SILESIAN UNIVERSITY OF TECHNOLOGY PUBLISHING HOUSE

SCIENTIFIC PAPERS OF SILESIAN UNIVERSITY OF TECHNOLOGY 2025
ORGANIZATION AND MANAGEMENT SERIES NO. 215

FACTORS DETERMINING CUSTOMER DATA SECURITY IN AGILE ORGANIZATIONS

Maria KOCOT[1*], Bartosz BŁASZCZAK[2]

[1] University of Economics in Katowice; maria.kocot@ue.katowice.pl, ORCID: 0000-0001-5150-3765
[2] Higher School of Professional Education Wroclaw; bartosz.blaszczak@wskz.pl,
ORCID: 0009-0002-0457-4434
* Correspondence author

Purpose: The purpose of this article is to identify and assess key factors that impact customer data security in agile organizations. The study aims to determine priorities in data security management and to indicate patterns in how respondents perceive these factors.
Design/methodology/approach: The study was conducted using a survey method on a sample of 303 respondents in April-May 2023. The results were subjected to multivariate correspondence analysis (MCA) to identify relationships and patterns between data security factors.
Findings: The results indicate that factors such as data encryption systems, access control, real-time monitoring, and employee training are key. The MCA analysis revealed the interconnections between these factors and identified areas for further optimization in data security.
Research limitations/implications: The study is limited to agile organizations and relies on subjective opinions of respondents. The results may be extended in the future to other types of organizations or through the use of mixed methods to deepen the analysis.
Practical implications: The presented results can support organizations in developing effective customer data protection strategies. Recommended actions include implementing advanced security systems, regular audits and intensifying employee training.
Social implications: Improving customer data security strengthens consumer trust and loyalty while contributing to a more secure digital environment. These activities also respond to societal expectations related to respect for privacy and ethics in data management.
Originality/value: The article provides a unique perspective on the issue of customer data security in the context of agile organizations. The use of MCA analysis allowed for an in-depth assessment of patterns and relationships between factors, which enriches the literature on the subject and supports decision-making in organizations striving for operational agility.
Keywords: data security, client, agile organizations, MCA analysis, digitalization.
Category of the paper: research paper.

1. Introduction

The issue of customer data security in agile organizations is becoming crucial in the context of contemporary challenges posed by digital transformation and dynamically changing market conditions (Awasthi, Awasthi, 2023). The ongoing digitalization of business processes, the growing importance of data as a strategic resource, and the growing number of cyber threats make data protection not only an operational priority, but also the foundation for building trust and long-term relationships with customers. The conducted research focused on the analysis of factors determining customer data security in agile organizations allows for a better understanding of which management elements in this area are key and what challenges are associated with their implementation (Kurnia, Chien, 2020).

The article begins with a theoretical introduction that focuses on the importance of protecting customer data in the context of organizational agility. Then, the research objective is presented, which is to identify and assess key factors for ensuring data security in agile organizations. The research methodology used is also described, including the use of a survey conducted on a sample of 303 respondents and multivariate correspondence analysis (MCA), which allows for the identification of patterns in the respondents' answers. The subsequent sections of the article present detailed research results, including the respondents' assessments of individual factors and the analysis of the relationships between them. The research conclusions are supplemented with recommendations that can support organizations in designing effective data protection strategies.

Taking up this topic has significant practical and theoretical value. Protecting customer data is not only a legal requirement, but also a key element of building a competitive advantage (García-Granero, Piedra-Muñoz, Galdeano-Gómez, 2020). The research results provide insight into areas that require special attention and indicate the importance of a holistic approach to security management. The article adds value by identifying the most important factors affecting customer data security and by formulating specific recommendations that can be implemented by agile organizations. Thanks to the applied MCA analysis, it was possible to deepen the understanding of the mutual relationships between the studied factors, which enriches the existing literature on the subject with new perspectives and conclusions.

1.1. The Importance of Keeping Customer Data Secure

Ensuring the security of customer data is a key element of the functioning of modern organizations, especially in the era of dynamic development of digital technologies and the growing importance of data as a strategic resource. Customer data, both personal and business, are one of the most valuable assets of every organization, which is why their protection is not only a legal requirement, but also a fundamental aspect of building trust and reputation (Jones, Adam, 2023).

Customer data security directly affects the perception of an organization as professional, responsible, and trustworthy. As customers become more aware of the risks associated with privacy breaches, expectations of organizations regarding data protection are growing significantly. Data loss or improper protection can lead to serious consequences, such as loss of trust, decreased customer loyalty, and a negative impact on the organization's financial results. Moreover, in an era of increasingly stringent legal regulations, such as GDPR in the European Union, improper management of customer data can result in severe financial and legal penalties (LexDigital, 2022).

