WSB Journal of Business and Finance
Year 2023, Vol. 57, No.1
eISSN 2657-4950

Assessment of Data Security Implementation in the Supply Chain Enterprises in Latvia

Ingūna Jurgelāne-Kaldava[a1], Agnese Batenko[b],

[a]Riga Technical University, Kalnciema street 6, Riga, LV-1048, Latvia
[b]Riga Technical University, Kalnciema street 6, Riga, LV-1048, Latvia

© 2023 Inguna Jurgelāne-Kaldava, Agnese Batenko. This is an open-access article distributed under the Creative Commons Attribution-NonCommercial-NoDerivs license (http://creativecommons.org/licenses/bync-nd/3.0/

DOI 10.2478/WSBJBF-2023-0003

Abstract

The importance of data security in the supply chain has increased in the last few years. The study identifies recent trends and shortcomings in data security, assessing enterprises operating in Latvia's transport and storage industry. The research aims to study and identify the current trends in data security in the Transport and Storage industry to develop recommendations for improving data security in the supply chain. The research focuses on studying data security in the supply chain in Latvia. The theoretical literature review was used to learn the main aspects of the supply chain concept and the data security measures applied. Statistical and content analysis shows the industry's primary data security trends and issues. The results of the research concluded that in Latvia, enterprises providing supply chain operations are focusing on something other than mandatory education about the data security of their employees; thus, they need to apply sophisticated measures to protect data through all supply chain processes.

Keywords: Data security, GDPR, Supply chain

1 Introduction

The importance of data security and protection has increased over the past two decades. More preventive data security measures are necessary to ensure the safety of the growing usage of ICT systems in different supply chain processes.

A supply chain is the process of creating and delivering a goods or service, starting from the procurement of raw materials and ending with the delivery of the item to the customer. It should be emphasized that the supply chain outlines every step of the production process, including the tasks carried out at each one, the information that is being communicated, the natural resources that are converted into valuable materials, the human resources, and other elements that go into the finished good or service (Dubey et al., 2020). A supply chain is linked together through physical flows, including information flows, thus allowing multiple persons involved in the organization of the supply chain to control the flow of materials and goods (Zhang et al., 2019).

Gurtu (Gurtu et al., 2015), in his research, emphasizes various supply chain concepts such as sustainable supply chains, green supply chains, environmental supply chains, and closed-loop supply chains. Ageron and Bentahar (Ageron & Bentahar, 2020) focus on a new era of supply chain management – a digital supply chain. They point

[1] Corresponding author. Tel.: +371 67089553; E-mail address: Inguna.Jurgelane-Kaldava@rtu.lv

out that the digital supply chain should improve information systems and use technologies to increase its integration, thus enhancing customer service and the organization's long-term viability.

Changes in customers' expectations related to the supply speed have increased the supply chain's importance in facilitating competitive advantage and customer satisfaction (Malkus & Wawak, 2015). Consequently, supply chain development leads to the necessity of integration of data security measures. During recent years, data commercialization in supply chains (Yu et al., 2023) has become a new business model to add value to both businesses and customers.

For over two decades, enterprises involved in ensuring supply chain functions have tried to adopt and integrate newer technologies to increase work capacity and customer satisfaction. Mahmood (Mahmood et al., 2020) agree that despite adopting and implementing enterprise resource planning (ERP) systems in organizations, these systems' success rate is questionable. For the areas impacted by the supply chain (Menon, 2019), like procurement, distribution of goods and services, and controlling stock, there is a critical requirement for a continuous flow of data inside and across functional units. If the information is collected and processed correctly, it increases overall customer satisfaction and decreases data protection risks in supply chains.

Another tool applied for applying technologies in supply chains is the customer relationships system (CMR). According to Buttle (Buttle & Maklan, 2004), CRM has been defined as one of the core business strategies that aims to automatize and integrate customer-related processes in business daily functions as well as internal and external processes. Guo (Guo, 2021) refers to a business strategy to pursue customer satisfaction and loyalty. The primary emphasis of using CRM systems to create customer-focused front-end tools based on e-commerce should be more prominent in terms of speed, accuracy, efficiency, and the needs of individual customers.

