when choosing a technology platform.

A modern freight platform is no longer sitting at the edge of the business. It sits at the centre of operations. It can hold shipment records, customer information, commercial documents, freight rates, customs data, financial transactions, invoices, credit exposure, approvals and years of operational history.

It also connects employees, customers, overseas agents, carriers, customs partners, banks, finance teams and external systems across multiple locations.

In practical terms, the system is carrying the working memory of the business.

That is why security should no longer be treated as a technical checklist at the end of a software evaluation. It has to be part of the platform decision from the beginning.

A cyber incident in freight is not simply an IT disruption. It can affect live shipments, delay documentation, expose commercial information, interrupt billing, weaken customer confidence and create financial and reputational damage. When hundreds or thousands of shipments and transactions move through a platform every day, even temporary loss of access or trust can put pressure on operations, finance and customer service at the same time.

The issue is becoming more important as cloud platforms, APIs, automation and connected logistics ecosystems become the norm. A forwarder's digital environment now extends well beyond its own organisation. Customers, agents, carriers, customs platforms, finance systems and external applications all touch the operating environment in some form.

That means the security standard of a technology provider becomes part of the forwarder's own risk profile.

This should change the questions forwarders ask during technology evaluation.

How is data stored and encrypted?

How is user access governed, reviewed and removed?

Can sensitive actions be controlled through roles and permissions?

Is multi-factor authentication supported?

How are vulnerabilities, patches and platform updates managed?

What safeguards exist around APIs and third-party integrations?

Who, including the technology provider and its subcontractors, can access customer data, and under what controls?

If AI is used, is customer data used to train models, and how is that data isolated and governed?

How resilient is the platform when freight operations depend on it every day?

What backup, recovery and continuity measures exist if access is disrupted?

These are not back-office IT questions. They are business continuity questions.

Security is still a shared responsibility. Forwarders must maintain discipline around passwords, permissions, employee awareness, access reviews and user behaviour. But internal discipline works only when the platform itself is built with strong controls.

The same applies to AI. Freight platforms are beginning to use AI capabilities to read documents, support users, automate decisions and analyse operational data. That can create real value, but it also introduces a new question: what happens to the data that is being processed? Forwarders should know whether their data is retained, reused, shared with external model providers or used for training. They should also understand what controls exist to prevent one customer's information from becoming visible to another.

The responsibility of the technology provider therefore goes beyond keeping servers available. It includes protecting access, limiting exposure, managing integrations carefully, maintaining recovery capability and being clear about how customer data is handled.

"When a freight forwarder selects a technology platform, it is not simply choosing software. It is entrusting years of shipment history, customer information, financial data and commercial intelligence to that provider. Protecting that information is therefore not another software feature. It is one of the basic responsibilities of the technology partner."

Amit Maheshwari, Founder & CEO, Softlink Global

For forwarders, the technology decision is therefore changing.

It is no longer enough to ask what a platform can automate, how quickly it can be implemented or what AI capabilities it offers. They also need to understand who can access their data, how that access is controlled, what happens when systems fail,

how integrations are protected and what responsibility the technology provider accepts for protecting the environment.

As freight operations become more digital, the technology provider increasingly becomes part of the forwarder’s own risk chain.

The system does not just hold data.

It holds control.