From the perspective of agile organizations, which are flexible and able to quickly adapt to changing market conditions, ensuring the security of customer data is particularly important. Such organizations often operate in a highly digitalized environment and use advanced technological tools to manage processes and communicate with customers (EITT, 2024). As a result, their activities are exposed to various threats, such as hacker attacks, data leaks or unauthorized access to systems (Chen, Siau, 2020). Ensuring data security requires a systemic and multi-faceted approach. A key element is the use of advanced technologies, such as data encryption, access control, regular security audits or real-time monitoring. At the same time, education of employees plays an important role, who must be aware of the threats and properly trained in data protection. Implementing procedures for handling security incidents helps minimize the potential effects of breaches (LexDigital, 2022).

Customer data security also has an important ethical dimension. Organizations are responsible for protecting the information entrusted to them, and any failure to do so can be perceived as a lack of respect for customers and their privacy (Joiner, 2019). Therefore, building an organizational culture in which data protection is a priority plays a key role in long-term business success (ODO24, 2024). In the context of contemporary challenges such as globalization, the development of cloud computing, or the growing number of cyberattacks, ensuring the security of customer data is not a one-time action, but a process that requires continuous optimization and adaptation to new threats. Organizations that effectively integrate data security management with daily operations not only gain a competitive advantage, but also build lasting relationships with customers based on trust and loyalty (Luo, Ren, Cao, Hong, 2020).

1.2. Customer Perception in Agile Organizations

The customer in agile organizations is a key element of the strategy of action, because it is the customer who is the center of all processes and decisions (Raschke, 2010; Womack, Jones, 2003; Yang, Liu, 2012). In the context of organizational agility, the customer is not perceived only as a recipient of a product or service, but as an active participant whose needs, expectations and opinions significantly shape the functioning of the organization. This way of thinking results from the philosophy of agility, which assumes dynamic adaptation to the changing environment and continuous improvement of the offer (Gadomska-Lila, 2013). In agile

organizations, the customer is perceived as a co-creator of value. The processes of designing and implementing products or services take place with their participation, for example by collecting feedback, organizing workshops or engaging in testing phases (Chen, Li, 2021). Thanks to this, organizations can better understand the real needs of customers, which allows for the delivery of solutions that are more tailored and meet their expectations. Such interaction has a positive impact on building long-term relationships based on mutual trust and commitment (Mrugalska, Ahmed, 2021).

Agile organizations also perceive the customer as a source of knowledge and inspiration. Information obtained from customers is an important element in the process of making strategic and operational decisions (Munodawafa, Johl, 2019). Thanks to this, organizations can respond to changing trends, identify new market opportunities, and anticipate future customer needs. Instead of relying on outdated patterns of action, agile organizations dynamically adapt to the environment, which allows them to remain competitive. Another important aspect of customer perception in agile organizations is personalization (Doz, Kosonen, 2008). Agile organizations strive to provide individually tailored solutions that take into account the specific preferences and expectations of each customer. Using advanced analytical tools such as big data or artificial intelligence, agile organizations are able to anticipate customer needs and provide them with the right products or services at the right time. Personalization not only increases customer satisfaction, but also strengthens their loyalty to the brand (Gao, Zhang, Gong, Li, 2020).

The customer in agile organizations is also seen as a partner in the process of building organizational value. The agile approach assumes that the relationship with the customer does not end at the sales stage, but lasts throughout the entire life cycle of the product or service. Regular interactions and collecting feedback allow organizations to continuously improve the offer and increase the value delivered to customers. However, such an approach requires openness to dialogue and flexibility in responding to criticism and changing needs (Rahimi, Mansouri, 2019). In agile organizations, the importance of the customer is not limited only to activities related to marketing or sales. The customer is an integral part of the organizational culture, in which every employee understands that their actions have a direct impact on the customer's experience. Thanks to this, agile organizations can effectively build their reputation as a trustworthy partner who can deliver high-quality solutions quickly and efficiently (Nath, Agrawal, 2020).

The perception of the customer in agile organizations also includes the aspect of social and ethical responsibility (Porter, Kramer, 2006). Customers increasingly expect organizations to operate in a transparent, ecological and ethical manner. Agile organizations try to respond to these expectations by implementing solutions promoting sustainable development and taking into account the needs of local communities in their activities (Borowski, 2021; Fiddler, 2017). This holistic approach allows an agile organization not only to meet customer needs, but also to build a positive image and engage customers in activities with a wide social reach.

1.3. Customer Data Security in Agile Organizations

Customer data security in agile organizations is an important element of management that affects the integrity of business processes and the reputation of the organization (BCO-Integrity, 2024). In the era of digitalization and a dynamically changing technological environment, ensuring customer data protection is becoming a priority, especially in the context of agile organizations that must constantly adapt to new challenges and threats (Attar, Almusharraf, Alfawaz, Hajli, 2022). Data security is not only a legal requirement, but also the foundation for building customer trust and long-term cooperation (Prieto, Talukder, 2023). One of the key elements of data protection in agile organizations is the use of encryption systems and advanced data protection technologies. Encryption is a basic mechanism that protects information from unauthorized access. However, its effectiveness depends on the quality of the algorithms used and regular updates of security systems, which should be adapted to changing attack methods. Agile organizations that are flexible in their operations must quickly implement new technologies and respond to potential threats to minimize the risk of data breaches (Rosário, Raimundo, 2021).