Increasing data leakage (Inman & Nikolova, 2017) shows that data protection in supply chain processes must be more robust for B2B and B2C customers. It highlights the necessity to increase measures in customers' personal data protection and the viability of educating entrepreneurs about acquiring, processing, and storing customer data.

General Data Protection Regulation (GDPR) is an EU law applied to control data collection, monitoring, storage, and usage in enterprises (Regulation (EU) 2016/679 of the European Parliament and of the Council, 2016). It states that one of the fundamental rights is the right to personal data protection, which has increased due to rapid technological development. The regulation entered into force on 24 May 2016 and has been applied in the European Union since 25 May 2018.

Data protection and information security measures should be applied through all supply chain processes. Transparency and traceability of each stage (Ravi et al., 2022) define the level of security achievable. In supply chain management, data leakage or fraud may happen during production, processing, packing, and transportation.

The study aims to study and identify the recent trends in data security in the Transport and Storage industry to develop recommendations for improving data security in the supply chain enterprises in Latvia.

Tasks:

1. To analyze theoretical aspects of data security and protection role in the transport and storage industry;
2. To collect and analyze statistical data about data security and protection in the transport and storage industry in Latvia;
3. To assess the main measures applied to ensure data security in the transport and storage industry in Latvia;
4. To develop a model of improvement of data security in the supply chains.

According to the NACE 2 classification, the supply chain is a part of the Transport and storage industry, which refers to the H industry; therefore, the data assessed belongs to the general sector if no detailed statistics are available yet.

When the research of the data security measures in the supply chain enterprises is examined, it is noted that a large part of the information and data is being found with a focus on the transport and storage industry in general, with little or no reference to supply chain enterprises. However, the importance of supply chain management, especially in navigating crises such as the COVID-19 pandemic (Craighead et al., 2020), is influenced by the strong link (Ghadge et al., 2019) between information technology, organizational, and supply chain security systems.

2 Materials and Methods

The research used general scientific research methods such as the monographic or descriptive method, analysis and synthesis method, literature analysis, and statistical data analysis. With the methods, the concept and importance of the supply chain and the leading software used in the supply chain enterprises in Latvia have been assessed. The share of the data security incidents, trends in using different software and systems, and the main data security measures applied by Latvian companies focusing on the supply chain have been examined.

The literature analysis was conducted to define the supply chain and historical developments using different software used in planning, implementing, and analyzing supply chain processes. The literature analysis focused on collecting information regarding the main threats in the data security processes and current legislation determining mandatory data security measures in Latvia. The preliminary search was conducted in the following

databases: EBSCO, Web of Science, Science Direct, and was based on the following keywords: data security, supply chain management, and data. Primary literature sources were selected based on the availability of full-text articles as well as on the aim of the research. The selection of statistical data was based on the general availability of the data related to the research topic in databases such as Eurostat and the National Statistical Office. The research is based on many data sources as topical data security trends have limited coverage in the official state or the European Union (EU) level statistical databases due to time delay in publishing. The research period is 2013-2022. The research methods applied in statistical data analysis include graphical and content analysis.

The assessment of the literature and statistical data allowed the authors to specify the article's previously mentioned aim and focus on the general evaluation of data security implementation trends in supply chain enterprises in Latvia. This research should be considered the first step for more detailed analysis.

3 Results and Discussion

Global trends in information systems security affect data security in the supply chain. Regional differences in the level of security of data and information systems depend on the level of development of the information technologies sector in a particular country.

The number of recorded crimes in the internet environment has increased in the European Union in past years. The offenses registered in Latvia from 2017-2021 have remained below average compared to other European Union countries. For example, according to the Eurostat (Eurostat, 2022a), in 2017, 2019, and 2020, the number of registered offenses reached 5, while in 2018 and 2021 – 18. In comparison, in 2021, the highest number of recorded crimes in the internet environment was registered in Turkey and France, with corresponding 1966 and 734 cases, but the least in Malta and Iceland – 2 points per country.

