Creating Knowledge-Based Value for Data Security in Enterprises

Justyna Żywiołek
Faculty of Management, Czestochowa University of Technology, Poland

justyna.zywiolek@wz.pcz.pl

Abstract: The objective of this study is to analyze and understand how knowledge-based value creation can enhance data security in enterprises. In today's rapidly evolving technological landscape, data has become a critical strategic asset. In this context, knowledge management and its application to strengthen information security processes are essential priorities for organizations. The study identifies factors influencing the effectiveness of knowledge management in data security, such as organizational culture, innovative technologies, and employee engagement. It integrates theoretical frameworks from knowledge management, including Nonaka and Takeuchi's SECI model, with practical approaches to information security, such as the ISO 27001 standard. The findings suggest that organizations effectively combining knowledge management processes with cybersecurity initiatives achieve greater resilience against threats and enhanced incident response capabilities. Special attention is given to the role of tacit knowledge and its transfer in employee education and awareness programs. The study concludes with recommendations for implementing knowledge management practices to improve data security. These include fostering continuous employee skill development, leveraging technologies such as artificial intelligence and blockchain, and creating systems to support knowledge sharing within organizations. The proposed model serves as a tool to help enterprises build sustainable knowledge-based value, enhancing not only data security but also their overall competitiveness in the market.

Keywords: Knowledge management, Data security, Knowledge-bas knowledge transfer, Organizational culture, Innovative technologies, Employee awareness

1. Introduction

In the contemporary digital economy, data security has emerged as a critical concern for enterprises. With the increasing volume of sensitive data being generated, processed, and stored, organizations face growing challenges in safeguarding information from cyber threats, data breaches, and unauthorized access. Ensuring robust data security is not merely a technical issue but a multidimensional challenge that requires a strategic approach integrating technological, organizational, and human factors (Almustafa and Kalash 2025; Khan and Wallom 2022). One of the key strategies to enhance data security is leveraging knowledge management (KM) as a fundamental tool for creating knowledge-based value (Pandey et al. 2023; Żywiołek et al. 2022b). Knowledge, both explicit and tacit, plays a vital role in improving an organization's resilience to security threats by fostering a culture of awareness, continuous learning, and innovation. Effective knowledge management practices enable enterprises to develop proactive security measures, improve incident response capabilities, and minimize vulnerabilities arising from human error or lack of awareness (Żywiołek et al. 2025). This study aims to explore how knowledge management principles can be applied to enhance data security within enterprises. By integrating theoretical frameworks such as Nonaka and Takeuchi's SECI model with practical security approaches (Masucci et al. 2020), including the ISO 27001 standard, this research identifies the key factors influencing knowledge-based value creation for data security (Tarasova 2024). These factors include organizational culture, innovative technologies, and employee engagement, all of which contribute to strengthening cybersecurity resilience and fostering sustainable competitive advantages.

The intersection of knowledge management and data security has been the subject of extensive academic inquiry. Previous research highlights the crucial role of KM in improving cybersecurity practices and reducing organizational risks (Żywiołek and Abbas 2021). Nonaka and Takeuchi's SECI model (1995) provides a fundamental framework for understanding how knowledge is created, transferred, and utilized within organizations. This model emphasizes the conversion of tacit knowledge into explicit knowledge and vice versa, enabling enterprises to institutionalize security best practices and improve knowledge sharing among employees. ISO 27001, an internationally recognized standard for information security management systems, underscores the significance of a structured approach to data security (*Proceedings of the Second International Conference on Electronics and Renewable Systems (ICEARS 2023)* 2023; Żywiołek et al. 2022a). It aligns with KM principles by advocating for systematic policies, risk assessment, and continuous improvement mechanisms. Studies by Alavi and Leidner suggest that KM systems (Alavi and Leidner 2001), when integrated with security protocols, enhance an organization's ability to mitigate threats and respond effectively to security incidents.

Furthermore, research by von Solms and van Niekerk highlights the role of organizational culture in shaping cybersecurity awareness (Solms and van Niekerk 2013). A strong security culture, supported by effective knowledge-sharing mechanisms, reduces vulnerabilities and improves compliance with security policies.

Employee engagement, training programs, and leadership commitment are critical components in fostering a knowledge-driven security approach. Innovative technologies such as artificial intelligence (AI) and blockchain have also gained attention in the context of knowledge-based security enhancement. AI-driven threat detection and predictive analytics enable enterprises to identify potential risks proactively, while blockchain technology ensures data integrity and traceability. Studies by Xu et al. and Salah et al. emphasize the potential of these technologies in strengthening data security frameworks (Salah and Ayyash 2024; Xu et al. 2020).

