



Publisher

<http://jssidoi.org/esc/home>

DATA SECURITY RISKS AND THEIR PREVENTION: LATVIAN ENTERPRISES IN THE CONTEXT OF SELECTED COUNTRIES

Ingūna Jurgelāne-Kaldava¹, Agnese Batenko,² Anatolijs Krivins,³ Esat Durguti ⁴,
Kristina Garškaitė-Milvydienė ⁵

^{1,2} Riga Technical University, Riga, Latvia

³Daugavpils University, Daugavpils, Latvia

⁴University "Isa Boletini", Mitrovica, Kosovo

⁵Vilnius Gediminas Technical University (VILNIUS TECH), Lithuania

E-mails :¹ Inguna.Jurgelane-Kaldava@rtu.lv; ² Agnese.batenko@rtu.lv; ³ anatolijs.krivins@du.lv;
⁴ esat.durguti@umib.net; ⁵ kristina.garskaite-milvydiene@vilniustech

Received 20 February 2024; accepted 16 May 2024; published 30 June 2024

Abstract. An increasing number of organizations in Latvia are directing their efforts toward digitizing information and data storage. With the onset of the COVID–19 pandemic, there was an essential surge in the number of employees working remotely, eliminating the constraints of their physical workplace. Consequently, the challenges concerning data security within organizations have amplified. The main aim of this study is to explore and recognize the risks related to logistics data protection and subsequently formulate recommendations for mitigating or preventing logistics data security risks in Latvian enterprises. This research is centred on examining the prevailing data security trends in Latvia. An academic literature review was undertaken to gain insights into the core attributes and legislative measures governing data security in Latvia. Statistical and content analyses were employed to uncover deficiencies and risks in data security. The main results show that the data security and risk management measures in Latvian enterprises do not depend on the industry represented by the enterprise, thus applying the commonly used data security protection measures and risk management approaches. The research concluded that, in Latvia, the primary data security risks arise from internal and external threats.

Keywords: logistics; data security; ICT security measures; data security regulations; data privacy; business enterprises

Reference to this paper should be made as follows: Jurgelāne-Kaldava, I., Batenko, A., Krivins, A., Durguti, E., Garškaitė-Milvydienė, K. 2024. Data security risks and their prevention: Latvian enterprises in the context of selected countries. *Entrepreneurship and Sustainability Issues*, 11(4), 78-90. [http://doi.org/10.9770/jesi.2024.11.4\(5\)](http://doi.org/10.9770/jesi.2024.11.4(5))

JEL Classifications: O10, R49

Additional disciplines: law; sociology; information and communication; informatics

1. Introduction

The significance of data security and the application of preventive measures related to ensuring logistics data safety in enterprises has considerably increased over the past decade. The growth of digital solutions such as IoT, robotics, and big data in logistics automation (Navickas et al., 2022; Nica et al., 2023; Lincenyi et al., 2023; Shen & Zhang, 2024) raised people's concerns about the security of those technological advancements (Hick et al., 2024). Nowadays, the amount of processed logistics data has significantly increased (AlShaer et al., 2019) due to the use of sensors for tracking delivery or product maintenance, which has assisted in connecting humans, factories, shipments, and machines. Shameli-Sendi (2020) points out the necessity of defining enterprises' security needs, allowing the integration of preventive measures and risk assessment in everyday operations. It

should be emphasized that logistics data security should be assessed in terms of logistics operations, e-commerce (Ding & Zhao, 2021; Markos et al., 2023; Androniceanu & Georgescu, 2023), and national security (Nguyen et al., 2023).

Therefore, the study aims to study and identify risks associated with data protection to develop recommendations for preventing or reducing logistics data security risks in Latvian businesses. The main tasks undertaken in this regard were:

- To analyze theoretical aspects and the legal acts regulating data security.
- To gather and examine empirical information regarding data security (DS) and protection (DP).
- To evaluate the core measures and risks related to logistics DS in enterprises.
- To come up with recommendations for logistics DS risk reduction in enterprises.

The research begins by undertaking an academic overview of the literature that recognizes Latvia's key concepts and legal mechanisms regulating data security. Then, it turns to statistical and content analysis that reflects the challenges and issues encountered in logistics data protection. Moreover, the research delves into the various data security measures implemented by Latvian enterprises. This includes security measures like strong password authentication, software updates, and data backup, which are evaluated in the context of different categories of enterprises. Afterwards, the study identifies and analyzes the main measures and risks associated with data security in Latvian enterprises. It specifically focuses on internal and external threats and the implications of logistics data security risks on organizations. Based on the findings from the various analyses, the research develops recommendations for preventing or reducing logistics DS risks in Latvian enterprises. These recommendations aim to provide practical solutions for enhancing data security.

Data used in the study can only be obtained from official countries or European Union (hereinafter – EU) level statistical datasets due to publishing delays, which restricts data sources to those dealing with data security. The research period is from 2013 to 2022. This case study has assessed the main trends and risks associated with data security in enterprises in Latvia; situation analysis regarding another country and comparisons with other countries are included in the research.

2. Theoretical background

The problem of data security is actively discussed in entrepreneurship. Doss et al. (2022) raised concerns about excessive DS demand, while Qatawneh & Al-Okaily (2024) highlighted the importance of interconnectedness between technologies, operational efficiency, and system operations. Ali (2020) points out safety problems arising from the lack of data security measures and people's training and compliance problems. In contrast, Li et al. (2020) point out that data security risks should be divided into two categories: DS issues and application security matters, thus agreeing that the main concerns regarding DS arise from integrity, confidentiality, and privacy protection and communication.