A similar situation could be observed by assessing the percentage of security incidents and consequences in industry in the European Union (see Figure 1). In 2022, the % of industry companies facing data security incidents in Latvia accounted for 7.1%, while in 2021, it was 10.4%. The most significant percentage of companies facing data security incidents was observed in Denmark –71.3%, and Malta at 42.1%, but the least in Bulgaria – 3.1% and Lithuania – 3.8 (Eurostat, 2023).



Fig. 1. Share of security incidents and consequences Transport and Storage industry in European Union in 2022, % (Eurostat, 2023)

According to the Central Statistics Bureau of Latvia (Official Statistics Portal of Latvia, 2022a), in 2022, 78.8% of Transport and storage industry employees had remote access to the enterprise's e-mail system, documents, applications, or software. On average, 77.6% of employees in Latvia have remote access to enterprise systems.

The number of enterprises in the Transport and storage industry using ERP systems for resource planning in the supply chain has increased from 7.1% in 2013 to 39.6% in 2021. Significant changes could be observed in customer data and information processing. Until 2015, the share of enterprises collecting customers' data for facilitating business activities and active selling and marketing purposes, but after the GDPR came into force, the percentage of the companies decreased to 15.5 % and 13.7%, respectively.

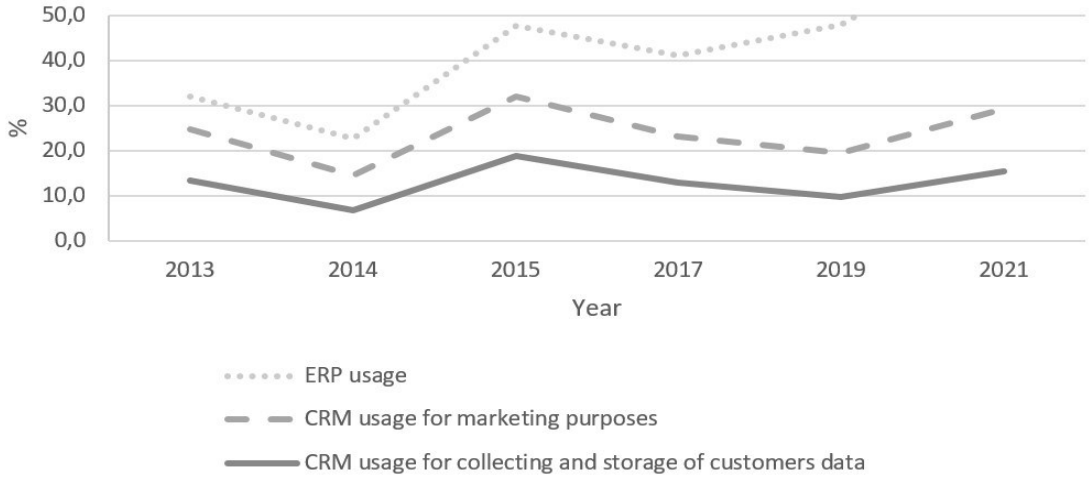

Fig. 2. Share of industry enterprises using ERP and CRM systems for resource planning and customer data processing in 2013-2021, % (Official Statistics Portal of Latvia, 2021a; Official Statistics Portal of Latvia, 2021b)

Global trends in information systems security affect data security in the supply chain. Regional differences in the level of security of data and information systems depend on the level of development of the information technologies sector in a particular country.

Table 1. Share of Transport and Storage industry enterprises that have sold goods or services via the internet or other computer networks in 2013-2021, % (Official Statistics Portal of Latvia, 2022b)

	2013	2014	2015	2016	2017	2018	2019	2020	2021
Total	6.6	4.3	5.1	7.2	5.3	8.1	6.6	6.1	6.7
Base growth rate	-	-34.8	-22.7	9.1	19.7	22.7	0.0	-7.6	1.5
Using Internet homepages or applications	3.5	3.9	5.1	5.8	5.3	6.1	5.9	4.0	4.4
In computer networks, using EDI messages	2.9	1.4	0.7	2.1	0.3	2.4	1.8	3.4	3.5

Information system security and supply chain data protection are closely related. Secure the enterprise's internal and external systems could improve data protection measures. On average, 86.9 % of enterprises in Latvia are using strong password authentification to protect information systems and customers' and employees' data. In turn, only 11.1% are using biometric data as a tool for user identification and authentication.

