SILESIAN UNIVERSITY OF TECHNOLOGY PUBLISHING HOUSE

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

DETERMINANTS OF DATA SECURITY OF THE ORDERING COMPANY DURING AN OUTSOURCING PROJECT

Damian KOCOT[1*], Bartosz BŁASZCZAK[2]

[1] University of Economics in Katowice; damian.kocot@ue.katowice.pl, ORCID: 0000-0001-9240-857X
[2] Higher School of Professional Education Wroclaw; bartosz.blaszczak@wskz.pl,
ORCID: 0009-0002-0457-4434
* Correspondence author

Purpose: The purpose of this study is to identify and analyze the key factors that enhance data security in outsourcing processes. The research aims to provide practical recommendations for organizations seeking to mitigate risks associated with the transfer and management of sensitive information in an outsourcing context.

Design/methodology/approach: The study employed a quantitative approach, utilizing a structured survey conducted in 2023 on a sample of 723 respondents. The collected data were analyzed using multiple correspondence analysis (MCA) to identify patterns and relationships between variables related to data security practices.

Findings: The research highlights that developing a comprehensive data security policy, employing advanced encryption technologies, conducting regular security audits, and fostering employee awareness significantly enhance data security in outsourcing processes. The findings emphasize the interconnectedness of these factors and their collective role in minimizing security risks.

Research limitations/implications: The study is limited by its reliance on a single quantitative method and a uniform sample, which may not fully capture sectoral or regional variations in outsourcing practices. Future research should explore qualitative methods and a more diverse sample to deepen the understanding of contextual factors affecting data security.

Practical implications: The study provides actionable insights for organizations to improve data security through structured policies, technological advancements, and targeted training programs. It underscores the importance of collaboration with outsourcing providers to ensure adherence to high security standards.

Social implications: Improved data security in outsourcing processes enhances trust between organizations, clients, and stakeholders. It contributes to broader societal benefits by safeguarding personal and sensitive information, thereby reducing the likelihood of data breaches and their associated consequences.

Originality/value: This study integrates theoretical perspectives with empirical findings, offering a comprehensive understanding of data security challenges in outsourcing. The use of MCA provides a novel approach to identifying the interrelations between key determinants, delivering valuable insights for both academics and practitioners in the field.

Keywords: outsourcing, data security, contracting company, project, survey.

Category of the paper: research paper.

http://dx.doi.org/10.29119/1641-3466.2025.215.10

1. Introduction

Modern organizations increasingly decide to outsource as a tool enabling cost optimization, access to specialist knowledge and increased operational flexibility. Along with the dynamic development of this cooperation model, the importance of issues related to data security is growing, which is becoming one of the key challenges in the process of outsourcing functions to external entities (Uhl-Bien, Arena, 2017). The problem of data protection in outsourcing is becoming particularly important in the face of the growing number of cyber threats, tightening legal regulations and the growth of expectations of customers and business partners. Data is a strategic resource of an organization, and its loss, theft or unauthorized access can lead to serious financial, legal and image consequences (Yin et al., 2020).

Taking up the topic of data security determinants in outsourcing processes results from the need to deepen knowledge in an area that is crucial for maintaining the integrity and stability of modern enterprises. The importance of this issue is particularly visible in the context of globalization and digitalization of the economy, where data is often processed and stored outside national borders, which additionally complicates their protection. This article attempts to analyze the factors influencing the effectiveness of data security activities in outsourcing, focusing on technological, organizational and educational aspects.

The article consists of several parts, which in a way lead to a full understanding of the discussed problem. The introduction presents the justification of the undertaken topic and discusses its importance in the context of contemporary business challenges. Then, a literature review and the most important theoretical concepts related to data security in outsourcing are presented. The next part describes the research methodology, including the use of multivariate correspondence analysis (MCA) and the characteristics of the studied sample. The results of the study are presented in the form of a detailed analysis, which identifies the most important determinants of data security. The final part discusses the conclusions from the conducted research, presents practical recommendations for companies and indicates future directions of research in this area.

The aim of the article is to identify and analyze factors that increase data security in outsourcing processes and to indicate practical solutions that can be used by organizations to minimize risk. The added value of the work is to combine a theoretical perspective with the results of empirical research, which allows not only to understand the complexity of the discussed problem, but also to develop practical tips for enterprises. The article contributes to the development of knowledge on data security management in the context of outsourcing, while emphasizing the importance of a multi-faceted approach to information protection in a dynamic and global business environment.