In addition, Kennedy and Millard (2016) focus on data security as one of the main problems in enterprises and summarize the main benefits and challenges of laws related to data protection regulation. Therefore, data protection legislation in Latvia is divided into EU legislation and national laws. Three principal regulations regulate the data collection, storage, and usage industry in Latvia – General Data Protection Regulation 2016/679 (hereinafter – GDPR), The Data Protection Law Enforcement Directive 2016/680 as well as Personal Data Processing Law, which is the national law in data protection in Latvia:

- GDPR (REGULATION (EU) 2016/679, 2016) entered into force on 24 May 2016 and has been applied since 25 May 2018. This regulation was developed to reduce fragmentation in national systems and unnecessary administrative burdens by clarifying rules for companies and public bodies.
- Data Protection Law Enforcement Directive 2016/680 (DIRECTIVE (EU) 2016/680, 2016) entered into force on 5 May 2016 with the condition that EU countries had to transpose it into their national law. The directive secures the fundamental right of citizens to data protection when law enforcement bodies use personal data for law enforcement objectives. It aims to guarantee that the personal data of victims,

witnesses, or suspects of crime are appropriately secured and will facilitate cross-border collaboration in the fight against corruption and terrorism.

- Personal Data Processing Law (2018) entered force on 5 July 2018. As this is national law, it is designed to supplement the General Data Protection Regulation and The Data Protection Law Enforcement Directive. The objective of this law is to create legal prerequisites for setting up a system for the protection of personal data (hereinafter – the data) of a natural person at a national level by providing for the institutions necessary for such purpose, determining the competence and essential principles of operation thereof, as well as regulating the process of data protection officers and provisions of data processing and free movement.

The concept of the data and the risks are discussed in scientific literature. Patil et al. (2020) define the data as representing ideas or objects previously collected as characters, symbols, numbers, and pictures. In turn, the term "data security" is discussed by Naim et al. (2023), referring to it as the process of ensuring the safety of digital information. However, Patil et al. (2020) emphasize that data protection relies on confidentiality, authenticity, and integrity. Moreover, Gupta et al. (2021) focus on data assurance as the significant reason causing data security risks. Data security is the leading indicator for measuring the level of data privacy. In addition, Filippova et al. (2021) and Katina et al. (2023) defined risk factors that influence key performance indicators in an enterprise and affect the effectiveness of systems and processes.

As Kraska et al. (2019) stated, data may be treated in compliance with one of the six lawful instances: consent, agreement, legal obligation, lifeless interests, public interest, and legitimate interest. It confirms the content of the legal norms that obtaining approval or permission to process and store data is necessary.

In addition to the classification provided by Kraska et al. (2019), the EU has determined the requirements for systems that store data. Shastri et al. (2019) consider that these requirements are: 1) Controlled data storage and access to the storage system based on a legal basis, including access limitations; 2) Queries, in which access is defined and all data collected is associated with purpose; 3) System-wide erasure is based on data subject rights to erase data stored by the enterprise.

According to Subbalakshmi and Madhavi (2018), four significant risks associated with company IT data security are data security, privacy, reliability, and storage threats. Liu et al. (2016) focus on the increase in data usage and security and protection problems associated with big data and cloud data, as well as safety from intruders and controlling user accessibility in the CSPs. These two major and foremost requirements are of primary importance.

IT data security concerns are studied not exclusively by researchers but also by international auditing companies such as PwC or EY. For example, PwC (A Practical Guide to Risk Assessment, 2008) indicates that to prevent IT data security threats resulting from legal requirements and professional or self-regulatory obligations, several forms of risk assessments are frequently undertaken within enterprises. EY has addressed an equivalent evaluation in the information security study (EY Global Information Security Survey, 2020).

Contrary to Liu et al. (2016), the EY information security survey divides threats or risks by the person category – outsiders, neutral or unknown, and insiders. The report highlighted that “the increase in activist attackers, who this report shows were the second most common source of material or significant breaches, underlines how the cybersecurity function needs a much deeper understanding of its organization’s business environment.” EY survey (EY Global Information Security Survey, 2020) shows that “the cyber and privacy threat is increasing and expanding”. 6 out of 10 organizations (59%) have confronted an occurrence of threats in the previous 12 months. As the EY discloses, 48% of boards accept as true that cyber-attacks and data breaches will more than moderately influence their business in the following 12 months. Around one-fifth of these attacks (21%) arose from “hacktivists” (defined as tech-enabled, political, and social activists) and another one-fifth from organized crime groups (23%). Undoubtedly, all this impacts not only the crime problem but also more global problems in the economy (Remeikiene et al., 2022).

In turn, Bruni et al. (2023) suggest reconsidering collaboration with 3PL service providers to reduce data security risks, justifying this opinion by the level of experience those companies have in different logistics operations management. Another suggestion for risk prevention is the establishment of effective communication channels (Sravan et al., 2023) and investment in the newest digital technologies (Helmold et al., 2022) mentioned before.

Despite a separate strand of research in data security issues, more research is still needed in the context of ongoing digitalization. The authors seek to fill this gap by studying Latvia's enterprises in the context of other European countries.

3. Research methodology

The research incorporated conventional scientific methods, including literature review, data visualization, statistical analysis, synthesis, and monographic or descriptive methods. Through the methods above, we could examine the significance of data security, its concept, and the preventative actions taken by Latvian enterprises. The share of employees using the Internet to perform their duties regularly, the main activities of the enterprises in terms of customer data processing, and the core data security measures employed in Latvian enterprises have been examined. The literature was previously discussed to identify DS, logistical data, regulations focusing on data security, and the most common risks encountered by organizations processing data. The literature evaluation concentrated on gathering the most important details about the core risks associated with data processing in Latvian enterprises and the main preventive measures to ensure the security of logistical data.

The initial examination was steered in the following databases: Web of Science, Scopus, and Science Direct, and was constructed on the following keywords: logistics data, DS legislation, DS, and data. Primary literature sources were carefully chosen and grounded on the aim and topic of the research, as well as the availability of full-text articles. The research paper was developed on multiple data sources associated with data security, as the primary source was the Official Statistics Portal of Latvia. Still, due to the limited coverage in EU-level databases and delay in publishing, the information related to the data security measures applied was used with the latest available data. The study's scope covers from 2013 until 2023. The study methodologies employed were graphical and content analysis.