Information systems protection measures in the transport and storage sector are general and related to available standards in another industry. Strong password authentication was used by 8.4% of industry enterprises in 2019. However, the share of activities involved varies significantly – user identification and authentification using biometric methods were used by 13.9%, while encryption techniques for data, documents, and e-mails – by 25.2% (see Table 2).

Table 2. Share of applied data protection measures in 2019, % (Official Statistics Portal of Latvia, 2020).

Data protection measure	**Share, %**
Strong password authentication	88.4
Keeping the software up-to-date	66.2
Data backup to a separate location	55.1
Network access control	50.4
ICT security tests	27.6
Encryption techniques for data, documents, or e-mails	25.2
ICT risk assessment	21.8
VPN	19.1
Maintaining log files for analysis after security incidents	14.3
User identification and authentication via biometric methods	13.9

Trends show that the share of enterprises in the transport and storage industry that provide employees with information on ICT security requirements and questions related to data protection increases; however, the central claim is made from voluntary learning of the information related to data protection. For example, in 2019, only 11.7% of enterprises offered mandatory training, while in 2022 - 14.4%. In 2019, 56.3% of industry employees participated in voluntary activity, while in 2022 – 40.4% of employees.

It reflects the necessity in the industry for organized learning related to data protection, not only for information technology specialists but for other employees, too. On average, in 2019, 14.8% of enterprises offered training for their employees regarding data protection and information security, while in the Transport and storage industry, this number reached 12.6% of total enterprises.

To increase data security in Latvian supply chain enterprises, the authors propose implementing a simple framework for integrating data security measures in the supply chain (see Figure 3). This model consists of five stages and should be focused on weak areas in the current data gathering, processing, storage, or usage processes.

The first step focuses on mandatory training of the primary data security measures during onboarding and employment. During the second stage, data security measures described in Table 2 should be applied based on the complexity and size of the enterprise. The third and fourth stages are devoted to integrating these measures into the daily work of the enterprise as well as in the work with customers. During the final stage, "Implementation of the supply chain," all those measures are successfully applied, and the company can focus on their daily tasks (supply chain implementation) - planning, sourcing raw materials, manufacturing, delivery, and returns of goods.

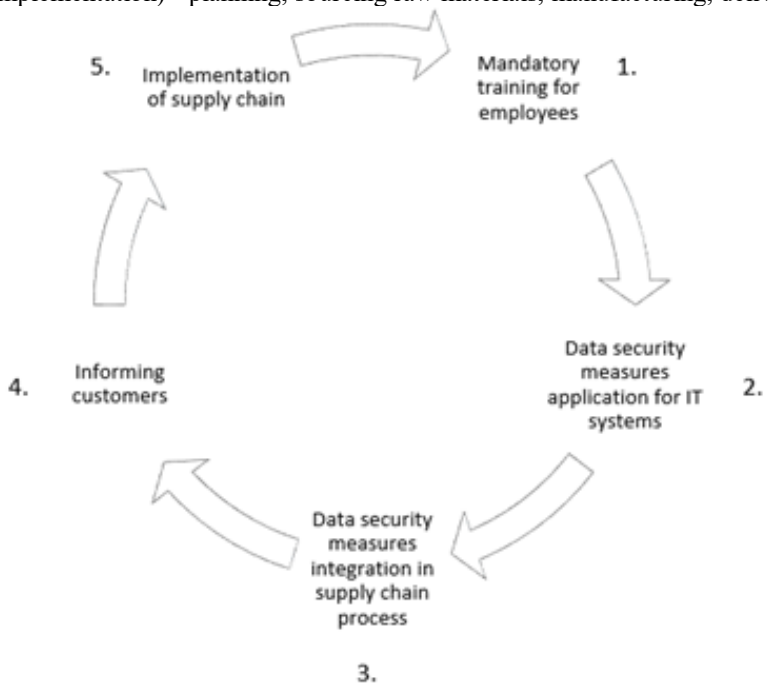

Fig. 3. Schematic framework of integrating data security measures in the supply chain

Targeted activities and resources allocated for strengthening data protection in the supply chain in the format proposed data protection model for integrating into the supply chain leads to reduced registered data leakage and higher customer satisfaction. In the transport and storage sector, all supply chain processes are necessary to organize mandatory training of employees about data safety during transportation or purchasing, for example. This refers to all operations of the supply chain. Data security measures should be integrated into general IT systems and all activities implemented in the supply chain.