1.1. The essence of an outsourcing venture

The essence of an outsourcing project is that an organization outsources specific processes, functions, or activities to external service providers, which allows it to focus on key areas of activity and manage resources more effectively (Pearson, Benameur, 2010). Outsourcing is a practice that has gained popularity in many sectors, including information technology, logistics, finance, and administration (Zhang, Liu, 2010) . The decision to implement outsourcing usually results from the need to optimize costs, improve the quality of services, access to specialist knowledge, or flexibility in adapting to changing market conditions (Zhen, Xie, Dong, 2021). The fundamental assumption of outsourcing is to use the experience and infrastructure of an external provider, which allows the ordering party to avoid the need to invest in resources that could be expensive and time-consuming to build and maintain. Outsourcing service providers typically offer specialized solutions based on industry best practices that increase operational efficiency and process quality (Wang, Chow, Wang, Ren, Lou, 2011).

However, an outsourcing undertaking involves not only benefits but also challenges that require appropriate management (Cullen, Seddon, Willcocks, 2005). A key element is building a partnership relationship between the outsourcing company and the service provider. This cooperation should be based on trust, transparency and clearly defined rules (Ateniese et al., 2007). In particular, outsourcing agreements must contain precise provisions regarding quality standards, deadlines, responsibilities of the parties and monitoring and reporting mechanisms (Chow et al., 2009). The lack of clear rules can lead to misunderstandings and potential financial losses (Subashini, Kavitha, 2011).

An important aspect of an outsourcing project is managing the risk that results from transferring part of the company's activities to external entities. This applies in particular to data protection, process integrity and compliance with legal regulations (Quelin, Duhamel, 2003). Outsourcing companies must pay special attention to the selection of suppliers, assessing their credibility (Nassimbeni, Sartor, Dus, 2012), competences and ability to ensure security and compliance with industry standards. Outsourcing can also affect the organizational culture and employee engagement (Ravichandran, 2016). Transferring part of the functions to external suppliers can be perceived by the staff as a threat to their professional position, which requires appropriate change management in the organization. It is important for the company to clearly communicate the goals and benefits of outsourcing and to engage employees in the adaptation processes (Porter, Heppelmann, 2014).

Outsourcing can give organizations greater operational flexibility, especially in the context of changing market conditions (Bertino, 2009; Chakrabarty, 2006). Handing over tasks to external specialists allows for faster adaptation to new requirements, introduction of innovations and scaling of operations in response to growth or decline in demand. However, for an outsourcing undertaking to be effective, a strategic approach is necessary, which takes into account both potential benefits and risks. Proper management of outsourcing can bring long-term benefits in the form of increased efficiency, reduced costs and improved competitiveness in the market.

1.2. The importance of data security for the company commissioning the outsourcing project

In the context of an outsourcing undertaking, the security of the outsourcing company's data plays an extremely important role (Ren, Wang, Wang, 2012). Modern organizations base their operations on data, which is the basis for making decisions, building strategies and maintaining a competitive advantage. Transferring part of the processes to an external service provider means that key company information, such as customer data, financial data or data related to operational processes, must be properly protected to prevent their loss, unauthorized access or breach. Data security in such a context is particularly important due to the complexity of the relationship between the company and the service provider (Li, Li, Chen, Lee, Lou, 2014). When outsourcing processes, the organization relies to a large extent on the capabilities and infrastructure of the provider, which is why it is crucial for the outsourcing partner to comply with the highest standards of data protection. The lack of appropriate security measures can lead to serious consequences, such as loss of customer trust, high financial penalties resulting from non-compliance with regulations, and even permanent damage to the organization's reputation (Turban et al., 2018).

One of the most important aspects of data security in outsourcing is ensuring its confidentiality. Organizations often work with sensitive information, which may include personal data of customers, trade secrets or details of research and development projects (Galvin, 2019). The confidentiality of this information must be secured both through appropriate technological mechanisms, such as encryption, and clear provisions in outsourcing agreements. It is important that suppliers are obliged to comply with principles consistent with international standards, such as GDPR or ISO 27001.

Data integrity is another key aspect that is particularly important in the context of outsourcing. This means that data must be stored and processed in a way that guarantees its accuracy and completeness. Any errors or manipulations can lead to incorrect business decisions and, consequently, to financial or operational losses. In practice, this means the need to use advanced monitoring systems that allow for the rapid detection and elimination of potential breaches (Kamara, Lauter, 2010; Kern, Willcocks, Van Heck, 2013; Murphy, 2024). Data availability protection is another pillar of security in outsourcing. Companies must be sure that their data will be available whenever they are needed, regardless of the circumstances. This is especially true in crisis situations, such as system failures, cyberattacks or logistical problems on the supplier's side. Therefore, it is important that outsourcing agreements include business continuity mechanisms such as backups, contingency plans, and service level agreements (SLAs) (Raišienė, Bilan, Smalskys, Gečienė, 2019).

