Navigating Digital Revolution: Why Data Security Is Paramount For A Thriving Logistics Industry

The logistics industry, much like other sectors, has been at the forefront of adopting cutting-edge technologies.

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, digitalisation 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.

Charting Digital Transformation In Logistics

The migration from traditional to digital logistics has enabled the creation of a circular supply chain that optimises costs, raw materials, and transport management. Innovations powered by machineries, such

as electro-mobility, high-speed rail systems, and last-mile optimisation, paired with IoT-enabled operations like warehouse automation, intelligent transportation systems, predictive maintenance, drone supervision, blockchain solutions, and artificial intelligence applications, are transforming the industry, thereby augmenting efficiency and adaptability to market demands.

Data has ascended to become the cornerstone of the logistics industry, driving the optimisation of processes, resources, costs, quality, and customer satisfaction. A multitude of sources — sensors, GPS, RFID, barcode scanners, cameras, and mobile devices — enable data collection. Further, an array of tools like artificial intelligence (AI), machine learning (ML), big data analytics, cloud computing, and blockchain facilitate data analysis. 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.

Traditional IT environments integrating with previously unconnected OT (Operational Technology) systems and expanding connected endpoints through IoT significantly magnify the security risks for consumers and businesses. The presence of a multitude of stakeholders and third-party vendors in the logistics chain only escalates the sector's susceptibility. Many companies presently lack a comprehensive strategy to mitigate the risks arising from the advantages of digitalisation. A recent PwC survey disclosed that 38% of logistics companies are wrestling with significant unresolved concerns about data privacy and security. The circumstances necessitate a robust data security infrastructure, specifically for the logistics industry.

Navigating Data Security Challenges And Imperatives In Logistics

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.

One critical concern is the operation of foreign automation technology providers such as Chinese firms in India. There is increasing anxiety over how the data collected from Indian users may be used once it reaches the servers in the origin countries of these companies, given the absence of a structured method of governing its usage. The use of Chinese machinery in logistics automation systems poses a high risk of data leakage due to the potential existence of built-in backdoors or vulnerabilities that can be exploited by malicious actors, including state-sponsored hackers.

During our conversation with industry stakeholders about “the critical role of data security in enabling a thriving logistics sector amid digitisation and automation," they expressed their perspectives and insights on the matter.

As per one of the spokespersons of a large logistics firm, “Data security remains our topmost concern when utilising foreign automation technology, particularly from countries like China. There is always a potential threat of data leakage due to unknown built-in backdoors or vulnerabilities in these systems. This not only puts our operational integrity at risk but could also undermine the trust of our customers and stakeholders.”

Vishal Salvi, CEO of Quick Heal said, “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 Act emphasises data security and classification's importance and its 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, organisations can implement targeted security measures, comply with regulations, and effectively manage data throughout its lifecycle. SEQRITE's Hawkk suite plays a pivotal role in helping enterprises today across sectors to strengthen their cybersecurity posture".
"Through intelligent scanning and data classification, SEQRITE's intuitive data privacy management solution, Hawkk Scan empowers enterprises to discover, categorise, and identify sensitive information scattered throughout their digital resources. It also helps manage subject rights requests to ensure total compliance with national and international data privacy regulations to avoid heavy penalties. This tailored security approach ensures the safeguarding of valuable customer information and brand reputation in the era of logistics digitisation."

Ms. Zaiba Sarang, Co-founder of iThink Logistics added, "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".

Udit Mehrotra, MD and CEO, Spectra, said, "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."

Furthermore, Chinese law mandates all firms to "support, cooperate with, and collaborate in national intelligence work," meaning any data collected by Chinese firms or through Chinese technology could potentially be accessed by the Chinese government. In a tense geopolitical environment marked by ongoing tech wars among major economies, this constitutes a significant threat to the data security of logistics firms using Chinese machinery, potentially undermining the confidence of customers, partners, and stakeholders in the logistics industry.

According to Mordor Intelligence, the Indian freight and logistics market is anticipated to reach USD 406.23 billion by 2029, growing at a CAGR of 6.46 per cent. Data security can aid Indian logistics companies in capitalising on the opportunities presented by digitisation and automation while delivering value to their customers and stakeholders. In an interconnected global supply chain, the secure exchange, storage, and processing of data are indispensable for efficient logistics operations and maintaining the trust of customers, partners, and stakeholders. Robust data security, therefore, requires the implementation of encryption, access controls, firewalls, intrusion detection systems, regular data backups, and employee training on cybersecurity.

Boosting Data Security Via Domestic Players

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 minimise 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.

With the proposed Personal Data Protection Bill (PDPB), the government intends to regulate the collection and usage of user data by companies. However, until this bill is enacted, it is crucial to foster transparency and visibility, manage risks associated with people, processes, and technologies, identify gaps, and plan future steps accordingly. Recognising that data security is a continuous journey, it is essential to invest in cutting-edge technologies, conduct regular security audits, and promote a culture of cybersecurity awareness. In doing so, the personal data of logistics clientele can be safeguarded effectively.

In conclusion, the insights and wisdom of industry players in the logistics and data security space serve as a guiding beacon in our journey towards a secure and thriving logistics industry amidst digitisation and automation. It is clear that data security is paramount, and by embracing these insights, we can navigate the challenges and opportunities of the digital age while safeguarding the trust of our customers, partners, and stakeholders.