4. Conclusions

The authors' main conclusions include several issues that should be addressed in the future. However, over the past ten years, the influence of technological development and the COVID-19 pandemic has increased the number of industry enterprises using ERP or CMR systems and the number of industry enterprises operating in an internet environment and selling their services online. It indicates the signs of the industrial revolution (İyigün & Görçün, 2022) in logistics and supply chain management. It is essential to apply data security measures as the topicality and importance of the Internet of Things (IoT), smart cities, enterprises' digital transformation, and the world's digital economy (Yang et al., 2020) are increasing yearly, showing future trends.

In this study, as the main one for identifying data security issues in Latvian enterprises related to supply chain management, the conceptual schematic framework for integrating the data security measures in the supply chain has been drawn. The current situation and the main threats to data security in the supply chain have been examined. At first, despite the overall number of recorded crimes on the internet increasing steadily in the European Union, the number of crimes registered in Latvia is below average compared to the European Union and, in 2021, reached 18 records. Similarly, security incidents in the Transport and Storage sector in the European Union show that, in

2022, 7.1% of Latvian companies have faced data security incidents, which is below average in the European Union. Businesses that are involved in supply chain management could be divided based on the level of already applied data security measures. The number of industry enterprises requiring mandatory acquisition of data security knowledge is relatively small. It indicates that data security risks may arise in any supply chain stage due to the need for more understanding of employees involved in supply chain coordination. It could mean either a positive tendency to apply data security measures in these enterprises or a lack of interest in crime commitment. The following studies should assess the reasons why supply chain enterprises are applying data security measures at an advanced level or there are no applications for them.

In line with these findings, a more detailed and justified model for applying data security measures in supply chain enterprises with a focus on weak areas could help strengthen data security through all supply chain processes.

In further studies, it could be recommended to cover the data security process in one specific stage of the supply chain to determine the possible scenarios or models for increasing the data security level, as this research could be classified as the first step in this process. It can be recommended to support future studies with field research.

References

Ageron, B., Bentahar, O., & Gunasekaran, A. (2020, July). Digital supply chain: challenges and future directions. In Supply Chain Forum: An International Journal (Vol. 21, No. 3, pp. 133-138). Taylor & Francis. https://doi.org/10.1080/16258312.2020.1816361

Buttle, F., & Maklan, S. (2015). Customer relationship management: concepts and technologies. Routledge.

Craighead, C. W., Ketchen Jr, D. J., & Darby, J. L. (2020). Pandemics and supply chain management research: Toward a theoretical toolbox. Decision Sciences, 51(4), 838-866.

Eurostat. (2023). Security incidents and consequences by NACE Rev.2 activity. Retrieved 13 July 2023, from https://ec.europa.eu/eurostat/databrowser/view/ISOC_CISCE_ICN2__custom_6866441/

Eurostat. (2022a). Recorded offenses by offence category - police data. Retrieved 13 July 2023, from https://ec.europa.eu/eurostat/databrowser/view/CRIM_OFF_CAT/default/table?lang=en

Dubey, S., Singh, R., Singh, S. P., Mishra, A., & Singh, N. V. (2020). A brief study of the value chain and supply chain. Agriculture Development and Economic Transformation in Global Scenario, 177-183.

European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ec (general data protection regulation) (2016). https://eur-lex.europa.eu/eli/reg/2016/679/oj

Ghadge, A., Weiß, M., Caldwell, N. D., & Wilding, R. (2019). Managing cyber risk in supply chains: A review and research agenda. Supply Chain Management: An International Journal, 25(2), 223-240.