The comprehensive examination of the scientific works and statistical information endorsed the writers of the research to accomplish the previously indicated purpose of the article. This research should be considered as the next step of the previously conducted research by the authors Jurgelāne-Kaldava and Batenko (2023) about the topic "Assessment of Data Security Implementation in the Supply Chain Enterprises in Latvia" where the authors focused on the DS measures applied in supply chain enterprises and recommendations for their improvement.

4. Results and discussion

The potential logistics data security risks are directly linked to internet usage at the workplace. Even though many enterprises in Latvia focus on process automation, the primary data security concerns arise from the employees' knowledge of the preventive measures applied. According to data from the Central Statistical Bureau of Latvia (Official Statistics Portal of Latvia, 2024), as evidenced by Figure 1, the overall usage of the Internet has increased among all sizes of companies.

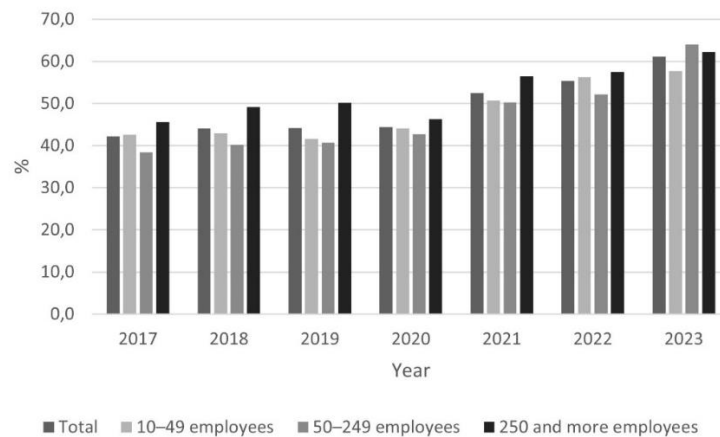


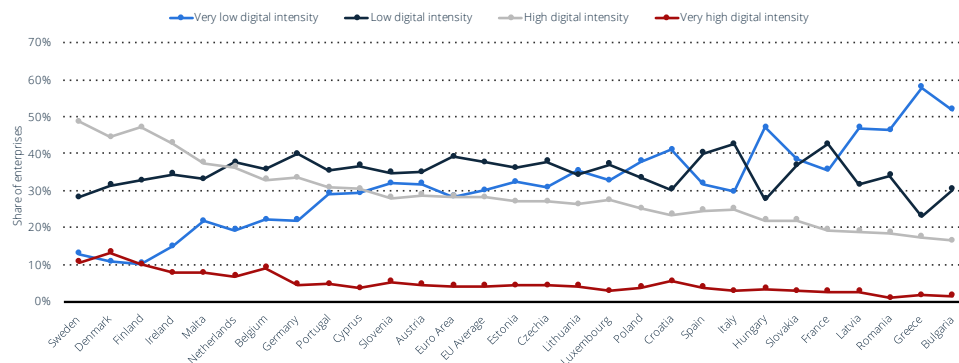
Figure 1. Employees using internet connection regularly in their jobs in Latvian enterprises from 2017 – 2023, %.

Source: authors created based on Official Statistics Portal of Latvia, 2024

Despite the increased use of the Internet by employees of all companies, it is essential to understand how digitalization in Latvian companies looks in the context of other countries. Figure 2 below shows that Latvian companies with over 10 employees are characterized as having very low or low digital intensity. Anyway, the digital intensity in Latvian enterprises is much higher than in Romania, Greece, and Bulgaria). Since the increase in digitalization is inevitable, data security issues will become more urgent.

Digital intensity of enterprises with more than 10 employees in the European Union in 2022, by member state

Digitalization in the EU: digital intensity for enterprises with 10 employees or more



Note(s): Europe, EU; 2022
Further information regarding this statistic can be found on page 8
Source(s): Eurostat; ID 1379056

statista

Figure 2. Digital intensity in European and Scandinavian countries in enterprises with more than 10 employees

Source: Statista

It should be reflected that the notable increase in Internet and mobile internet usage is related not only to technological advancements and the digitalization of services but also to the COVID-19 pandemic and the necessity for transferring services offered online.

To ensure the performance and functioning of essential business operations, companies must compile and store various logistics data related to their activities, employees, and customers. Table 1 illustrates the activities' growth as a percentage relative to the baseline year 2013.

Table 1. The growth of activities conducted by companies in Latvia to process information on clients (CRM) in 2013 – 2021, % compared to the baseline year 2013

Enterprises	Activity	2013	2014	2015	2017	2019	2021
Total	The collection*	12.9	10.6	17.6	15.4	12.4	16.3
	The analysis**	12.1	10.4	13.6	13.2	12.2	12.4
10–49 employees	The collection*	10.4	8.0	14.6	12.2	10.6	13.5
	The analysis**	10.0	8.2	11.5	10.7	10.8	10.3
50–249 employees	The collection*	24.2	21.1	28.0	27.6	18.6	26.7
	The analysis**	21.4	19.0	21.1	22.9	16.3	19.9
250 and more employees	The collection*	36.5	37.8	56.1	46.7	36.1	48.0
	The analysis**	30.7	33.4	38.3	37.3	32.8	37.6

Source: Official Statistics Portal of Latvia, 2022

* The collection refers to “the collection, storing and making available information about customers to various business functions”