Another important aspect is access control and authorization, which help reduce the risk of unauthorized use of data. The introduction of multi-level user verification procedures, such as multi-factor authentication, enables effective management of access to sensitive information. Access control is particularly important in agile organizations, where cooperation between teams often requires dynamic allocation and modification of permissions (He, Harris, 2021). Appropriate access management allows for maintaining a balance between agility and data security. Regular security audits are another pillar of customer data protection. Audits enable the identification of potential security gaps and assessment of the effectiveness of implemented procedures. In agile organizations, these audits should be carried out periodically to adapt protection systems to changing operational and technological conditions. Their results allow for making informed decisions regarding further investments in security and minimizing the risk of breaches (Sedej, Justinek, 2021).

An essential element of the security strategy in agile organizations is employee education in the field of data protection. Training in this area allows to increase awareness of potential threats and develop appropriate habits in the daily use of IT systems. In the context of organizational agility, where teams work in a dynamic environment, this education must be a permanent element of the company's policy (Routledge, 2020). Employee knowledge is a key factor in data protection, because even the most advanced technologies can be ineffective in the face of human errors (Thales, 2022). Real-time monitoring and response play a key role in quickly detecting and neutralizing threats. Modern agile organizations use analytical tools that allow for continuous tracking of activity in IT systems. Implementing monitoring systems allows not only the identification of potential breaches, but also rapid response to incidents, which minimizes the risk of problem escalation (Seifollahi, Shirazian, 2021).

Protecting customer data also requires regular software and technology infrastructure updates. In agile organizations that often use modern tools and platforms, these updates are essential to ensure compliance with the latest security standards. Failure to update can lead to potential attackers exploiting known vulnerabilities, which poses a significant risk to data integrity (Syteca, 2020). Developing and implementing data breach procedures is another important element of a security strategy. In agile organizations, these procedures should be flexible to allow for quick adjustments to the specific situation. Proper incident management, including identifying the causes of the breach, informing customers, and implementing corrective measures, helps minimize the effects of breaches and rebuild customer trust (Sajdak, 2021).

In the context of agility, interdisciplinary cooperation in security management is of particular importance. Combining knowledge and experience from different areas of the organization allows for a more comprehensive approach to data protection (Brown, Jones, 2018). Teams consisting of IT experts, lawyers, managers and compliance specialists can jointly develop and implement solutions that provide a high level of data protection in a dynamically changing environment (Sherehiy, Karwowski, 2017). Ensuring the security of customer data in agile organizations requires a systemic approach that combines advanced technologies, procedures and employee awareness. These organizations must constantly adapt their strategies and practices to meet data protection challenges while maintaining the flexibility of operations and the ability to quickly respond to changing customer needs and external threats (Skyrius, Valentukevič, 2020).

1.4. Research Methodology

The aim of the research was to identify and assess key factors determining the security of customer data in agile organizations. The research aimed to indicate which elements of security management are most important from the perspective of respondents, and to analyze their mutual dependencies in the context of the dynamically changing needs of agile organizations.

A research hypothesis was formulated, assuming that there is a set of key factors with a high level of importance in ensuring customer data security, and their perception varies depending on the organizational specificity and the experiences of respondents. The study was to verify whether factors such as data encryption systems, access control or real-time monitoring are considered a priority by the majority of the study participants. Research questions were asked, which aimed to obtain detailed answers regarding the analyzed issue. In particular, it was tried to determine what are the most important factors related to customer data security in agile organizations, how respondents assess their importance and whether there are patterns in the answers that allow for grouping individual categories of factors.

The research method used in this project was a survey conducted in April-May 2023 on a sample of 303 respondents. The survey included questions on various aspects of data security management, including protection systems, audits, training, and technological infrastructure.

The collected data allowed for statistical analysis, including the use of MCA (Multiple Correspondence Analysis), which allowed for the identification of patterns and relationships between individual response categories.

MCA analysis was used to reduce the dimensionality of the data and visualize the relationships between factors, which allowed for a more precise understanding of the structure of the respondents' answers. This made it possible to indicate which of the studied factors were most closely related to the respondents' assessment and how these relationships could be used to optimize data security management practices in agile organizations.

1.5. Presentation of Research Findings

The research aimed to determine the factors determining the security of customer data in agile organizations, taking into account various areas of data management activities (see Table 1).