Data security in outsourcing is not limited to technical aspects (Wang, He, Tang, 2015). An appropriate organizational culture that promotes awareness of threats and responsibility for protecting information is also crucial. Outsourcing companies must ensure that both their own staff and the supplier's staff are properly trained in good security practices (Qureshi, 2016).

Finally, the importance of data security in outsourcing also stems from growing regulatory requirements and market expectations. Customers and business partners increasingly expect organizations to be able to demonstrate a high level of information protection, which poses additional challenges for companies in terms of monitoring and reporting security activities. Therefore, proper data security management is becoming not only an operational requirement but also a strategic success factor in long-term outsourcing cooperation (Arshad, Ahmad, Maynard, 2022).

1.3. Factors that increase the security of the outsourcing company's data during the outsourcing process

Increasing the security of the outsourcing company's data during the outsourcing process requires a multi-faceted approach that takes into account both technological, organizational and educational aspects. One of the key factors is the development and implementation of a coherent data security policy. Such a document should clearly define the principles of data management, procedures for handling incidents and requirements for outsourcing service providers (Annarelli, Colabianchi, Nonino, Palombi, 2021). The security policy should be dynamic, which means it should be regularly updated in response to changing threats and technological developments. The use of data encryption is one of the most important technical measures in data protection. Encryption allows you to protect information from unauthorized access, both during data transfer and storage. In the context of outsourcing, where data is often transferred between different locations and stored in the cloud, the use of advanced cryptographic methods becomes particularly important. The implementation of encryption should cover both data in motion and data at rest, which minimizes the risk of their interception or theft.

Another factor that increases data security is the regular conduct of security audits (Wang, Wang, Ren, Cao, Lou, 2012). These audits allow for the assessment of the effectiveness of implemented data protection measures and the identification of potential gaps and threats. They should be conducted both internally, by the organization's security department, and externally, by independent auditing entities. The results of audits should be the basis for taking corrective and improvement actions, which allows for continuous improvement of security standards (Infinit-O Global, 2022).

Building awareness among employees is an equally important element of data protection. In the context of outsourcing, where interaction between the outsourcing company’s staff and the service provider is inevitable, employee education plays a key role in minimizing the risk of human errors. Training should cover topics such as recognizing social engineering attacks, adhering to security policies, and responsibility for data protection. Aware and trained employees are the first line of defense against threats related to improper data processing (Pandita, Singhal, 2017).

In addition to the above activities, it is also important to implement mechanisms for monitoring and reporting data-related activities. Constant supervision over access to data and analysis of system logs allow for quick detection of unauthorized activities and appropriate response. As part of outsourcing, it is important for these mechanisms to also be used by service providers, which should be included in agreements regulating cooperation (Ghosh, Scott, 2008; Gupta, Puranam, Srikanth, 2006). An additional factor that increases data security is the use of a multi-layered protection strategy. This means combining various technologies and procedures, such as encryption, multi-factor authentication, access control, or backup. An integrated approach provides greater resistance to various threats, both those related to cyberattacks and system failures (Infinit-O Global, 2022).

In summary, data security in the outsourcing process can be effectively increased by combining appropriate technologies, procedures and educational activities. Clear rules of cooperation with suppliers, appropriately selected technical tools and a conscious approach to security management at every stage of project implementation are of key importance. Only such a comprehensive approach allows for minimizing risk and ensuring data protection in a dynamic environment of external cooperation.

1.4. Research Methodology

The aim of the conducted research was to determine the key determinants of data security in the context of business process outsourcing and to understand their mutual relations in the perception of people involved in such ventures. The research aimed to deepen knowledge about practices that increase data security, such as developing a security policy, using encryption, conducting audits and building awareness among employees. The research hypothesis assumed that individual activities related to data security have a different impact on the perception of their importance and are to a different extent related to organizational and technical factors.

The research asked questions about which activities have the greatest impact on the perception of data security and what are the relationships between individual determinants in terms of their effectiveness. Particular attention was paid to issues related to technology, audits and education, as well as their mutual relationships and differences in the perceptions of respondents.

The research method used was a survey conducted in 2023 on a sample of 723 respondents. The survey allowed for collecting quantitative data on opinions on the importance of various practices related to data security in outsourcing processes. Multivariate correspondence analysis (MCA) was chosen to analyze the obtained data. The aim of using this method was to identify patterns and relationships between the variables studied, which allowed for presenting their complex structure in two dimensions. Thanks to the MCA analysis, it was possible to better understand the dynamics of the relationships between the determinants of data security, as well as to indicate those activities that play a key role in data protection within outsourcing.

1.5. Presentation of Research Findings

The research aimed to determine the determinants of data security in companies commissioning outsourcing projects. The analysis included the opinions of 723 respondents in relation to four key areas related to data security (see Table 1).