Guo, F. (2021, March). Research on customer relationship management in an E-commerce environment. In IOP Conference Series: Earth and Environmental Science (Vol. 693, No. 1, p. 012072). IOP Publishing. https://doi.org/ doi:10.1088/1755-1315/693/1/012072

Gurtu, A., Cory, S., & Jaber, M.J. (2015). An analysis of keywords used in the literature on green supply chain management. Management Research Review, 38(2), 166-194. https://doi.org/10.1108/MRR-06-2013-0157

Inman, J.J., & Nikolova, H. (2017). Shopper-Facing Retail Technology: A Retailer Adoption Decision Framework Incorporating Shopper Attitudes and Privacy Concerns. Journal of Retailing, 93(1), 7-28. https://doi.org/10.1016/j.jretai.2016.12.006

İyigün, İ., & Görçün, Ö. F. (Eds.). (2022). Logistics 4.0 and Future of Supply Chains. Springer.

Mahmood, F., Khan, A. Z., & Bokhari, R. H. (2020). ERP issues and challenges: a research synthesis. Kybernetes, 49(3), 629-659. https://doi.org/10.1108/K-12-2018-0699

Małkus, T., & Wawak, S. (2015). Information security in logistics cooperation. Acta logistica, 2(1), 9-14. https://doi.org/10.22306/al.v2i1.32

Menon, S. (2019). Critical challenges in enterprise resource planning (ERP) implementation. International Journal of Business and Management, 14(7), 54-69. https://doi.org/10.5539/ijbm.v14n7p54

Official Statistics Portal of Latvia. (2022a). Enterprises whose employees have remote access to the enterprise's e-mail system, documents, applications, or software. Retrieved 13 July 2023, from https://data.stat.gov.lv/pxweb/en/OSP_PUB/START__IKT__DL__DLU/DLU111/

Official Statistics Portal of Latvia. (2022b). Enterprises that have sold goods or services via the Internet or other computer networks 2008 - 2021. Retrieved 13 July 2023, from https://data.stat.gov.lv/pxweb/en/OSP_PUB/START__IKT__EK__EKU/EKU020

Official Statistics Portal of Latvia. (2022c). Enterprises that provide any type of training to develop ICT related skills of the persons employed 2012 - 2021. Retrieved 13 July 2023, from https://data.stat.gov.lv/pxweb/en/OSP_PUB/START__IKT__EP__EPD/EPD030/

Official Statistics Portal of Latvia. (2021a). Use of enterprise resource planning (ERP) software in enterprises 2012-2021. Retrieved 13 July 2023, from https://data.stat.gov.lv/pxweb/en/OSP_PUB/START__IKT__DL__DLU/DLU080/

Official Statistics Portal of Latvia. (2021b). Activities carried out by enterprises that are using some IT solution to process information on clients (CRM) 2013-2021. Retrieved 13 July 2023, from https://data.stat.gov.lv/pxweb/en/OSP_PUB/START__IKT__DL__DLU/DLU090/

Official Statistics Portal of Latvia. (2020). ICT security measures in enterprises 2019. Retrieved 13 July 2023, from https://data.stat.gov.lv/pxweb/en/OSP_PUB/START__IKT__EP__EPD/EPD060/

Ravi, D., Ramachandran, S., Vignesh, R., Falmari, V., & Brindha, M. (2022). Privacy-preserving transparent supply chain management through Hyperledger Fabric. Blockchain: Research and Applications, 3(2), 100072. https://doi.org/10.1016/j.bcra.2022.100072

Yang, P., Xiong, N., & Ren, J. (2020). Data security and privacy protection for cloud storage: A survey. IEEE Access, 8, 131723-131740. 10.1109/ACCESS.2020.3009876

Yu, H., Zheng, S., & Wu, H. (2023). User Privacy Awareness, Incentive, and Data Supply Chain Pricing Strategy. Sustainability, 15(4), 3362. https://doi.org/10.3390/su15043362

Zhang, H., Nakamura, T., & Sakurai, K. (2019, August). Security and trust issues on the digital supply chain. In 2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech) (pp. 338-343). IEEE. https://doi.org/ 10.1109/DASC/PiCom/CBDCom/CyberSciTech.2019.00069