Despite these advancements, challenges remain in integrating KM effectively with cybersecurity practices. Many organizations struggle with knowledge silos, resistance to change, and inadequate knowledge-sharing infrastructures. Addressing these issues requires a holistic approach that combines technological solutions with strategic knowledge management initiatives. This study builds upon existing literature by proposing a comprehensive model that merges knowledge management principles with advanced security strategies. By emphasizing the role of tacit knowledge transfer, continuous learning, and technological innovation, the research aims to provide actionable insights for enterprises seeking to enhance their data security through knowledge-based value creation (Corvello et al. 2023).

2. Literature Review

Despite the extensive research on the role of knowledge management in cybersecurity, a significant gap remains in understanding how tacit knowledge transfer and organizational culture specifically influence data security practices. While technological advancements such as artificial intelligence and blockchain have been recognized for their security potential, their integration within knowledge-based security frameworks is still underexplored (Hussain et al. 2024). Addressing these gaps, this study investigates how knowledge management processes contribute to enhanced cybersecurity resilience and strategic data protection in enterprises (Suuronen et al. 2022; Schiavone et al. 2021; Żywiołek et al. 2024). To achieve this objective, the following hypotheses are proposed. First, the effective implementation of knowledge management processes positively influences data security performance in enterprises (H1). Knowledge-based value creation fosters an environment where employees develop a deeper awareness of security threats, share best practices, and strengthen risk management strategies. Second, the integration of innovative technologies, such as artificial intelligence and blockchain, within knowledge management frameworks enhances organizational resilience against cybersecurity threats (H2). As enterprises increasingly rely on data-driven decision-making, these technologies support advanced threat detection, secure information sharing, and improved incident response mechanisms. By validating these hypotheses, the study aims to contribute both theoretically and practically to the understanding of how enterprises can leverage knowledge management and technological innovation to fortify their data security strategies.

The relationship between knowledge management (KM) and data security has been examined in various contexts, reflecting the growing importance of intellectual assets in protecting digital infrastructures. Alavi and Leidner (2001) were among the first to emphasize that knowledge management systems can facilitate better decision-making and enhance organizational responsiveness to security incidents. Their foundational work underscores the role of KM in building institutional memory, which is critical for incident response and risk mitigation. Nonaka and Takeuchi's (1995) SECI model serves as a conceptual cornerstone for many KM-based studies, explaining how tacit and explicit knowledge interact within an organization. In the context of data security, this model helps illuminate how experiential knowledge (e.g., from previous incidents) can be codified into protocols and procedures, supporting ISO 27001-aligned practices (Żywiołek et al., 2022a). This integration of formal and informal knowledge flows is increasingly recognized as a vital mechanism for developing organizational resilience (Masucci et al., 2020). Additionally, research highlights the importance of organizational culture and leadership in enabling effective knowledge-sharing for security purposes (Solms & van Niekerk, 2013). Without a supportive culture, even the most advanced knowledge systems are unlikely to deliver security benefits. Trust, engagement, and communication are consistently identified as enablers of secure knowledge environments (Xu et al., 2020; Żywiołek & Abbas, 2021). Technological innovation is another major dimension explored in the literature. Artificial intelligence and blockchain technologies have been cited as powerful tools for improving data protection and facilitating secure knowledge exchange (Salah & Ayyash, 2024; Hussain et al., 2024). AI enhances real-time threat detection and response, while blockchain ensures traceability and authenticity of shared knowledge assets. However, integrating these tools into KM systems presents both technical and organizational challenges, including user skepticism and knowledge silos (Żywiołek et al., 2024). Despite extensive academic focus, there is a research gap in examining how tacit knowledge transfer, particularly in the context of employee behavior and organizational learning, contributes to data security. Few studies systematically assess how informal knowledge-sharing mechanisms influence compliance,

incident handling, or resilience (Schiavone et al., 2021). Similarly, while ISO 27001 and GDPR are widely implemented, their synergy with KM strategies remains underexplored, especially across different cultural and regulatory environments (Tarasova, 2024; Suuronen et al., 2022). This study seeks to bridge these gaps by proposing a model that integrates knowledge-based value creation with data security enhancement. Specifically, the research focuses on how enterprises operationalize knowledge management to foster awareness, strengthen internal protocols, and adopt innovative technologies for cyber resilience.

3. Materials and Methods

This study employed a quantitative research approach using the Computer-Assisted Web Interviewing (CAWI) method to examine the role of knowledge management in enhancing data security within enterprises. The research was conducted in three European countries—Poland, Germany, and Spain—to provide a cross-national perspective on the integration of knowledge-based value creation into cybersecurity strategies. The primary objective was to assess how enterprises implement knowledge management processes to improve data security, increase employee awareness, and leverage technological solutions for cybersecurity resilience.