Table 1.
Factors determining the security of customer data in agile organizations (N = 303)

Category	Definitely not	Rather not	No opinion	Rather yes	Definitely yes
Encryption and data protection systems	20	37	59	130	57
Access control and authorization	22	40	45	128	68
Regular security audits	28	33	47	119	76
Employee data protection training	21	34	43	121	84
Real-time monitoring and response	19	42	55	118	69
Software and infrastructure updates	15	39	51	125	73
Procedures for data breaches	18	30	60	120	75
Interdisciplinary collaboration in security management	24	29	44	126	80

Study: own.

Respondents rated the importance of each of these factors on a scale from "definitely not" to "definitely yes". In the case of encryption and data protection systems, the largest number of respondents, as many as 130 people, indicated the answer "rather yes", and another 57 people chose "definitely yes", which indicates the high importance of this factor. At the same time, 37 people indicated "rather not" and 20 people chose "definitely not", which indicates a varied approach to this issue.

Access control and authorization were rated similarly, with 128 people indicating "rather yes" and 68 respondents "definitely yes". Smaller groups chose negative answers, with 40 people indicating "rather no" and 22 people "definitely no". Regular security audits received the most support in the "rather yes" and "definitely yes" groups, with 119 and 76 indications, respectively. At the same time, 28 people rated this factor as "definitely no" and 33 as "rather no". Staff training in data protection was rated particularly positively, with 121 respondents

indicating "rather yes" and 84 people "definitely yes". On the other hand, 34 people considered this factor as "rather unimportant" and 21 as "definitely unimportant". Real-time monitoring and response also received high marks, with 118 respondents choosing “rather yes” and 69 “definitely yes.” Negative responses were smaller, with 42 people choosing “rather no” and 19 choosing “definitely no.”

Software and infrastructure updates received support with 125 “rather yes” and 73 “strongly yes” responses. “rather no” and “strongly no” responses were given by 39 and 15 people, respectively. Data breach procedures also received high marks, with 120 “rather yes” and 75 “strongly yes” responses. “rather no” and “strongly no” responses were given by 30 and 18 people, respectively. Interdisciplinary collaboration in security management received 126 “rather yes” and 80 “strongly yes” responses . Negative responses were less numerous, with 29 “rather no” and 24 “strongly no.”

In order to identify patterns in respondents’ answers regarding the factors determining the provision of customer data security in agile organizations, MCA (Multiple Correspondence Analysis) analysis was conducted. This method allows for visualization of the relationships between the studied categories and assessment of which aspects are most closely related to specific dimensions of the analysis.

In the presented Figure 1, two main axes are marked, labeled "Dimension 1" and "Dimension 2", which represent dimensions of data variability. The horizontal axis (Dimension 1) explains the largest part of the variability between categories, while the vertical axis (Dimension 2) allows to capture additional differences that were not included in the first dimension. Each point on the graph corresponds to one of the analyzed categories, such as encryption and data protection systems, access control and authorization, or regular security audits.

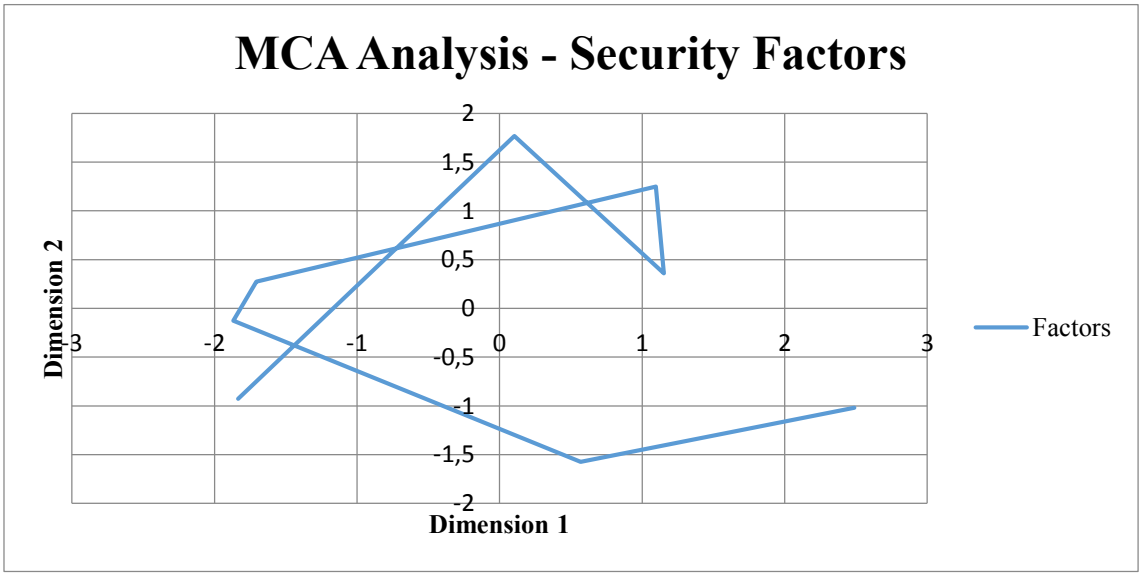

Figure 1. MCA Analysis – Security Factors.

