ZEEBUSINESS

Data security is paramount for a thriving logistics industry amidst digitisation and automation, say experts

Data security plays a key role in preserving the confidentiality, integrity, and availability of data while ensuring compliance with legal and ethical standards.

The migration from traditional to digital logistics has also a role to play in the rapid growth of the industry.

In an era where technological proliferation is the new norm, with digitisation and automation leading the way, concerns surrounding data security have taken centre stage. The protection of customer data from unauthorised access, manipulation, or destruction is critical to seamless operations across multiple industries, particularly those heavily dependent on data such as finance, healthcare, education, and notably, logistics. Data security plays a key role in preserving the confidentiality, integrity, and availability of data while ensuring compliance with legal and ethical standards.

The logistics industry, much like other sectors, has been at the forefront of adopting cutting-edge technologies. As per predictions by the World Economic Forum, digitalization holds the potential to spawn approximately $1.5 trillion in business opportunities for logistics players by 2025. This exponential growth is largely attributed to the industry's enthusiastic adoption of innovative technologies. Despite the numerous advantages, including efficiency, productivity, accuracy, speed, safety, and sustainability that come with digitisation and automation, these technologies also present a considerable challenge—data security.

According to Vishal Salvi, CEO of Quick Heal data drives efficiency and innovation but also exposes us to cyber threats if not secured and classified properly.

“Logistics industry deals with massive amounts of personal and critical data. This data drives efficiency and innovation but also exposes us to cyber threats if not secured and classified properly. The DPDP (Digital Personal Data Protection) Act emphasises data security and classification's importance and compliance for all data fiduciaries. Classification plays a crucial role in data privacy and protection for businesses operating in the digital landscape. By categorising data based on its sensitivity and criticality, organizations can implement targeted security measures, comply with regulations, and effectively manage data throughout its lifecycle," Salvi added.

The migration from traditional to digital logistics has also a role to play in the rapid growth of the industry. The flip side, however, is that the surge in digital transformation and automation has turned the logistics industry into a prime target for cybercrime, resulting in significant cybersecurity risks. Also, data security in logistics entails the implementation of measures and practices to safeguard sensitive information and data intrinsic to the industry, including data related to shipments, inventory, customer details, financial transactions, supplier information, and other crucial logistics data. As the penetration of digital solutions continues to expand, the logistics industry encounters various data security challenges. "As the logistics industry continues to experience rapid growth and global competitiveness, the importance of data security cannot be overstated. In a world where the movement of goods relies heavily on digital connectivity, the integrity of our networks is paramount. It's the assurance that data flows seamlessly, operations remain efficient, and our supply chains remain robust, no matter the distance. Network security isn't just a component; it's the very framework that upholds our global logistics competence," Udit Mehrotra, MD and CEO, Spectra, said. According to Zaiba Sarang, Co-founder of iThink Logistics, logistics companies must establish a dedicated privacy team to safeguard the personal information they handle.

Personal data, including age, location, purchase history, spending habits, and other sensitive information, can easily be exploited by third-party data brokers to construct detailed digital profiles, which they then sell to other entities. Logistics companies must establish a dedicated privacy team to safeguard the personal information they handle. This team should ensure strict compliance with regulations such as GDPR, SOC2, and other pertinent international standards," Sarang added.

Enhancing data security in the logistics industry can be achieved by bolstering domestic players in the industry. Indian logistics firms, being subject to Indian jurisdiction, are inherently more secure as they abide by Indian laws and regulations designed to protect data security. This could minimize the risk of foreign interference, strengthen control over data processing and storage, improve compliance with local laws and regulations, foster local innovation and expertise, and advocate for national interest and sovereignty.