Table 1.
Determinants of data security of the contracting company during an outsourcing project (N = 723)

Variable	Definitely not	Rather not	I don't have an opinion	Rather yes	Definitely yes
Development of data security policy (1)	34	71	113	228	277
Using data encryption (2)	47	59	102	221	294
Conducting regular security audits (3)	39	68	117	214	285
Creating security awareness among employees (4)	43	54	125	229	272

Source: Own study based on research.

In the case of the variable concerning the development of a data security policy, 34 people strongly disagreed with this solution, while 71 respondents rather disagreed with it. A neutral position on this issue was adopted by 113 people, while 228 respondents rather approved of this approach. It was strongly supported by 277 respondents. The second variable concerned the use of data encryption. In this category, 47 people declared that they definitely did not see the need to introduce this solution, while 59 respondents rather disagreed with it. Neutral opinions were expressed by 102 respondents, while 221 people considered it rather justified. Strong support was expressed by 294 respondents, which indicates significant appreciation for encryption as an element increasing data security. The third variable referred to conducting regular security audits. In this category, 39 respondents strongly disagreed with the need to implement them, while 68 people rather expressed such a position. Neutrality towards this practice was demonstrated by 117 respondents, while 214 people assessed it as rather beneficial. This solution was strongly supported by 285 respondents, which indicates its significant importance in the context of data protection.

The fourth variable analyzed the impact of creating security awareness among employees on improving data security. 43 respondents expressed strong opposition to this approach, while 54 people rather did not support this idea. Neutral opinions were declared by 125 respondents, and 229 respondents assessed this solution as rather effective. It was strongly supported by 272 people, which indicates wide acceptance of activities related to educating employees about data security.

Figure 1 presents the results of the multivariate correspondence analysis (MCA) for four variables: "Policy Development", "Data Encryption", " Security Audits" and "Awareness Creation". Each variable is embedded in two dimensions – Dimension 1 and Dimension 2 – which allows for visualization of the mutual relationships between them and their characteristics. Dimension 1, which is the horizontal axis, illustrates the differences in the importance assigned to individual variables in the analysis.

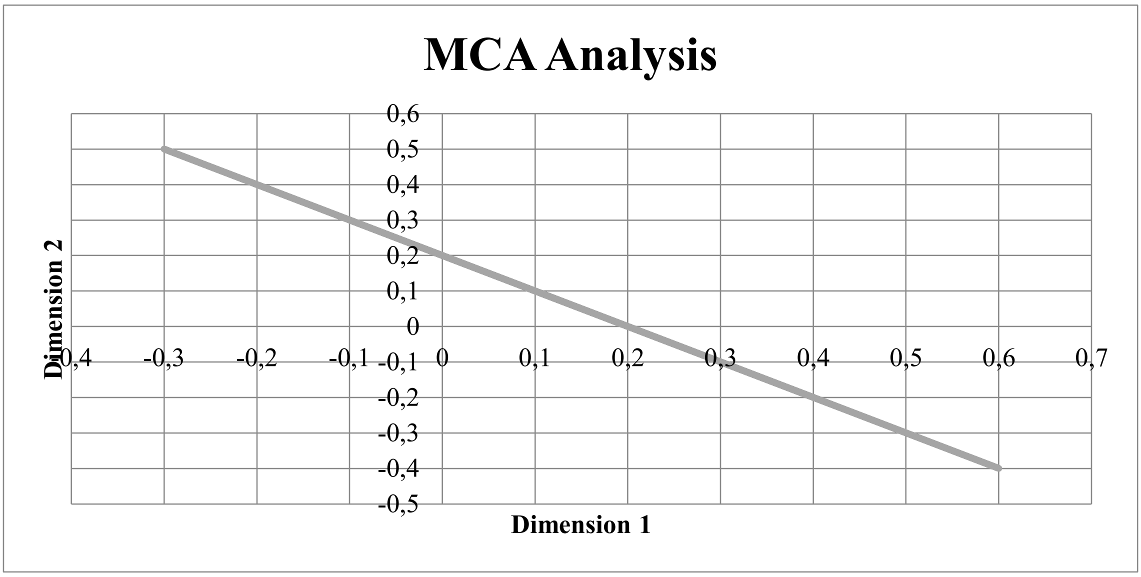

Figure 1. MCA Analysis.

Study: own.