Study: own.

The distribution of points can reveal differences in the perception of individual factors. Categories placed close to each other on the graph indicate similarity in terms of the respondents' responses, which may indicate that they are commonly perceived as important elements of ensuring security. For example, the proximity of points related to access control and encryption systems may suggest their key importance in managing data security. Outliers, located further from the center of the graph or from other categories, may indicate more specific characteristics of these factors that distinguish them from the rest. This may indicate the need to take special account of these aspects in further data security activities.

The MCA analysis was justified by the need to better understand the structure of the data, which includes multidimensional relationships between respondents' assessments. Thanks to this method, it is possible not only to indicate the most influential factors, but also to create a basis for further, more detailed analyses that can support management decisions in agile organizations. The chart is a graphical representation of the analysis results and facilitates the interpretation of key relationships between the categories studied.

2. Discussion

The research results allowed us to draw several important conclusions regarding the factors determining the security of customer data in agile organizations. First of all, it was indicated that respondents are characterized by a high awareness of the importance of actions aimed at protecting data, and individual categories, such as encryption systems, access control or staff training, received clear support as key elements in building security. However, differences in the level of assessment for individual categories indicate a different approach to their importance, which indicates a diverse perception of priorities in this area.

Data encryption and protection systems, which received high marks in the “rather yes” and “strongly yes” categories, were identified as fundamental in protecting customer data. The results suggest that these technologies are perceived as a basic measure to prevent security breaches, which indicates their widespread acceptance among respondents. Similarly, access control and authorization were considered crucial, which indicates the importance of procedures limiting access to data only to authorized persons. Such an approach minimizes the risk of unauthorized access and emphasizes the importance of consistency of security policies in organizations. Regular security audits received high support, which indicates their perception as an effective tool in identifying potential weaknesses in data protection systems. These audits, being part of prevention and monitoring, are seen as essential in the process of continuous improvement of security systems. The results emphasize the need for their cyclical conduct to ensure compliance with dynamically changing standards and technological requirements.

Data protection training was rated particularly highly by respondents, indicating its key importance in building employee awareness and responsibility. The results suggest that education in this area is an essential element of a security strategy, especially in agile organizations, where flexibility and variability of processes require the involvement of all team members. It was also emphasized that employee knowledge can act as the first line of defense in threat situations. Real-time monitoring and response were considered an important tool in the rapid identification and neutralization of potential incidents. The results indicate that dynamic and continuous monitoring of systems is perceived as a key element of proactive data security management. Real-time monitoring allows for detection of threats at an early stage, which reduces the risk of serious breaches.

Respondents also noted the importance of regular software and infrastructure updates, which underscores the need to maintain systems compliant with the latest security standards. The results suggest that neglecting this aspect can lead to serious consequences, including the exploitation of security holes by unauthorized persons. The need to develop procedures for handling breaches that enable rapid and effective crisis management and minimizing the effects of potential incidents was also mentioned. Interdisciplinary cooperation in security management was rated as an important factor, which indicates the need to involve different departments of the organization in the development and implementation of security policies. The results suggest that combining knowledge and experience from different areas, such as IT, law or management, can lead to more comprehensive and effective solutions.

Based on the MCA analysis, patterns in the perception of individual factors were identified, which allowed for the separation of the most influential elements in data security management. The proximity of individual categories on the chart indicates their mutual connections and similarity in the respondents' assessment, which can be the basis for further actions aimed at optimizing processes. The results of the MCA analysis also indicate the need for greater attention to factors that are perceived as less important, but can have a significant impact on security in specific contexts.

Overall, the research confirms the importance of a holistic approach to customer data protection in agile organizations. The results indicate that effective security management requires not only advanced technologies, but also conscious employee involvement, regular audits, and cooperation between different areas of the organization. This allows building lasting customer trust and ensuring security at a level that meets contemporary technological and social challenges. Based on the research conducted and the conclusions drawn, a number of recommendations can be formulated for companies that want to effectively manage customer data security in agile organizations. A key element of the strategy should be the adoption of a holistic approach that takes into account both advanced technologies and organizational and educational factors.

It is recommended to implement advanced data encryption systems and access control based on multi-level authentication procedures. These technologies should be regularly updated to keep up with dynamically changing threats. Organizations should also invest in real-time monitoring and response systems that allow for quick detection of security incidents and immediate preventive action.

It is important to regularly conduct security audits to identify potential gaps in systems and assess the effectiveness of implemented solutions. The results of these audits should be the basis for taking corrective actions and adapting security policies to current challenges. Introducing clear procedures for handling data breaches will allow for quick response and minimizing the effects of potential incidents.