The study was conducted in two phases. In the first phase, a conceptual framework was developed to outline key constructs related to knowledge management and data security. This framework guided the creation of the research instrument. In the second phase, a large-scale CAWI survey was conducted to gather empirical data efficiently while minimizing the limitations associated with in-person interviews. The survey took place in the latter half of 2023, and a total of 9,837 valid responses were collected, with 3,256 from Poland, 3,421 from Germany, and 3,160 from Spain. These countries were selected due to their comparable levels of digital transformation, cybersecurity regulations under the General Data Protection Regulation (GDPR), and shared approaches to knowledge management.

The survey instrument was a structured questionnaire divided into three sections: (1) demographic and organizational background, including participants' roles, industries, and experience in data security management; (2) knowledge management and data security practices, evaluating knowledge-sharing mechanisms, employee training, and the adoption of innovative technologies; and (3) perceived effectiveness and challenges, measuring confidence in cybersecurity strategies, organizational resilience, and existing knowledge gaps. Responses were collected using a five-point Likert scale (1 = Strongly Disagree, 5 = Strongly Agree) to assess attitudes, awareness, and the perceived impact of knowledge management on security. The questionnaire comprised twenty-four inquiries, including nine specific questions based on the Servqual methodology, designed to analyse discrepancies between expected and actual knowledge-based security implementations.

The sample was designed to be representative of enterprises operating within the selected countries. Although national contexts may differ, the study assumes that economic development levels, regulatory cybersecurity frameworks, and organizational security strategies are comparable across these nations. Additionally, the freedom of movement and cross-border knowledge exchange within the European Union facilitate a unified approach to knowledge management in cybersecurity.

For data analysis, Microsoft Excel was used to perform descriptive statistics, including frequency distributions and percentage breakdowns, to identify trends in cybersecurity awareness and knowledge-sharing practices. Comparative analyses were conducted across the three countries to assess regional differences and similarities in the implementation of knowledge-driven cybersecurity strategies. The findings from this study contribute to a deeper understanding of how enterprises can integrate knowledge-based value creation to strengthen their cybersecurity frameworks and enhance data protection measures.

Figure 1 illustrates the research process, outlining the sequential steps undertaken in the study, from defining the research objectives to data collection, analysis, and deriving conclusions. The diagram highlights the structured approach, including the conceptual framework development, survey implementation using the CAWI method across three countries (Poland, Germany, and Spain), and the subsequent data analysis using Excel-based statistical processing. Each stage is designed to ensure a comprehensive examination of how knowledge management contributes to enhancing data security in enterprises. To ensure methodological transparency, additional details regarding the sampling frame and response metrics are provided. The total population targeted in this study included medium and large enterprises operating in Poland, Germany, and Spain, which actively engage in digital transformation and implement cybersecurity measures. Based on data from national enterprise registries and business databases, the estimated total population across these three countries was approximately 145,000 enterprises. The final dataset comprised 9,837 valid responses, which corresponds to an

overall response rate of approximately 6.8%. This rate is considered appropriate for large-scale CAWI (Computer-Assisted Web Interviewing) studies targeting organizational representatives on specialized topics such as data security and knowledge management.