** The analysis refers to “the analysis of information about customers for marketing purposes”

Examining the objective of information and data processing: “The collection, storing and making available information about customers to various business functions,” it should be stated that the total percentage of enterprises engaged in such operations increased by 26.4%, with the most significant increase by 31.5% for enterprises with 250 and more employees, followed by 29.8% and 10.3% increase for enterprises with 10 – 49 employees and 50 – 249 employees accordingly. Compared with the previous, the purpose of information and data processing: “The analysis of information about customers for marketing purposes,” has an overall growth of 2.45% compared with 2013. The number of companies processing customer data with 10 – 49 employees and companies with more than 250 employees has increased by 3.0% and 22.5%, respectively, but for companies with 50–249 employees, it has decreased by 7.0%. This decrease is related to the start of the implementation of the GDPR in 2017, which means that companies need to ask permission from the data subject (customer) to obtain, collect, and store the data. The most considerable decrease for the companies with 50 – 249 employees could be explained by the fact that companies did not have an internal data collection, compilation, and storage policy and policy related to customer relations, while the smaller companies with 10 – 49 employees have more robust relationships with customers and similarly, as companies with 250 and more employees have better customer relationships management and can more easily get the permission of data processing and storage (Official Statistics Portal of Latvia, 2024).

The most significant risks related to logistics data in ensuring business operations are associated with organized criminal groups implementing organized attacks. Still, it is necessary to highlight that a substantial amount (approximately 32%) comprises insiders – employees. It should be noted that in some instances, the Republic of Latvia laws even provide criminal liability to the company board (Teivāns-Treinovskis et al., 2022). Therefore, limiting access to different data and monitoring employees' activities is essential to eliminate or prevent data security risks.

Notably, 19 per cent of Latvia's enterprises experienced cyber security incidents in 2022, while Poland experienced 29,7 per cent and Bulgaria just 11 per cent (Figure 3). The differences can be caused by various reasons: level of digitalization, resilience, or decisions not to disclose incidents. No data available allows us to compare countries according to cyber incidents. Still, we assume that types of incidents are similar and can be illustrated by those in Italy in 2018 (see Figure 4 below). The main reasons for not reporting cyberattacks in Italy in 2018 are illustrated in Figure 5. These available data signal that there might also be numerous cyberattacks in other countries, which are not reflected by statistical data.

Cyber security incidents and consequences in enterprises in Central and Eastern Europe in 2022

Cyber security incidents and consequences in enterprises in CEE 2022

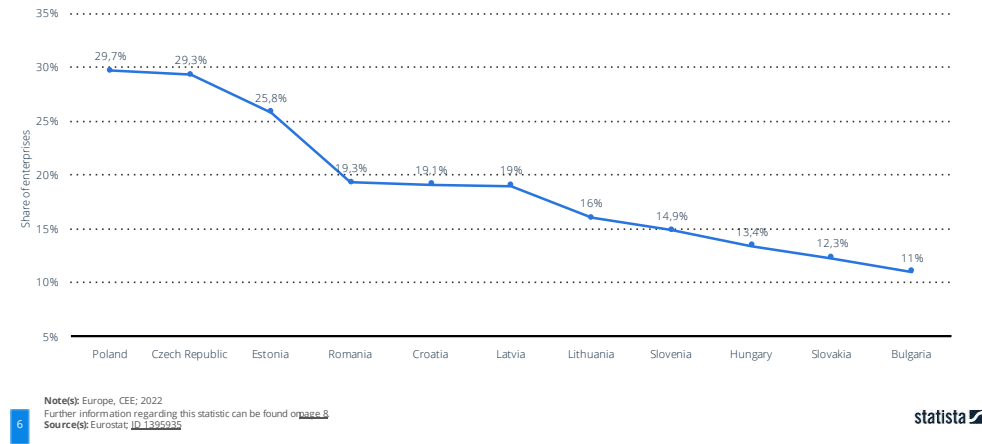


Figure 3. Share of enterprises experienced cyber security incidents in Central and Eastern Europe in 2022
Source: Statista

Main types of cyberattacks in Italy in 2018

Main types of cyberattacks in Italy 2018

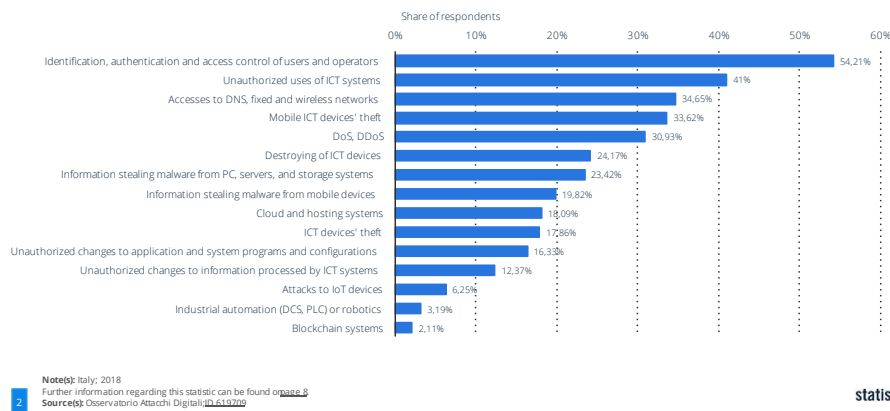


Figure 4. Types of cyber-attacks in Italy in 2018
Source: Statista

Main reasons for not reporting cyberattacks in Italy in 2018

Main reasons for not reporting cyberattacks in Italy 2018

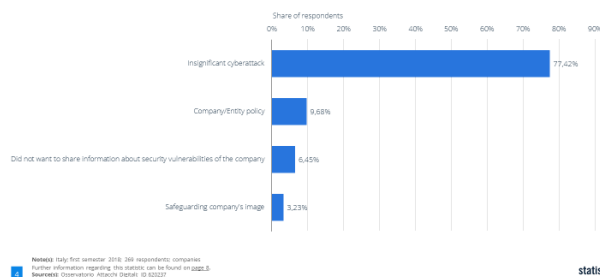


Figure 5. Main reasons for not reporting cyberattacks in Italy in 2018
Source: Statista

For further analysis of activities carried out by enterprises to ensure the prevention of logistics data security risks, categories defined by the Central Statistical Bureau of Latvia will be used. IT security measures can be divided into the following categories – strong password authentication, keeping the software up-to-date, user identification and authentication via biometric methods, encryption techniques for data, documents or e-mails, data backup to a separate location, network access control, VPN, maintaining log files for analysis after security incidents ICT risk assessment, ICT security tests (see Figure 6).