In this dimension, variables such as "Policy Development" and "Security Audits" have positive values, which may suggest their strong connection with factors with a higher priority in the perception of respondents. In turn, variables "Data Encryption" and "Awareness Creation" have negative values, which may indicate a different nature of their connections or a lower importance perceived by respondents in the studied context. Dimension 2, located on the vertical axis, refers to the second factor differentiating the studied variables. In this dimension, "Data Encryption" and "Awareness Creation" have positive values, which indicates their clearly distinct profile in comparison to "Policy Development" and "Security Audits", which have negative values. Such a difference can be interpreted as an indication of a more practical use of positive variables in comparison to the more procedural nature of negative variables.

"Policy Development" is located in the first quadrant of the graph, which suggests its positive correlation with both Dimension 1 and Dimension 2. This may indicate that the development of a data security policy is perceived as important in the context of the studied characteristics. "Data Encryption" is located in the second quadrant, which indicates its positive correlation with Dimension 2 and negative with Dimension 1, emphasizing the specific role of encryption as a technical aspect of security. "Security Audits", located in the fourth quadrant, are characterized by a positive value of Dimension 1 and a negative value of Dimension 2, which may indicate their importance as a control tool. "Awareness Creation" in the third quadrant indicates a strong connection with the educational and awareness dimension of security activities.

Figure 1 enables easy identification of similarities and differences between variables and their positioning on two key dimensions. This makes it a useful tool for analyzing the relationships between variables and allows for further drawing conclusions about their role in the data security process in the context of outsourcing.

2. Discussion

The conclusions from the conducted research indicate that the determinants of data security in the context of outsourcing are diverse in terms of importance and perceived effectiveness. The development of a data security policy, which obtained high values in both dimensions of the MCA analysis, was identified as one of the most important activities. This results from the fact that clearly defined rules and procedures are the foundation of effective data security management. It also provides the basis for other activities, such as audits or employee education, which can only be effectively implemented within the framework of a well-defined security management system.

Data encryption, which received mixed results in two dimensions of the analysis, was assessed as a key element of technical data protection, although its perception is strongly dependent on the specifics of the organization and the level of technological advancement of the respondents. Respondents who rated encryption highly most often indicated its ability to protect data from unauthorized access, especially in the context of external cooperation. In turn, lower ratings may result from implementation difficulties, such as costs or the need for specialist knowledge. Security audit was identified as a practice with high control value. The results indicate that conducting regular audits increases trust in the security mechanisms used, allowing for early detection of potential gaps and threats. Audits also play a preventive role, affecting the responsibility of external entities for compliance with security standards. Nevertheless, some respondents indicated limitations of this practice, such as time consumption and dependence on the quality of the procedures performed.

Creating awareness of security among employees was assessed as an important, yet complementary element of the security strategy. The results suggest that employee education increases the effectiveness of other activities, such as security policy and data encryption, by reducing the risk of human errors. However, lower values in the first dimension of the analysis may be due to the perception of educational activities as less directly related to technological aspects of security, which does not reduce their importance in the overall strategy.

The MCA analysis also showed that different determinants are strongly interconnected. Developing a security policy is a key starting point, on which other activities, such as encryption or audits, are based. Educational activities, in turn, play a supporting role, increasing the overall effectiveness of the remaining elements of the security strategy. The results also indicate the need to integrate technical and organizational activities, which allows for a more comprehensive and effective approach to data protection in outsourcing processes.

In summary, the research confirms that effective data security management requires a multi-faceted approach, taking into account both technological and organizational elements. Security policy, regular audits and the use of advanced technologies such as encryption, supported by building awareness among employees, are of key importance. Such an approach allows to minimize the risk and ensure effective data protection within the framework of outsourcing cooperation.

To effectively manage data security in outsourcing processes, companies should focus on several key activities. First of all, it is necessary to create a comprehensive data security policy that will become the basis for all security practices. Such a policy should clearly define standards, procedures and responsibilities both within the organization and in relations with outsourcing partners. It is equally important to conduct regular security audits, which allow for early detection of gaps and potential threats. These audits should be carried out systematically and take into account both technological and organizational aspects, which allows for a full assessment of the effectiveness of the implemented actions. Commissioning audits to independent entities can additionally increase the objectivity of the results.

Implementing advanced technologies, such as data encryption, should be a priority for every organization. Encryption protects data from unauthorized access, especially when transferring information between a company and an outsourcing service provider. It is important that this technology is used consistently and adapted to the specifics of the company's operations. The role of employee education cannot be forgotten either. Regular data security training is crucial because it allows not only to increase knowledge about threats, but also to build awareness of responsibility for protecting information. Employees should not only know the basic principles of security, but also be able to recognize more advanced threats, such as attempted social engineering attacks.

It is also important to develop transparent relationships with outsourcing service providers. Building trust through clear communication of requirements and joint planning of data security activities can significantly increase the effectiveness of the actions taken. It is important that the cooperation is grounded in detailed agreements regulating data protection standards, and their compliance is systematically monitored. An approach that combines technological, organizational and educational aspects allows companies to manage data protection risks more effectively. Implementing these activities not only strengthens security, but also builds trust among customers and partners, which translates into the stability and long-term development of the company.