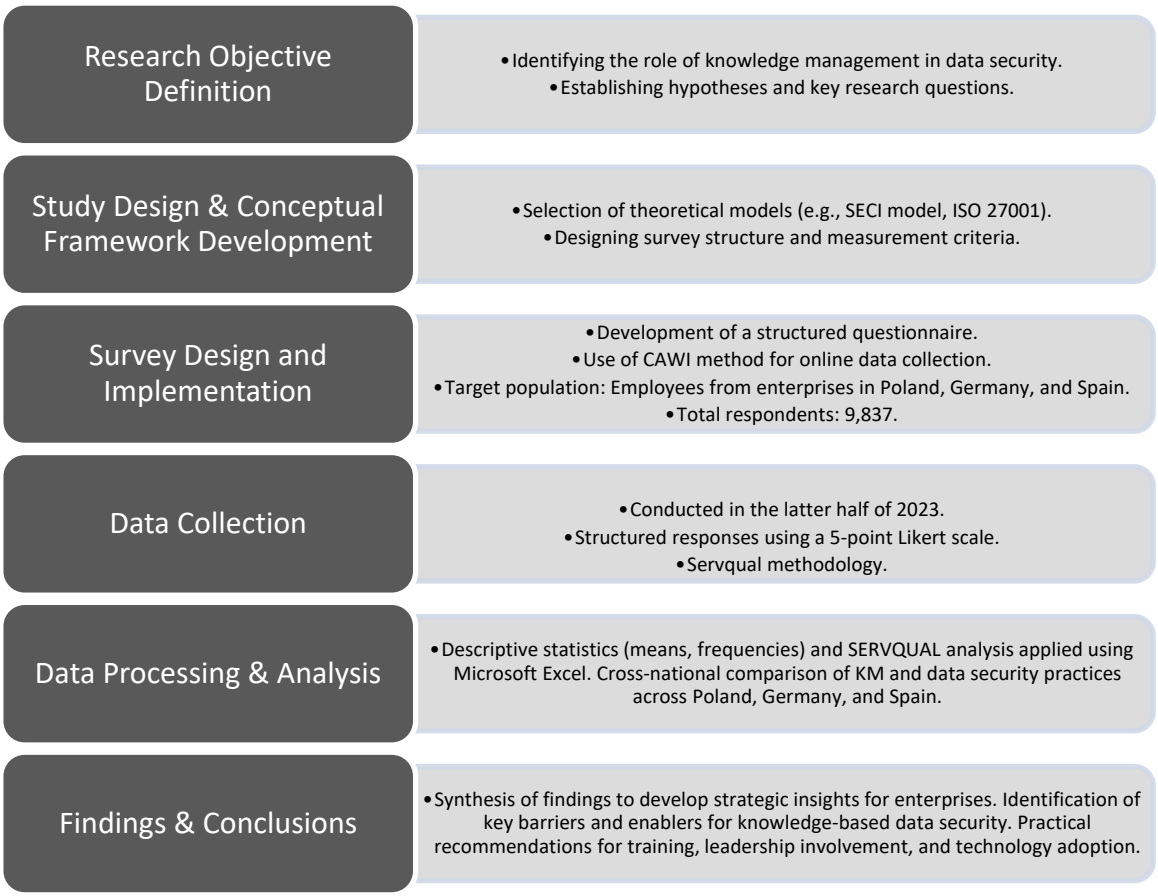

Figure 1: Research procedure

Figure 1 provides a structured overview of the research process, from defining objectives and designing the survey to data collection and analysis. This systematic approach ensures a comprehensive examination of how knowledge management influences data security in enterprises. The following section presents the study's findings, offering insights into the effectiveness of knowledge-sharing practices, employee cybersecurity awareness, and the impact of technological solutions on organizational resilience.

4. Results

Figure 2 illustrates key challenges and concerns related to knowledge management and data security in enterprises. The increasing reliance on digital technologies and cybersecurity frameworks highlights the importance of effectively managing security knowledge within organizations. While enterprises recognize the value of cybersecurity awareness and structured knowledge-sharing mechanisms, several issues persist, including gaps in employee training, resistance to adopting new security protocols, and inconsistencies in knowledge transfer. These challenges impact the overall effectiveness of cybersecurity strategies and increase vulnerability to cyber threats. Figure 2 presents an overview of these factors, emphasizing the need for comprehensive knowledge-based security solutions to enhance organizational resilience.