Employee education should be a permanent element of the security strategy. Regular training is recommended to increase awareness of threats and develop appropriate habits in the field of data protection. Employees should also be informed about security procedures and the responsibility associated with their compliance.

Agile organizations should pay special attention to interdisciplinary cooperation in the field of security management. Combining the knowledge and experience of experts from various fields, such as IT, law or management, will allow for a more comprehensive approach to data protection and the development of solutions that will be consistent with both legal requirements and customer expectations.

Companies should also develop the ability to respond quickly to changing market and technological conditions. To this end, it is recommended to create flexible management structures that will allow for dynamic adjustment of security policies to new challenges. In addition, it is worth investing in the development of an organizational culture that promotes transparency, responsibility and commitment to protecting customer data.

According to the survey results, special attention should be paid to factors that are considered most important by respondents, such as encryption systems, access control, real-time monitoring and employee training. However, less obvious aspects, such as regular infrastructure updates or breach procedures, cannot be neglected, which in certain situations can be crucial for data protection.

Adopting these recommendations will allow companies to create a coherent and effective customer data security management strategy that will not only meet legal requirements, but also build customer trust and loyalty, which in the long term will contribute to increasing the organization's competitiveness in the market.

3. Conclusions

The results of the conducted research on factors affecting customer data security in agile organizations are consistent with the findings of other researchers. Particular importance is attributed to data encryption systems, which are considered a key element of information protection. As indicated by the study conducted by Thales, the lack of appropriate encryption mechanisms leads to numerous security breaches, especially in the case of data stored in the cloud (Thales, 2022). The literature also emphasizes that access control and authorization are an indispensable element of data protection. An approach based on the Zero Trust principle is increasingly recommended, which assumes that every user is a potential threat (Syteca, 2020).

Regular security audits are another important aspect discussed in both research and literature. Their role is to identify potential gaps in systems and ensure compliance with applicable standards. It is emphasized that audits should be conducted systematically to effectively manage risk (BCO-Integrity, 2024). At the same time, staff education in the field of data protection is considered a key element of the security strategy. As indicated in the literature, regular training increases awareness of threats and helps develop appropriate habits in the field of data protection (Syteca, 2020).

Real-time monitoring and response play a key role in quickly detecting and neutralizing threats. Today's agile organizations increasingly use analytical tools that enable ongoing control and response to security incidents (ODO24, 2024). Regular updates of software and technological infrastructure are equally important. Lack of updates can lead to the exploitation of known vulnerabilities in systems, which significantly increases the risk of security breaches (LexDigital, 2022).

Developing and implementing procedures for handling data breaches is another important element of the security strategy. The literature emphasizes that appropriate incident management and rapid response to breaches are crucial to minimizing the effects of such events (BCO-Integrity, 2024). Interdisciplinary cooperation in security management has been assessed as an important factor, which is confirmed by research by other authors. Combining knowledge and experience from different areas, such as IT, law or management, leads to more comprehensive and effective solutions (EITT, 2024).

In summary, the research results and their comparison with the literature on the subject indicate the need for a comprehensive approach to managing customer data security. Technical aspects, such as encryption and monitoring, must be supplemented with organizational activities, including staff education and interdisciplinary cooperation, to effectively protect data in a dynamically changing organizational environment.

The limitations of the research stem from several key aspects that may affect the interpretation of the results and their generalization. First, the study was conducted exclusively in the context of agile organizations, which may limit the applicability of the conclusions to

other types of enterprises, such as hierarchical or traditional organizations. The results reflect the specificity of agile work environments, which are characterized by high dynamics and flexibility, which may differ from structures less susceptible to rapid changes.

Another limitation is the data collection method. A survey based on subjective opinions of respondents may lead to errors resulting from the interpretation of questions, the diversity of professional experiences of participants, or their individual preferences. Although the sample size of 303 people provides a solid basis for analysis, the results may be partially limited by the lack of full representativeness of different industries and sectors. In addition, the multivariate correspondence analysis (MCA) method used, although extremely useful in discovering relationships between variables, has its limitations. The results are sensitive to the quality of the input data and may not fully reflect more complex relationships between the categories studied. MCA analysis allows for the identification of patterns and relationships, but does not provide direct information about causality or the direction of these relationships.

The time context of the study may also have an impact on its limitations. The study was conducted in April–May 2023, which means that the results reflect the specific technological and social conditions of that period. The rapid development of technology and changing legal regulations may mean that some conclusions require regular updates to remain relevant in a dynamically changing organizational environment. Another limitation may be the lack of consideration for the perspective of customers whose data is subject to protection. The study focused on the perception of representatives of organizations, which may not fully reflect the expectations and needs of customers themselves in terms of the security of their data. These aspects indicate the need for continued research that could include more diverse groups of respondents and additional methods of analysis.