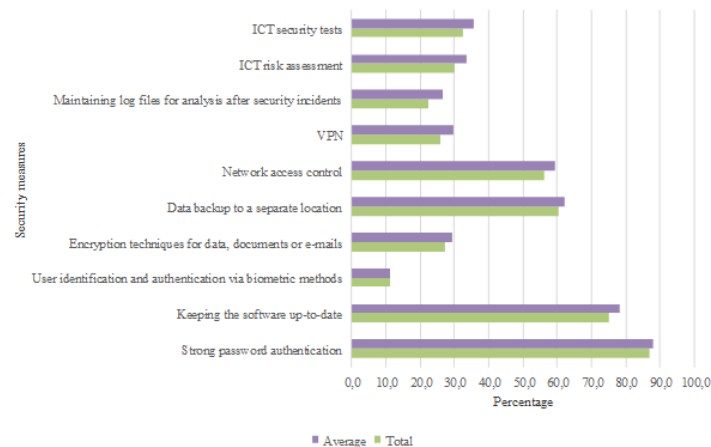


Figure 6. ICT security measures in Latvian enterprises in 2019, %.

Source: authors created based on Official Statistics Portal of Latvia, 2020

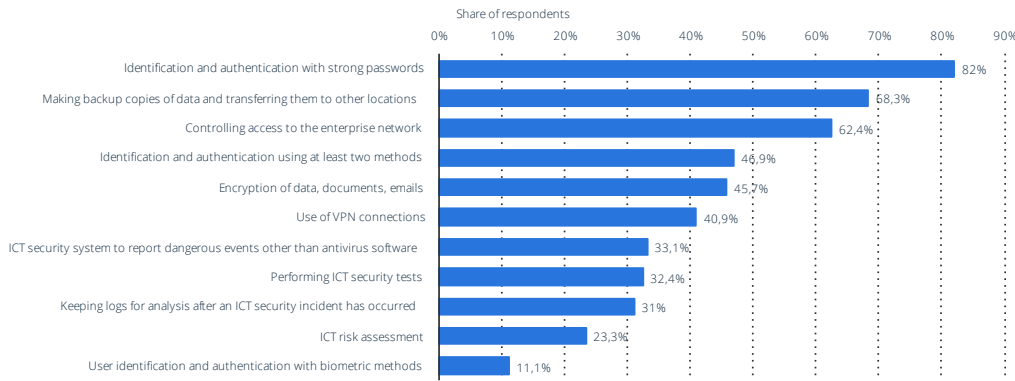
The most commonly used data security measures applied for all categories of enterprises are strong password authentication and keeping software up-to-date. On average, strong password authentication is one of the security measures used by 86.9% of companies analyzed (88.6% on average), but 75.1% keep software up-to-date (78.1% on average) (Official Statistics Portal of Latvia, 2024).

Generally, everything in terms of security is adopted by enterprises to secure intellectual property, client data, and confidential information of the enterprise. In addition, the less common security measures applied are user identification and authentication via biometric methods. This method uses 11.1% of companies analyzed (11.3% on average). This method is more widely used in information and communication technology companies (23.3% of all enterprises) and scientific laboratories (16.6% of all enterprises), where it is necessary to restrict access to confidential data. Based on the research, the companies processing logistics data apply strong password authentication (23.0% of all enterprises) and keep software updated (38.5% of all enterprises). (Official Statistics Portal of Latvia, 2024). This summary shows that enterprises collecting, storing, and processing data related to logistics do not apply customized security measures but rely on the traditionally accepted data security measures followed by average or non-existent risk management strategy applications.

Latvian enterprises' ICT data security measures are similar to those in other countries. Data on security measures in Poland (Figure 7), Czechia (Figure 8) and Belgium (Figure 9) are provided below.

Companies using information and communication technologies (ICT) security measures in Poland in 2022, by type

Companies using ICT security measures in Poland 2022, by type



Note(s): Poland; 2022; Enterprises with at least 10 employees
Further information regarding this statistic can be found on [page 8](#)
Source(s): Central Statistical Office of Poland [ID_1358276](#)

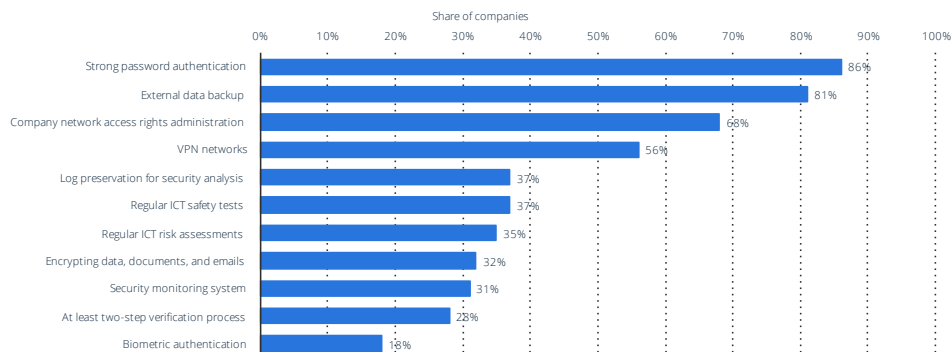
statista

Figure 7. ICT security measures in Poland in 2022

Source: Statista

Measures taken by companies to ensure ICT safety in Czechia in 1st half 2022

Company measures taken to ensure ICT safety in Czechia 2022



Note(s): Czechia; February to June 2022; Enterprises with 10 and more employees.
Further information regarding this statistic can be found on [page 8](#)
Source(s): Czech Statistical Office [ID_1362433](#)