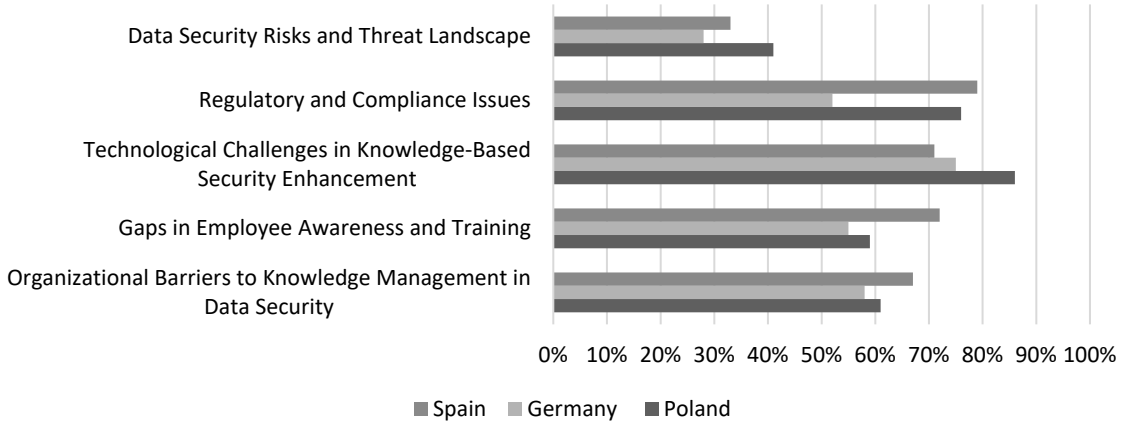

Figure 2: Problems with data security in selected countries

The identification of barriers and challenges in cybersecurity knowledge management has enabled a clearer definition of strategies to enhance security practices within enterprises. Table 1 presents an overview of key areas influencing knowledge management in data security, assessing factors such as employee awareness, organizational responsibility, accessibility of security knowledge, trust in security technologies, and challenges in knowledge transfer. The descriptive statistics for these constructs indicate moderate levels of awareness and implementation of security knowledge within organizations. The mean value for Knowledge and Awareness of Data Security Practices is 3.28, reflecting a need for improved training and education initiatives to enhance employees' understanding of cybersecurity threats and best practices. Similarly, Organizational Responsibility and Leadership in Data Security scored 3.07, suggesting that while leadership acknowledges the importance of cybersecurity, there are gaps in policy enforcement and managerial involvement in knowledge-sharing initiatives. Furthermore, Accessibility and Implementation of Security Knowledge received a mean score of 2.94, indicating challenges in integrating structured security knowledge management systems across enterprises. The Trust and Awareness in Security Technologies score of 2.83 highlights a lack of confidence in automated security solutions such as AI-driven threat detection and blockchain-based security frameworks. Lastly, Challenges in Security Knowledge Management were rated at 2.91, pointing to issues such as resistance to adopting new security protocols, gaps in cybersecurity literacy, and difficulties in transferring security expertise across teams. These findings emphasize the need for a holistic approach to cybersecurity knowledge management, integrating structured training programs, leadership commitment, and technological innovations to enhance organizational resilience against cyber threats. The study's next section further explores how enterprises can address these challenges by adopting knowledge-based security strategies.

Table 2: Mean values and Cronbach's α coefficient

Variable	Average value	Cronbach's α
Knowledge and Awareness of Data Security Practices	3,28	0,82
Organizational Responsibility and Leadership in Data Security	3,07	0,87
Accessibility and Implementation of Security Knowledge	2,94	0,76
Trust and Awareness in Security Technologies	2,83	0,81
Challenges in Security Knowledge Management	2,91	0,85

The initial phase of the study was establishing the presence and magnitude of the relationship. In the initial stage of the Servqual study, we calculated the discrepancies between the levels of energy management perception and consumer awareness and the expected levels for the five dimensions. Table 3 presents the outcomes.

Table 3: Differences in perceptual levels were studied using Servqual

	Features	P	E	Servqual Results "SS" Is the Level of Satisfaction SS = E − P
Knowledge and Awareness of Data Security Practices				
Average Servqual: 0,23				
1	Level of employee cybersecurity knowledge	7	7,35	0,35
2	Knowledge-sharing culture	8	7,86	-0,14
3	Effectiveness of training programs	6	6,42	0,42
4	Awareness of phishing and social engineering threats	8	7,93	-0,07
5	Adoption of best practices for password security	8	8,17	0,17
Organizational Responsibility and Leadership in Data Security				
Average Servqual: 0,35				
6	Commitment from top management	5	5,24	0,24
7	Implementation of formal security policies	6	6,64	0,64
8	Collaboration between IT and other departments	6	5,61	-0,39
9	Security incident response effectiveness	6	6,28	0,28
10	Investment in cybersecurity knowledge development	8	8,19	0,19
Accessibility and Implementation of Security Knowledge				
Average Servqual: 0,21				
11	Availability of cybersecurity resources	7	7,36	0,36
12	Ease of interpreting security policies	8	7,82	-0,18
13	Integration of knowledge management systems (KMS)	8	8,61	0,61
14	Automation of knowledge-based security insights	7	7,39	0,39
15	Use of blockchain for secure knowledge storage	7	6,76	-0,24
Trust and Awareness in Security Technologies				
Average Servqual: 0,66				
16	Perceived reliability of cybersecurity tools	5	6,14	1,14
17	Adoption of emerging security technologies	7	7,67	0,67
18	Trust in automated security processes	8	8,49	0,49
19	Perceived effectiveness of knowledge-based security models	4	3,75	-0,25
20	Security knowledge retention in remote work environments	7	6,28	-0,72
Challenges in Security Knowledge Management				
Average Servqual: 0,43				
21	Gaps in cybersecurity literacy	5	5,11	0,11
22	Resistance to adopting new security protocols	8	8,24	0,24
23	Barriers to knowledge transfer	7	6,18	-0,82
24	Misinformation and cybersecurity myths	5	4,37	-0,63
25	Employee engagement in cybersecurity initiatives	5	4,67	-0,33

A graph was produced based on the Table 3 data, which included the results of the Servqual method of perception and expectancies analysis. Figure 3 depicts the graphical representation of the Servqual method's outcomes.