The key studies highlight important determinants of data security in outsourcing, such as security policies, encryption, audits, and employee education. However, the research has limitations, including reliance solely on quantitative methods, lack of consideration for specific sectors (e.g., medical, financial), and omission of the dynamic development of new technologies like artificial intelligence or blockchain. Additionally, the uniform sample and restriction to MCA analysis do not fully capture the complexity of the issue. Despite these weaknesses, the studies provide valuable practical insights and a solid foundation for further exploration.

The new knowledge brought by the conducted research includes a detailed identification and analysis of data security determinants in outsourcing processes, such as security policies, data encryption, audits, and employee awareness-building. The study demonstrated that the effective and integrated implementation of these elements significantly reduces risks related to data loss or unauthorized access. One key conclusion is the necessity of developing a coherent security policy, which serves as the foundation for other actions, such as audits and education. It was also shown that data encryption is perceived as a crucial element of technical protection, though its effectiveness may be limited by implementation costs and technological requirements.

Another important finding is the role of employee education in minimizing the risk of human errors, which enhances the effectiveness of other protective measures. Moreover, the analysis of interdependencies among security determinants highlights the need for a comprehensive approach that integrates technological, organizational, and educational aspects. The conclusions provide organizations with practical guidelines for improving data security in outsourcing and serve as a basis for further research in this area.

The conducted research is of significant importance for the practice of data security management in outsourcing processes, particularly in the context of increasing cyber threats and tightening legal regulations. Its findings contribute new knowledge about the key determinants of effective data protection, enabling organizations to better understand which actions are most effective in minimizing risks.

The impact of the research on the broader field includes supporting organizations in developing more advanced data protection strategies that can be tailored to various sectors and specific industry needs. Moreover, highlighting the importance of elements such as security policies, encryption, audits, and education provides valuable insights for both practitioners and further scientific studies. The information obtained can be used to develop comprehensive security standards applicable across different organizations. The findings can also serve as a starting point for further exploration of the topic, particularly in the context of dynamic technological changes such as the development of artificial intelligence and blockchain. Additionally, this research may inspire analyses in specific economic sectors, where data protection issues are of particular importance, such as the financial, medical, or educational sectors.

3. Conclusions

Comparing the results of the conducted studies with the findings of other researchers, one can notice both similarities and differences in the perception of the determinants of data security in the context of outsourcing. A study published in "Issues in Information Systems" indicated that despite concerns about security, some of the largest technology companies locate their operations in India, trusting the assurances of local service providers about data protection (Ghosh, Scott, 2008). Other sources emphasize the importance of physical data protection and quality management systems in the context of outsourcing, which is consistent with the results of the discussed studies, which indicate the importance of developing a security policy and regular audits (Infinit-O Global, 2022).

The literature also draws attention to the need to use advanced cryptographic technologies to ensure secure access to data stored in the cloud, which corresponds to the results of the discussed studies, emphasizing the importance of data encryption (Bertino, 2009). Furthermore, a review of the literature on secure outsourcing of computations indicates the need to use various security methods to cope with the threats associated with transferring IT functions to external entities (Wang et al., 2015).

In the context of IT outsourcing, other studies identify factors influencing organizations ' decisions to outsource IT security functions, emphasizing the importance of both managerial and legal aspects (Arshad et al., 2022). Furthermore, the analysis of risks related to outsourcing and offshoring services indicates the need to apply preventive and corrective measures to minimize potential threats (Nassimbeni et al., 2012). The results of the conducted research are consistent with the literature on the subject, emphasizing the importance of developing a security policy, using advanced cryptographic technologies, and regular audits to ensure data security in outsourcing processes. At the same time, differences in the perception of some aspects, such as employee education, may result from the specificity of the studied samples and the cultural and organizational context.

The limitations of research based on the analysis of data security determinants in outsourcing processes resulted from several factors. First, the research was based on data collected using a survey, which limits the possibility of in-depth qualitative analysis. Respondents could interpret the questions in a subjective way, which potentially influenced the results. In addition, the method used does not allow for full capture of the complex relationships between variables in the dynamically changing outsourcing environment, especially in the context of cultural and technological differences between companies.

The second limitation was the uniform sample of 723 respondents, which, although large in number, did not fully reflect the diversity of entities using outsourcing. The sample did not include specific sectors, such as the medical or financial industries, which may have different data security challenges. Additionally, the lack of data on the geographic origin of respondents limited the ability to analyze the impact of regional factors on the results. Another limitation was the lack of consideration of dynamic changes in data security technologies, which could have influenced the perception of some security determinants. Therefore, the results may not fully reflect current technological trends and innovations, such as the use of artificial intelligence or advanced encryption methods.