statista

Figure 8. ICT security measures in Czechia in 2022

Source: Statista

ICT security measures used by enterprises in Belgium in 2022, by company size

ICT security measures used by Belgian companies 2022, by company size

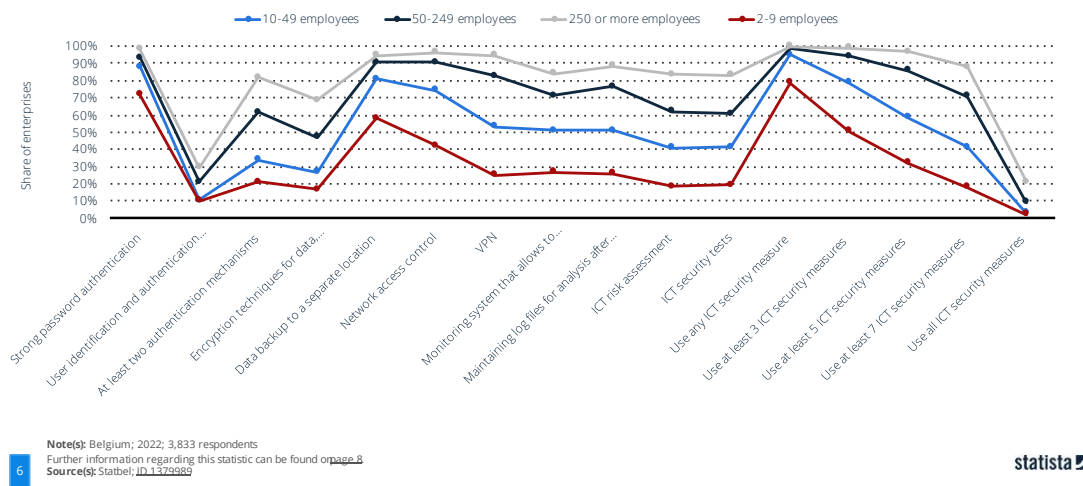


Figure 9. ICT security measures in Belgium in 2022

Source: Statista

The available data allows us to claim that Latvian enterprises' data security risks are similar to those of selected European countries. Latvia is characterized by slightly lower digital intensity in enterprises with more than 10 employees than analogic enterprises in European and Scandinavian countries. It allows us to expect the growth of digital intensity to bring more urgent issues in cyber security. Latvia has the potential to overcome the problems since the country applies contemporary measures similar to those used by other analyzed countries.

5. Conclusions

The study identified that the general measures to ensure data security in enterprises in Latvia are related to the frequency of data acquisition, processing, and storage. Latvian enterprises' most commonly used data security measures are strong password authentication, software updates, and data backup. It was not identified that the data security measures would differ based on the enterprise's industry or data processing type. Some patterns of the data analyzed require further investigation. For example, the factors leading to the decision to apply more advanced or customized data security measures and how to create customized data protection measures for the data related to the logistics operations that are usually linked to different internal systems and any internal or external threats may lead to the disruption in enterprises' operations.

In addition, the assessment of the main legal acts and different requirements related to data security in Latvia shows that enterprises should follow specific rules and procedures for data collection, storage, and usage, for example, the conditions included in GDPR and Personal Data Processing Law. In contrast, there was a significant decrease in the amount of data processed after the GDPR came into force and stabilized enterprises' business operations to meet the main legal requirements. This means that data security concerns regarding processing logistics data may arise due to the possible fines following the law and to customers' and employees' actions.

Moreover, the content and data analysis results show the necessity of more formal risk management in enterprises with 10 – 49 and 50 – 249 employees, as currently, following the data analyses, those enterprises steadily increase the amount and frequency of the data processed. The research showed that both enterprises with 10 – 49 and 50 – 249 employees have closer customer relations, thus facilitating risks related to violating the requirements for data processing and storage.

The most significant risks related to logistics data processing may arise not only from the outside but also from the employees due to personal interests or lack of knowledge in data management. The reported outcomes demonstrate that the overall number of crimes committed caused by DS in Latvia remains on a downward trajectory – 1/3 of crimes were explicitly committed by workforce members of the enterprise; hence, it is vital to enforce DS procedures for the protection of information and data for example, through restricting access to the systems or deploying various forms of authentication that gather information about files or information access. Therefore, data security risks concerning the data in wide-ranging logistics should be assessed and evaluated regularly. It is recommended that risk management strategies in the enterprise be developed, implemented, and regularly updated. It is suggested that the traditional data security measures mentioned above be incorporated.