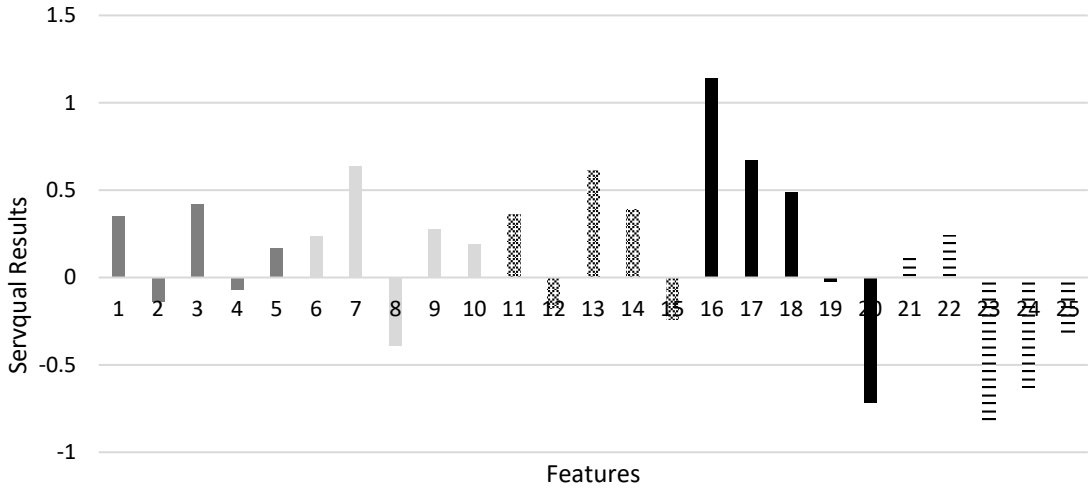

Figure 3: Results of the Servqual analysis

The Servqual analysis of the 25 cybersecurity factors reveals key strengths and weaknesses in knowledge management for data security. Strong areas include high confidence in firewall and intrusion detection systems (Factor 16), effective internal security communication (Factor 7), and the integration of knowledge-sharing platforms (Factor 12), indicating that organizations have successfully established structured mechanisms for security awareness and collaboration. However, critical weaknesses emerge in several areas. Awareness of phishing and social engineering threats (Factor 2) shows a negative gap, suggesting that employees remain vulnerable to cyberattacks due to insufficient training. Collaboration between IT security teams and other departments (Factor 8) also exhibits a deficit, highlighting a lack of interdisciplinary coordination in security management. Additionally, gaps in cybersecurity literacy (Factor 19) and trust in handling security breaches (Factor 25) indicate that many employees do not feel adequately prepared to respond to incidents, which could compromise organizational resilience. Overall, while organizations have successfully implemented security tools and communication strategies, deficiencies in employee awareness, IT collaboration, and breach response capabilities require immediate attention. Strengthening cybersecurity training programs, improving interdisciplinary cooperation, and fostering a more security-conscious workplace culture will be essential to closing these gaps and enhancing knowledge-based data security practices.

Figure 2 illustrates key challenges and concerns related to knowledge management and data security in enterprises. The increasing reliance on digital technologies and cybersecurity frameworks highlights the importance of effectively managing security knowledge within organizations. While enterprises recognize the value of cybersecurity awareness and structured knowledge-sharing mechanisms, several issues persist, including gaps in employee training, resistance to adopting new security protocols, and inconsistencies in knowledge transfer. These challenges impact the overall effectiveness of cybersecurity strategies and increase vulnerability to cyber threats. Figure 2 presents an overview of these factors, emphasizing the need for comprehensive knowledge-based security solutions to enhance organizational resilience. The identification of barriers and challenges in cybersecurity knowledge management has enabled a clearer definition of strategies to enhance security practices within enterprises. Table 1 presents an overview of key areas influencing knowledge management in data security, assessing factors such as employee awareness, organizational responsibility, accessibility of security knowledge, trust in security technologies, and challenges in knowledge transfer. The descriptive statistics for these constructs indicate moderate levels of awareness and implementation of security knowledge within organizations. The mean value for Knowledge and Awareness of Data Security Practices is 3.28, reflecting a need for improved training and education initiatives to enhance employees' understanding of cybersecurity threats and best practices. Similarly, Organizational Responsibility and Leadership in Data Security scored 3.07, suggesting that while leadership acknowledges the importance of cybersecurity, there are gaps in policy enforcement and managerial involvement in knowledge-sharing initiatives. Furthermore, Accessibility and Implementation of Security Knowledge received a mean score of 2.94, indicating challenges in integrating structured security knowledge management systems across enterprises. The Trust and Awareness in Security Technologies score of 2.83 highlights a lack of confidence in automated security solutions such as AI-driven threat detection and blockchain-based security frameworks. Lastly, Challenges in Security Knowledge Management were rated at 2.91, pointing to issues such as resistance to adopting new