Future research directions could focus on extending the analysis to other types of organizations, such as hierarchical or traditional structures, to see to what extent the factors determining data security differ depending on the specific organizational setting. An important area for further research is also comparative analysis between different industries, which would allow to determine which sectors are more exposed to threats related to data protection and which strategies are most effective in their context. It seems reasonable to take into account the perspective of customers to better understand their expectations and perceptions of data protection activities. Research could also include an analysis of the interactions between technological, organizational and cultural factors in ensuring data security, which would allow for a fuller understanding of their mutual dependencies and impact on the effectiveness of information protection.

Another research area could be the evaluation of the effectiveness of implementing individual recommendations resulting from the current study. Long-term analyses could provide data on the durability of implemented solutions and their adaptation in the changing technological environment. It is also worth considering the use of mixed methods, combining qualitative and quantitative analysis, to obtain a more comprehensive picture of the studied

issues. The development of technologies such as artificial intelligence and machine learning suggests the need for research on their application in the automation of processes related to data security. In the context of growing cyber threats, future research could also include an analysis of the effectiveness of preventive strategies in organizations, such as penetration tests or hacker attack simulations.

The global nature of data protection also suggests the need to consider cultural and legal differences in individual countries, which would allow for the identification of best practices on an international scale. Extending research to include these aspects would contribute to a better understanding of the challenges associated with ensuring data security in a complex, global organizational environment.

References

1. Attar, R.W., Almusharraf, A., Alfawaz, A., Hajli, N. (2022). New Trends in E-Commerce Research: Linking Social Commerce and Sharing Commerce: A Systematic Literature Review. *Sustainability, 14(23),* 16024. https://doi.org/10.3390/su142316024
2. Awasthi, K., Awasthi, S. (2023). Green computing: A sustainable and eco-friendly approach for conservation of energy (A contribution to saving the environment). In: S. Awasthi, G. Sanyal, C. M. Travieso-Gonzalez, P. Kumar Srivastava, D. K. Singh, R. Kant (Eds.), *Sustainable Computing: Transforming Industry 4.0 to Society 5.0* (pp. 319-333). Springer International Publishing. https://doi.org/10.1007/978-3-031-13577-4_19
3. BCO-Integrity (2024). *Data leak - how to act in its case?* Retrieved from: https://bco-integrity.pl/aktualnosci/wyciek-danych-jak-dzialac-w-jego-przypadku/
4. Borowski, P.F. (2021). Digitization, digital twins, blockchain, and Industry 4.0 as elements of management process in enterprises in the energy sector. *Energies, 14(7),* 1885. https://doi.org/10.3390/en14071885
5. Brown, K., Jones, L. (2018). The Impact of Decision-Making Speed on Organizational Agility. *Journal of Applied Psychology, 123(2),* 345-355.
6. Chen, X., Siau, K. (2020). Business Analytics/Business Intelligence and IT Infrastructure: Impact on Organizational Agility. *Journal of Organizational and End User Computing*. https://doi.org/10.4018/joeuc.2020100107
7. Chen, Y., Li, X. (2021). The Role of Organizational Agility in Managing the COVID-19 Pandemic: A Case Study of Two Chinese Hospitals. *International Journal of Environmental Research and Public Health, 18(1),* 70. DOI: 10.3390/ ijerph 18010070.
8. Doz, Y., Kosonen, M. (2008). The dynamics of strategic agility: Nokia's rollercoaster experience. *California Management Review, 50(3),* 95-118. https://doi.org/10.2307/ 41166447

9. EITT (2024). *Information Security Management – Key Aspects*. Retrieved from https://eitt.pl/baza-wiedzy/znaczenie-zarzadzania-bezpieczenstwie-informacji/
10. Fiddler, E. (2017). *Selected aspects of organizational agility*. SIGMA-NOT Publishing House. https://doi.org/10.15199/48.2017.12.2
11. Gadomska-Lila, K. (2013). Building the employer image and the efficiency of human resources management. *Education of Economists and Managers*, *4*, 185-197.
12. Gao, P., Zhang, J., Gong, Y., Li, H. (2020). Effects of technical IT capabilities on organizational agility: The moderating role of IT business spanning capability. *Industrial Management & Data Systems, 120(5),* 941-961. https://doi.org/10.1108/IMDS-07-2019-0394
13. García-Granero, E.M., Piedra-Muñoz, L., Galdeano-Gómez, E. (20202). Measuring eco-innovation dimensions: The role of environmental-mental corporate culture and commercial orientation. *Research Policy, 49(8),* 28-31. DOI: 10.1016/j.respol.2020.103948
14. He, H., Harris, L. (2021). The impact of organizational agility on crisis management and firm performance: A moderation analysis. *Journal of Business Research, 122,* 698-708. https://doi.org/10.1016/j.jbusres.2020.11.026
15. Joiner, B. (2019). Leadership Agility for organizational agility. *Journal of Creating Value, 5(2),* 194-208. journals. sagepub.com
16. Jones, E., Adam, C. (2023). New frontiers of trade and trade policy: digitalization and climate change. *Oxford Review of Economic Policy, 39(1),* 1-11. https://doi.org/ 10.1093/oxrep/grac048
17. Kurnia, S., Chien, S.W. (2020). Building organizational agility through strategic management accounting: A case study of an Indonesian manufacturing company. *Journal of Asia Business Studies, 14(4),* 591-612. https://doi.org/10.1108/JABS-09-2019-0253
18. LexDigital (2022). *Information security management system*. Retrieved from: https://lexdigital.pl/system-zarzadzania-bezpieczenstwo-informacji
19. Luo, B.N., Ren, X., Cao, Z., Hong, Y. (2020). Corporate sustainability paradox management: A systematic review and future agenda. *Frontiers in Psychology, 11*, 579272. https://doi.org/10.3389/fpsyg.2020.579272
20. Mrugalska, B., Ahmed, J. (2021). Organizational agility in industry 4.0: A systematic literature review. *Sustainability, 13(15),* 8272. Available at: mdpi.com
21. Munodawafa, R.T., Johl, S.K. (2019). A systematic review of eco-innovation and performance from the resource-based and stake-holder perspectives. *Sustainability, 11*, 60-67. DOI: 10.3390/su11030607.
22. Nath, V., Agrawal, R. (2020). Agility and lean practices as antecedents of supply chain social sustainability. *International Journal of Operations & Production Management, 40(10),* 1589-1611. https://doi.org/10.1108/IJOPM-10-2019-0676