Finally, the study's limitations also related to the choice of MCA analysis as the main analytical method. Although it allows for the identification of patterns and relationships between variables, its results are more difficult to interpret in the case of more complex relationships. The lack of complementary statistical analyses, such as regression or cluster analysis, may have limited the fullness of conclusions drawn from the obtained data.

In conclusion, the limitations of the study result mainly from the adopted methodology, sample characteristics and the lack of consideration of the dynamically changing technological environment. However, the results constitute an important starting point for further research, which can deepen and extend the conclusions, taking into account a broader context and more diverse analytical tools. Future research directions may focus on a more comprehensive understanding of the determinants of data security in the context of various economic sectors. An important area for exploration is the analysis of specific industry requirements, such as healthcare, the financial sector or education, where data protection is of particular importance due to its sensitivity and legal regulations. The research may also take into account geographical and cultural differences in the perception of data security, which would allow for adapting the strategy to regional needs and requirements.

An important aspect of further research may be the analysis of dynamic changes in technologies related to data protection, such as the development of artificial intelligence, blockchain or advanced encryption methods. Examining their impact on the perception of data security and the effectiveness of the practices used could provide valuable tips for organizations looking for modern solutions in this area. Another area to explore is the role of education and employee awareness in the context of minimizing the risk associated with human errors. Research could focus on assessing the effectiveness of various training methods and identifying best practices in building a security culture in organizations using outsourcing.

It is also possible to deepen the analysis of cooperation between companies and outsourcing service providers, especially in terms of building trust and transparency in business relationships. Research could include aspects of contract negotiations, mechanisms for monitoring and auditing suppliers, and the impact of these activities on the overall quality of data security management. Finally, an interesting direction of research would be to examine the effectiveness of integrating technologies and organizational strategies in the context of data security. Analyzing the synergies between technologies and security policies could provide knowledge on the most effective combinations of actions that provide holistic data protection in a dynamically changing business environment. Future research could provide more detailed and contextual recommendations that would support organizations in developing effective data security strategies.

References

1. Annarelli, A., Colabianchi, S., Nonino, F., Palombi, G. (2021). The effectiveness of outsourcing cybersecurity practices: A study of the Italian context. *Proceedings of the Future Technologies Conference (FTC) 2021, Vol. 3* (pp. 17-31). Springer.
2. Arshad, A., Ahmad, A., Maynard, S. (2022). Factors Influencing the Organizational Decision to Outsource IT Security: A Review and Research Agenda. *arXiv preprint arXiv:2208.12875.* Available at: https://arxiv.org/abs/2208.12875
3. Ateniese, G., Burns, R., Curtmola, R., Herring, J., Kissner, L., Peterson, Z., Song, D.X. (2007). *Provable data possession at untrusted stores*. Proceedings of the 14th ACM Conference on Computer and Communications Security, 598-609. https ://doi . org /10.1145/1315245.1315318
4. Bertino, E. (2009). Secure Data Outsourcing. In: *Encyclopedia of Database Systems* (pp. 2555-2559). Springer. Available at: https://link.springer.com/referenceworkentry/10.1007/978-0-387-39940-9_328
5. Chakrabarty, S. (2006). *Making Sense of the Sourcing and Shoring Maze: Various Outsourcing and Offshoring in the 21st Century: A Socio-Economic Perspective*. London: Idea Group Publishing.
6. Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R., Molina, J. (2009). *Controlling data in the cloud: Outsourcing computation without outsourcing control*. Proceedings of the 2009 ACM Workshop on Cloud Computing Security, 85-90. https://doi.org/10.1145/1655008.1655020
7. Cullen, S., Seddon, P., Willcocks, L. (2005). Managing outsourcing: The life cycle imperative. *MIS Quarterly Executive, 4(1),* 1-12.
8. Galvin, B. (2019). *Lean Sigma Mastery Collection: 7 Books in 1: Lean Six Sigma, Lean Analytics, Lean Enterprise, Agile Project Management, Kaizen, Kahban,* Scrum. Independently Published.
9. Ghosh, A., Scott, J.E. (2008). Outsourcing: Data Security and Privacy Issues in India. *Issues in Information Systems, 9(2)*, 15-24. Available at: https://iacis.org/iis/2008/S2008_888.pdf
10. Gupta, S., Puranam, P., Srikanth, K. (2006). *Services sourcing in the banking and financial services industries. Exploding myths and describing emerging best practices*. London: London Business School and Capco Institute.
11. Infinit-O Global (2022). *Data Security in Outsourcing*. Available at: https://resourcecenter.infinit-o.com/blog/data-security-in-outsourcing/
12. Kamara, S., Lauter, K. (2010). *Cryptographic cloud storage. Financial Cryptography and Data Security,* 136-149. https ://doi . org /10.1007/978-3-642-14992-4_13
13. Kern, T., Willcocks, L.P., Van Heck, E. (2013). The winner's curse in IT outsourcing: Strategies for avoiding relational trauma. *MIS Quarterly Executive, 12(3),* 109-123.