security protocols, gaps in cybersecurity literacy, and difficulties in transferring security expertise across teams. These findings emphasize the need for a holistic approach to cybersecurity knowledge management, integrating structured training programs, leadership commitment, and technological innovations to enhance organizational resilience against cyber threats. The initial phase of the study focused on evaluating the perception gaps between expected and experienced levels of knowledge-based data security practices within enterprises. Using the SERVQUAL method, we measured discrepancies across the five key dimensions outlined above. Table 3 presents the results of this analysis by comparing participants' expectations (E) and perceptions (P) for each of the 25 indicators. The SERVQUAL score (SS = E – P) reveals areas where expectations exceeded actual experience, as well as those where organizations performed better than anticipated. For instance, in the Knowledge and Awareness of Data Security Practices dimension, the largest positive gap (+0.42) appeared in the Effectiveness of training programs, suggesting that some organizations surpassed expectations in their employee development initiatives. However, Knowledge-sharing culture (–0.14) and Awareness of phishing and social engineering threats (–0.07) displayed negative gaps, indicating critical areas for improvement in informal knowledge transfer and threat preparedness. In the Organizational Responsibility and Leadership category, the implementation of formal security policies showed a strong positive gap (+0.64), reflecting well-established governance in some enterprises. In contrast, Collaboration between IT and other departments showed a significant negative gap (–0.39), pointing to the need for improved cross-functional coordination. The Accessibility and Implementation of Security Knowledge dimension was mixed, with positive outcomes such as Integration of KMS (+0.61) and Automation of knowledge-based insights (+0.39), but also weak areas like Use of blockchain for secure knowledge storage (–0.24). In the Trust and Awareness in Security Technologies domain, results varied significantly. Although Perceived reliability of cybersecurity tools showed the highest positive gap (+1.14), Security knowledge retention in remote work environments revealed a concerning negative gap (–0.72), highlighting persistent post-pandemic challenges. Lastly, the Challenges in Security Knowledge Management dimension uncovered significant weaknesses. For example, Barriers to knowledge transfer (–0.82) and Misinformation and cybersecurity myths (–0.63) were among the most severe negative gaps, confirming that human and cultural factors continue to hinder secure knowledge dissemination.

5. Discussion and Conclusions

The study demonstrated a strong organizational commitment to cybersecurity knowledge management, emphasizing the growing importance of structured security awareness and knowledge-sharing practices. As enterprises continue to integrate digital security strategies, there is a critical need to enhance knowledge-based cybersecurity frameworks to strengthen resilience against emerging threats. The increasing complexity of cyberattacks necessitates a proactive approach that incorporates structured training, technological advancements, and interdisciplinary collaboration. Organizations must focus on creating an integrated security culture, ensuring that employees at all levels understand best practices, security policies, and incident response protocols. The research findings highlight both progress and challenges in the implementation of cybersecurity knowledge management. The mean score for Knowledge and Awareness of Data Security Practices was 3.28, indicating that while organizations recognize the importance of security knowledge, there is room for improvement in raising employee awareness and providing more effective training programs. Organizational Responsibility and Leadership in Data Security scored 3.07, reflecting a moderate level of managerial commitment but suggesting that top leadership needs to be more actively involved in fostering a security-driven culture. Accessibility and Implementation of Security Knowledge scored 2.94, pointing to difficulties in integrating cybersecurity knowledge-sharing platforms and ensuring that employees can easily access and apply security-related information. Trust and Awareness in Security Technologies received a mean score of 2.83, highlighting skepticism toward AI-driven security monitoring and blockchain-based solutions, which may hinder adoption. Lastly, Challenges in Security Knowledge Management were rated at 2.91, revealing persistent barriers in knowledge transfer, resistance to new security policies, and difficulties in maintaining cybersecurity literacy across different organizational levels. These results indicate that organizations have successfully adopted firewalls, intrusion detection systems, and knowledge-sharing platforms, but significant gaps remain in social engineering awareness, interdisciplinary cooperation, and confidence in handling security breaches. Addressing these weaknesses requires a systematic approach to cybersecurity education, ensuring that employees possess the necessary skills to recognize, mitigate, and respond to threats effectively. The study also underscores the necessity of leadership commitment in driving security initiatives, as management involvement plays a crucial role in fostering a security-conscious workplace culture. Despite these advancements, limitations persist in the widespread adoption of emerging cybersecurity technologies. Employees exhibit skepticism regarding AI-driven security automation and blockchain-based data protection, indicating a need for further education on the

benefits and reliability of these technologies. Additionally, resistance to adopting new security protocols remains a significant challenge, often stemming from a lack of clear communication or inadequate training programs. Future research should explore the long-term impact of cybersecurity training and evaluate how organizations can integrate AI-driven risk assessment tools to enhance security knowledge-sharing processes. The study also identifies broader implications for cybersecurity knowledge management, particularly in the context of regulatory compliance and industry standards. As enterprises navigate complex data protection regulations, ensuring alignment with frameworks such as ISO 27001 and GDPR becomes essential. Future research should focus on assessing the effectiveness of security knowledge transfer in regulatory compliance, as well as the role of cybersecurity literacy in mitigating organizational risks. Longitudinal studies comparing security knowledge adoption across different industries would provide valuable insights into best practices for knowledge-based security implementation. One of the main limitations of this study is the inability to compare data across multiple research periods, which restricts the ability to assess long-term trends in cybersecurity knowledge adoption. Future studies should aim to conduct follow-up assessments within the next few years to track improvements in security knowledge management and identify evolving challenges. Additionally, further qualitative research could provide deeper insights into employee perceptions of cybersecurity training effectiveness and the practical challenges associated with implementing knowledge-based security solutions. By addressing these areas, organizations can develop more robust cybersecurity strategies that integrate both technological innovations and human-centered knowledge-sharing approaches, ultimately fostering a more resilient and security-aware enterprise environment. The study confirms that enterprises need to prioritize structured cybersecurity training, improve leadership engagement, and enhance security knowledge accessibility to effectively mitigate cyber risks and strengthen organizational security resilience.