References

- Ali, O., Shrestha, A., Chatfield, A., & Murray, P. (2020). Assessing information security risks in the cloud: A case study of Australian local government authorities. *Government Information Quarterly*, 37(1), 101419. <https://doi.org/10.1016/j.measen.2023.100856>
- Androniceanu, A., & Georgescu, I., (2023). Digital competencies and human development: a canonical correlation analysis in Romania. *Polish Journal of Management Studies*, 28 (1), 43-61. <https://doi.org/10.17512/pjms.2023.28.1.03>
- Bruni, M. E., Fadda, E., Fedorov, S., & Perboli, G. (2023). A machine learning optimization approach for last-mile delivery and third-party logistics. *Computers & Operations Research*, 157, 106262. <https://doi.org/10.1016/j.cor.2023.106262>
- Data Protection Law Enforcement Directive 2016/680 (DIRECTIVE (EU) 2016/680, 2016) https://www.eumonitor.eu/9353000/1/j4nvk6yhcbpeywk_j9vvik7m1c3gyxp/vk3t7p3lb4zo
- Ding, Q., & Zhao, H. (2021). Study on e-commerce logistics cost control methods in the context of COVID-19 prevention and control. *Soft computing*, 25(18), 11955-11963. <https://doi.org/10.1007/s00500-021-05624-5>
- DIRECTIVE (EU) 2016/680 (2016). *Official Journal of the European Union*. Retrieved February 20, 2024, from <https://eur-lex.europa.eu/legal-content/EN/TEXT/PDF/?uri=CELEX:32016L0680&from=EN>
- Doss, A. N., Shah, D., Smaism, G. F., Olha, M., & Jaiswal, S. (2022, April). A comprehensive analysis of the Internet of Things (IoT) in enhancing data security for better system integrity critical research on the security attacks and relevant countermeasures. In 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE) (pp. 165-167). IEEE. <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9823817>
- EY (2020). *EY Global Information Security Survey*. Retrieved February 20, 2024, from https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/advisory/ey-global-information-security-survey-2020-single-pages.pdf
- Filippova, N. A., Bashmakov, I. A., & Kochegura, D. Y. (2021). Goals and Risks of Activity as Factors of Regulation in Social Systems in Transport Sector. *World*, 19(2), 156-160. <https://doi.org/10.30932/1992-3252-2021-19-2-2>
- GDPR (REGULATION (EU) 2016/679, 2016) [https://uk.practicallaw.thomsonreuters.com/w-014-2751?transitionType=Default&contextData=\(sc.Default\)&firstPage=true](https://uk.practicallaw.thomsonreuters.com/w-014-2751?transitionType=Default&contextData=(sc.Default)&firstPage=true)
- Gupta, K., Gupta, D., Prasad, S. K., & Johri, P. (2021, March). A Review on Cryptography-based Data Security Techniques for the Cloud Computing. In 2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE) (pp. 1039-1044). IEEE. <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9404568>
- Helmold, M., Küçük Yılmaz, A., Dathe, T., & Flouris, T. G. (2022). Digitalization in Air Transportation and Reflections on SCRM. In *Supply Chain Risk Management: Cases and Industry Insights* (pp. 37-78). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-90800-3_3
- Hick, S., Biermann, H., & Ziefle, M. (2024). How deep is your trust? A comparative user requirements analysis of automation in medical and mobility technologies. *Humanities and Social Sciences Communications*, 11(1). <https://doi.org/10.1057/s41599-023-02575-0>
- Jurgelāne-Kaldava, I., & Batenko, A. (2023). Assessment of Data Security Implementation in the Supply Chain Enterprises in Latvia. *WSB Journal of Business and Finance*, 57(1), 21-27. <https://doi.org/10.2478/wsbjbf-2023-0003>

Katina, J., Plėta, T., Petkevičius, R., & Lelešienė, L. (2023). Industrial Control Systems (ICS) cyber prediction model. *Insights into Regional Development*, 5(1), 86-96. [https://doi.org/10.9770/IRD.2023.5.1\(6\)](https://doi.org/10.9770/IRD.2023.5.1(6))

Kennedy, E., & Millard, C. (2016). Data security and multi-factor authentication: Analysis of requirements under EU law and in selected EU Member States. *Computer Law & Security Review*, 32(1), 91-110. <https://doi.org/10.1016/j.clsr.2015.12.004>

Kraska T., Stonebraker M., Brodie M., Servan-Schreiber S., & Weitzner D. (2019) SchengenDB: A Data Protection Database Proposal. In: Gadepally V. et al. (eds) Heterogeneous Data Management, Polystores, and Analytics for Healthcare. DMAH 2019, Poly 2019. *Lecture Notes in Computer Science*, vol 11721. Springer, Cham. https://doi.org/10.1007/978-3-030-33752-0_2

Li, Y., Cheng, Q., Liu, X., & Li, X. (2020). A secure anonymous identity-based scheme in new authentication architecture for mobile edge computing. *IEEE Systems Journal*, 15(1), 935-946. <https://doi.org/10.1016/j.array.2023.100304>

Lincenyi, M., Svejnova Hoesova, K., & Fabus, M. (2023). Innovations in Marketing Communication in the Hospitality Business in Slovakia During the COVID-19 Pandemic. *Marketing and Management of Innovations*, 14(3), 230–242. <https://doi.org/10.21272/mmi.2023.3-20>

Liu, J. K., Liang, K., Susilo, W., Liu, J., & Xiang, Y. (2015). Two-factor data security protection mechanism for the cloud storage system. *IEEE Transactions on Computers*, 65(6), 1992-2004. <https://doi.org/10.1109/TC.2015.2462840>

Markos, E., Peña, P., Labrecque, L.I., & Swani, K. (2023). Are data breaches the new norm? Exploring data breach trends, consumer sentiment, and responses to security invasions. *Journal of Consumer Affairs*, 57(3), 1089-1119. <https://doi.org/10.1111/joca.12554>

Naim, A., Alqahtani, H., Muniasamy, A., Bilfaqih, S. M., Mahveen, R., & Mahjabeen, R. (2023). Applications of Information Systems and Data Security in Marketing Management. In Fraud Prevention, Confidentiality, and Data Security for Modern Businesses (pp. 57-83). IGI Global. <https://doi.org/10.4018/978-1-6684-6581-3.ch003>

Navickas, V., Grencikova, A., Kordos, M., & Sramka, M. (2022). The Information and Communications Technologies Usage within the Covid-19 Pandemic Issue. *Transformations in Business & Economics*, Vol. 21, No 1 (55), pp.101-113.