14. Li, J., Li, X., Chen, X., Lee, P.P.C., Lou, W. (2014). A hybrid cloud approach for secure authorized deduplication. *IEEE Transactions on Parallel and Distributed Systems, 26(5),* 1206-1216. https ://doi . org /10.1109/TPDS.2014.2318320

15. Murphy, L. (2024). The influence of IT outsourcing on organizational success and innovation. *Future Business Journal, 10, Article 84*.

16. Nassimbeni, G., Sartor, M., Dus, D. (2012). Security risks in service offshoring and outsourcing: An FMEA-based approach. *International Journal of Production Research, 50(17),* 4840-4856. Available at: https://www.researchgate.net/publication/220672171_Security_risks_in_service_offshoring_and_outsourcing

17. Pandita, S., Singhal, R. (2017). The influence of employee engagement on the work-life balance of employees in the IT sector. *IUP Journal of Organizational Behavior, 16(1),* 38-57.

18. Pearson, S., Benameur, A. (2010). *Privacy, security and trust issues arising from cloud computing.* IEEE Second International Conference on Cloud Computing Technology and Science, 693-702. https ://doi . org /10.1109/CloudCom.2010.66

19. Porter, M.E., Heppelmann, J.E. (2014). How smart, connected products are transforming competition. *Harvard Business Review, 92(11),* 64-88.

20. Quelin, B., Duhamel, F. (2003). Bringing together strategic outsourcing and corporate strategy: Outsourcing motives and risks. *European Management Journal, 21(5),* 647-661. doi:10.1016

21. Qureshi, S. (2016). Creating a better world with information and communication technologies: Health equity. *Information Technology for Development, No. 22(1).*

22. Raišienė, A.G., Bilan, S., Smalskys, V., Gečienė, J. (2019). Emerging changes in attitudes to inter-institutional collaboration: the case of organizations providing social services in communities. *Administratie si Management Public, No. 33*.

23. Ravichandran, T. (2016). Exploring the relationships between IT competence, innovation capacity and organizational agility. *Information Systems, No. 27(1).*

24. Ren, K., Wang, C., Wang, Q. (2012). Security challenges for the public cloud. *IEEE Internet Computing, 16(1)*, 69-73. https ://doi . org /10.1109/MIC.2012.14

25. Subashini, S., Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications, 34(1),* 1-11. https://doi.org/10.1016/j.jnca.2010.07.006

26. Turban, E., Outland, J., King, D., Lee, J.K., Liang, T.P., Turban, D.C. (2018). *Electronic commerce 2018: a managerial and social networks perspective.* Springer.

27. Uhl-Bien, M., Arena, M. (2017). Complexity leadership: Enabling people and organizations for adaptability. *Organizational Dynamics, 46(1),* 9-20. https://doi.org/10.1016/j.orgdyn.2016.12.001

28. Wang, C., Chow, S.S.M., Wang, Q., Ren, K., Lou, W. (2011). Privacy-preserving public auditing for secure cloud storage. *IEEE Transactions on Computers, 62(2),* 362-375. https://doi.org/10.1109/TC.2011.245
29. Wang, C., Wang, Q., Ren, K., Cao, N., Lou, W. (2012). Toward secure and dependable storage services in cloud computing. *IEEE Transactions on Services Computing, 5(2),* 220-232. https://doi.org/10.1109/TSC.2011.24
30. Wang, H., He, D., Tang, S. (2015). Security and searchability in secret sharing-based data outsourcing. *International Journal of Information Security, 14(4),* 307-318. Available at: https://link.springer.com/article/10.1007/s10207-015-0277-x
31. Yin, J. et al. (2020). Does it pay to align a company's competitive strategy with its industry IT strategic role? *Information and Management, No. 57(8).*
32. Zhang, R., Liu, L. (2010). *Security models and requirements for healthcare application clouds.* IEEE 3rd International Conference on Cloud Computing, 268-275. https://doi.org/10.1109/CLOUD.2010.35
33. Zhen, Z., Xie, Z., Dong, K. (2021). Impact of IT governance mechanisms on organizational agility and the role of top management support and IT ambidexterity. *International Journal of Accounting Information Systems, No. 40*.