References

Alavi, M. and Leidner, D.E. (2001), Review: Knowledge Management and Knowledge Management Systems: Conceptual Foundations and Research Issues, *MIS Quarterly* 25: 107.

Almustafa, H. and Kalash, I. (2025), The dynamic relationship between firms' cash reserves and financial leverage: evidence from MENA emerging markets, *JEAS* 41: 414–431.

Corvello, V., Felicetti, A.M., Steiber, A. and Alänge, S. (2023), Start-up collaboration units as knowledge brokers in Corporate Innovation Ecosystems: A study in the automotive industry, *Journal of Innovation & Knowledge* 8: 100303.

Hussain, I., Qureshi, M., Ismail, M., Iftikhar, H., Zywiołek, J. and López-Gonzales, J.L. (2024), Optimal features selection in the high dimensional data based on robust technique: Application to different health database, *Heliyon* 10: e37241.

Khan, S. and Wallom, D. (2022), A system for organizing, collecting, and presenting open-source intelligence, *J. of Data, Inf. and Manag.* 4: 107–117.

Masucci, M., Brusoni, S. and Cennamo, C. (2020), Removing bottlenecks in business ecosystems: The strategic role of outbound open innovation, *Research Policy* 49: 103823.

Pandey, A., Calyam, P., Lyu, Z., Wang, S., Chemodanov, D. and Joshi, T. (2023), Knowledge-Engineered Multi-Cloud Resource Brokering for Application Workflow Optimization, *IEEE Trans. Netw. Serv. Manage.* 20: 3072–3088.

(2023), *Proceedings of the Second International Conference on Electronics and Renewable Systems (ICEARS 2023): 02-04 March 2023, Tuticorin, India*, IEEE, Piscataway, NJ.

Salah, O.H. and Ayyash, M.M. (2024), Understanding user adoption of mobile wallet: extended TAM with knowledge sharing, perceived value, perceived privacy awareness and control, perceived security, *VJIKMS*.

Schiavone, F., Mancini, D., Leone, D. and Lavorato, D. (2021), Digital business models and ridesharing for value co-creation in healthcare: A multi-stakeholder ecosystem analysis, *Technological Forecasting and Social Change* 166: 120647.

Solms, R. von and van Niekerk, J. (2013), From information security to cyber security, *Computers & Security* 38: 97–102.

Suuronen, S., Ukko, J., Eskola, R., Semken, R.S. and Rantanen, H. (2022), A systematic literature review for digital business ecosystems in the manufacturing industry: Prerequisites, challenges, and benefits, *CIRP Journal of Manufacturing Science and Technology* 37: 414–426.

Tarasova, T.M. (2024), Protection of Trade Secrets to Ensure the Economic Security of the Enterprise. In Mantulenko, V.V., Horák, J. and Kučera, J. (Eds.), *Proceedings of the XI International Scientific Conference "Digital Transformation of the Economy: Challenges, Trends and New Opportunities" (ISCDTE 2024)*, *Lecture Notes in Networks and Systems*, Vol. 1064, Springer Nature Switzerland, Cham, pp. 95–102.

Xu, Z., Liu, W., Huang, J., Yang, C., Lu, J. and Tan, H. (2020), Artificial Intelligence for Securing IoT Services in Edge Computing: A Survey, *Security and Communication Networks* 2020: 1–13.

Żywiołek, J. and Abbas, A.A. (2021), Information Security in Information Systems Among Employees of Industrial Enterprises as Societies 5.0, *System Safety: Human - Technical Facility - Environment* 3: 64–70.

Żywiołek, J., Mathiyazhagan, K., Shahzad, U., Zhao, X. and Saikouk, T. (2025), Enhancing cognitive metrics in supply chain management through information and knowledge exchange, *IJLM*.

Żywiołek, J., Rosak-Szyrocka, J., Nayyar, A. and Naved, M. (2024), *Modern Technologies and Tools Supporting the Development of Industry 5.0*, CRC Press, New York.

Żywiołek, J., Trigo, A., Rosak-Szyrocka, J. and Khan, M.A. (2022a), Security and Privacy of Customer Data as an Element Creating the Image of the Company, *Management Systems in Production Engineering* 30: 156–162.
Żywiołek, J., Tucmeanu, E.R., Tucmeanu, A.I., Isac, N. and Yousaf, Z. (2022b), Nexus of Transformational Leadership, Employee Adaptiveness, Knowledge Sharing, and Employee Creativity, *Sustainability* 14: 11607