Nguyen, A., Bougacha, O., Lekens, B., Lamouri, S., Pellerin, R., & Couvreur, C. (2023). On the use of logistics data to anticipate drug shortages through data mining. *Procedia Computer Science*, 219, 949-956. <https://doi.org/10.1016/j.procs.2023.01.371>

Nica, E., Androniceanu, A., Sabie, O.-M., & Miša, A. (2023). Generative artificial intelligence and workplace tracking systems, synthetic training data, and computer-based teamwork simulations in 3D immersive spaces, *Analysis and Metaphysics*, 22, 24-42. <https://doi.org/10.22381/am2220232>

Official Statistics Portal of Latvia (2024). *Employees using any type of device with an Internet connection regularly (percent of total number of employees within the corresponding group) 2017 – 2023*. Retrieved February 20, 2024 from https://data.stat.gov.lv/pxweb/en/OSP_PUB/START_IKT_DL_DLU/DLU020/

Official Statistics Portal of Latvia (2022). *Activities carried out by enterprises using some IT solution to process the information on clients (CRM) (percent of the total number of enterprises within the corresponding group) 2013 – 2021*. Retrieved February 20, 2024 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 (percent of total number of enterprises within the corresponding group) 2019*. Retrieved February 5, 2024 from https://data.stat.gov.lv/pxweb/en/OSP_PUB/START_IKT_DL_DLU/EPD040

Patil, B. P., Kharade, K. G., & Kamat, R. K. (2020). Investigation of data security threats solutions. *International Journal of Innovative Science and Research Technology*, 5(1), 79-83. <https://ijisrt.com/assets/upload/files/IJISRT20JAN177.pdf>

Personal Data Processing Law (2018). Likumi. lv webpage. Retrieved February 5, 2024 from <https://likumi.lv/ta/en/en/id/300099>

PricewaterhouseCoopers (2008). *A Practical Guide to Risk Assessment*. Retrieved February 20, 2024 from http://www.pwc.com/en_us/us/issues/enterprise-risk-management/assets/risk_assessment_guide.pdf

Ramsaran-Fowdar, R. R., & Fowdar, S. (2013). The Implications of Facebook Marketing for Organizations. *Contemporary Management Research*, 9(1). <https://doi.org/10.7903/cmr.9710>

REGULATION (EU) 2016/679 (2016). Official Journal of the European Union Retrieved February 20, 2024, from <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN>

Remeikiene, R., Gaspareniene, L., Fedajev, A., Raistenskis, E. & Krivins, A. (2022). Links between crime and economic development: EU classification. *Equilibrium. Quarterly Journal of Economics and Economic Policy*, 17(4), 909–938. <https://doi.org/10.24136/eq.2022.031>

Shameli-Sendi, A. (2020). An efficient security data-driven approach for implementing risk assessment. *Journal of Information Security and Applications*, 54, 102593. <https://doi.org/10.1016/j.jisa.2020.102593>

Shastri, S., Wasserman, M., & Chidambaram, V. (2019) The seven sins of personal-data processing systems under GDPR. In: 11th USENIX Workshop on Hot Topics in Cloud Computing (HotCloud 2019), Renton, WA. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3425860

Shukla, S., George, J. P., Tiwari, K., & Kureethara, J. V. (2022). Data Security. In *Data Ethics and Challenges* (pp. 41-59). Singapore: Springer Singapore.

Subbalakshmi, S., Madhavi, K (2018). Security challenges of Big Data storage in a Cloud environment: A Survey. *International Journal of Applied Engineering*, 13(17), 13237-13244. https://www.ripublication.com/ijaer18/ijaerv13n17_36.pdf

Shen, Y., & Zhang, X. (2024). The impact of artificial intelligence on employment: the role of virtual agglomeration. *Humanities and Social Sciences Communications*, 11(1), 1-14. <https://doi.org/10.1057/s41599-024-02647-9>

Shavan, S. S., Ganesh, C. S., Kiran, K. V. D., Chandra, T. A., Aparna, K., Vignesh, T. (2023, March). Significant Challenges to espouse DevOps Culture in Software Organisations By AWS: A methodical Review. In 2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS) (Vol. 1, pp. 395-401). IEEE. <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10113021>

Teivāns-Treinovskis, J., Jefimovs, N., Velika, R. & Kriviņš, A. (2022). Conditions for application of criminal liability to the board of a company in the legal system of the Republic of Latvia. *Entrepreneurship and Sustainability Issues*, 9(4), 45-55. [http://doi.org/10.9770/jesi.2022.9.4\(2\)](http://doi.org/10.9770/jesi.2022.9.4(2))

Qatawneh, A. M., Al-Okaily, M. (2024). The mediating role of technological vigilance between IT infrastructure and AIS efficiency. *Journal of Open Innovation: Technology, Market, and Complexity*, 10(1), 100212. <https://doi.org/10.1016/j.joitmc.2024.100212>

Author Contributions: The authors contributed equally. All authors have read and agreed to the published version of the manuscript.

Ingūna JURGELĀNE-KALDAVA is an associate professor at the Faculty of Engineering Economics and Management at Riga Technical University. Research interests: logistics and supply chain management.

ORCID ID: <https://orcid.org/0000-0001-6756-7675>

Agnese BATENKO is Lecturer at the Faculty of Engineering Economics and Management at Riga Technical University. Research interests: logistics and supply chain management, digitalization, and data security in supply chain.

ORCID ID: <https://orcid.org/0009-0006-0631-8310>

Anatolijs KRIVINS is an associate professor at the Faculty of Law, Management Science, and Economics at Daugavpils University. Research interests: artificial intelligence, cyber security, corruption, and fraud prevention.

ORCID ID: <https://orcid.org/0000-0003-1764-4091>

Esat DURGUTI is an Associated Professor at the Faculty of Economics at the University "Isa Boletini". Research interests: Business, Financial Management, Banking Industry.

ORCID ID: <https://orcid.org/0000-0002-5982-3664>

Kristina GARŠKAITĒ-MILVYDIENĒ is an Associated Professor at Department of Financial Engineering, Faculty of Business and Management, Vilnius Gediminas Technical University.

ORCID ID: <https://orcid.org/0000-0002-2669-7630>