23. ODO24 (2024). *Agile and information security: how to protect data in agile projects.* Retrieved from: https://odo24.pl/blog-post.agile-i-bezpieczenstwo-informacji-jak-chronic-dane-w-projektach- agile
24. Porter, M.E., Kramer, M.R. (2006). Strategy & Society: The link between competitive advantage and corporate social responsibility. *Harvard Business Review, 84,* 78-92. DOI: 10.1225/R0606E.
25. Prieto, L., Talukder, M.F. (2023). Resilient Agility: A Necessary Condition for Employee and Organizational Sustainability. *Sustainability*. DOI: 10.3390/ su 15021552.
26. Rahimi, G., Mansouri, A.M. (2019). *The relationship between the organizational intelligence and organizational agility (Case study: employees of municipality of Tabriz).* IAJOBHRM. DOI: 10.9756/iajobhrm/v5i1/1810010.
27. Raschke, R.L. (2010). Process-based view of agility: The value contribution of IT and the effects on process outcomes. *International Journal of Accounting Information Systems, 11(4),* 297-313. https://doi.org/10.1016/j.accinf.2010.09.005
28. Rosário, A., Raimundo, R. (2021). Consumer Marketing Strategy and E-Commerce in the Last Decade: A Literature Review. *Journal of Theoretical and Applied Electronic Commerce Research, 16(7),* 3003-3024. https ://doi. org /10.3390/jtaer16070164.
29. Routledge, P. (2020). *Organizational Agility with Mobile ICT? The Case of London Black Cab Work.* DOI: 10.4324/9780080463681-26.
30. Sajdak, M. (2021). *Strategic agility of enterprises*. Poznań University of Economics and Business Press. DOI: 10.18559/978-83-66199-32-3.
31. Sedej, T., Justinek, G. (2021). *Effective Tools for Improving Employee Feedback during Organizational Change.* DOI: 10.4018/978-1-7998-7297-9. ch 022.
32. Seifollahi, S., Shirazian, Z. (2021). *On the relationship between employees empowerment with competitive advantage and organizational agility mediated by organizational intelligence (Case study: employees in gas company of Hamadan).* EJM. DOI: 10.35429/ ejm.2021.27.12.1.10.
33. Sherehiy, B., Karwowski, W. (2017). *Workforce Agility Scale*. American Psychological Association (APA). DOI: 10.1037/ t 62364-000.
34. Skyrius, R., Valentukevič, J. (2020). Business Intelligence Agility, Informing Agility and Organizational Agility: Research Agenda. *Informatics, 90,* 47. DOI: 10.15388/ im .2020.90.47.
35. Syteca (2020*). 7 methods for data security inside the company*. Retrieved from: https://www.syteca.com/pl/blog/7-metod-na-bezpieczenstwo-danych-wewnatrz-firmy
36. Thales (2022). Thales study finds that most companies fail to protect their sensitive data in the cloud. *Computerworld*. Retrieved from https://www.computerworld.pl/article/2508414/ badanie-firmy-thales-wykazalo-ze-most-companies-don't-protect-their-sensitive-data-in-the-cloud.html

37. Womack, J.P., Jones, D.T. (2003). *Lean Thinking: Banish Waste and Create Wealth in Your Corporation.* Free Press.
38. Yang, C., Liu, H.M. (2012). Boosting company performance via enterprise agility and network structure. *Management Decision, 59(6),* 4-12.