Digital Transformation Meets Cybersecurity: Managers' Experiences, Challenges, and Performance Implications

Oana Alexandra SARCEA (MANEA)[1]
Alexandra ZBUCHEA[2]

Abstract

This paper investigates the strategic integration of digital transformation (DT) and cybersecurity (CS) as a key driver of business performance. The primary objectives are to examine how the alignment of these two essential business elements influences operational efficiency, competitive advantage, and customer trust. Given a background where security is often secondary to rapid innovation, this research evaluates whether proactive cybersecurity acts as a barrier or a strategic enabler. Methodologically, the study adopts a qualitative approach, utilizing nine in-depth interviews with managers and subject-matter experts from different sectors such as banking, FMCG, and IT, conducted in October 2025. Data analysis was performed using ATLAS.ti software. The results indicate that early integration of cybersecurity into digital initiatives leads to superior organizational outcomes and enhanced risk management. The research concludes that managerial leadership and a "security-by-design" culture are essential for converting digital investments into sustainable competitive advantages within the current technological and regulatory framework.

Keywords: *Digital transformation, Cybersecurity, Managerial perspectives, Organizational change, Business performance, Technology adoption*

JEL classification: M15, O32, L25

DOI: 10.24818/RMCI.2026.1.23

1. Introduction

In the context of business organizations increasingly adopting digital transformation (DT) to enhance efficiency and competitiveness, cybersecurity (CS) has become critical. Many companies accelerate the adoption of digital technologies, but cybersecurity considerations are often addressed belatedly or treated as a compliance-driven necessity rather than an integral strategic component. This raises an important question: is cybersecurity perceived as a barrier that slows innovation, or as an enabler that supports sustainable and resilient digital transformation and

[1] Oana Alexandra SARCEA (MANEA), National University of Political Studies and Public Administration, e-mail: oana.manea89@gmail.com
[2] Alexandra ZBUCHEA, National University of Political Studies and Public Administration, e-mail: alexandra.zbuchea@facultateademanagement.ro

business performance? Moreover, organizations differ in whether they allocate cybersecurity resources proactively as part of their transformation strategy or reactively in response to security incidents. The perception of the direct effect of cybersecurity on organizational performance might also drive a more focused approach to CS within business operations and strategies.

Integrating DT and cybersecurity CS is important for modern organizations aiming to enhance performance and resilience. Alenezi et al. (2023) emphasize that DT offers significant benefits, but also introduces cybersecurity challenges that can impact business resilience and development. Therefore, research is needed to identify how organizations can proactively address these challenges to maintain operational effectiveness and business performance.

This research explores how firms manage the interactions between digital transformation and cybersecurity and examines whether early integration of cybersecurity into digital initiatives leads to superior organizational performance. In particular, the study investigates the relationship between integrated DT-CS strategies and key performance outcomes. It discusses dimensions such as operational efficiency, risk management effectiveness, financial performance, and customer trust and retention. By analyzing managerial perspectives across multiple industries, the study also considers how organizational context, including firm size, structural complexity, and leadership mindset, influences the adoption and alignment of digital transformation and cybersecurity practices to improve business performance.

Based on qualitative research with experienced managers and subject-matter experts, this article explores practical strategies organizations have used to ensure both innovation and security. The insights add value to both academic debate and real-world practice, offering guidance for businesses working to align digital transformation with cybersecurity, as well as for policymakers and regulators seeking to foster secure and sustainable digital innovation.

2. Business Performance Through Digital Transformation, Providing Cybersecurity and Competitiveness

Vial (2019) emphasizes that organizations should adapt their business strategies to the new digital reality, which often involves reconfiguring processes and operations to leverage digital capabilities. This ensures that digital initiatives support overarching business goals and drive value creation. The relationship between DT and organizational performance has been extensively studied in the past years. Rahman et al. (2024) found that effective implementation of DT strategies leads to improvements in staff productivity, job satisfaction, and organizational performance. Their literature review indicates that organizations adopting DT can achieve significant performance growth.

Successful digital transformation requires a complex approach that considers various organizational aspects to achieve desired outcomes (Henriette et al., 2015). Gebayew et al. (2018) identify critical success factors for digital

transformation, such as strong leadership, a clear vision, and a culture that embraces change. These elements are important for organizations to manage digital transformation and implement effective strategies.

A study by Hanelt et al. (2021) provides a review of digital transformation and offers guidelines for future research and practice. The authors suggest that digital transformation programs should be tailored to each organization's specific context, taking into account various factors such as industry dynamics, organizational structure, and existing capabilities. In the context of program management, Ahimbisibwe et al. (2023) examine the role of IT program management in achieving effective digital transformation. The study highlights the importance of effective governance structures, stakeholder engagement, and risk management in the execution of digital transformation programs.

A new dimension of digital transformation has been highly impactful in the past few years: artificial intelligence (AI) has changed the game. Sarcea (2024) explores the complex relationship between AI and CS, outlining how AI both strengthens defensive capabilities and introduces new security challenges. The analysis points to several important developments, including AI-powered threat detection and automated response, while also highlighting emerging challenges such as adversarial AI and privacy issues. Together, these trends show how deeply AI is reshaping the cybersecurity landscape. The paper further contends that continued investment in AI-driven security tools, strong ethical frameworks, improved threat intelligence, and effective human–machine collaboration will be essential to creating secure and resilient digital systems. At the same time, she stresses that these advances must be carefully governed to mitigate new risks and help close the cybersecurity skills gap.

Digital technologies such as artificial intelligence, cloud computing, automation, and data analytics are adopted by businesses to enhance efficiency, productivity, and customer engagement, considering various organizational contexts (Sarcea, Zbuchea, & Pinzaru, 2024). These technologies not only reduce costs and optimize processes but also improve product and service quality, thereby transforming traditional business models to support development and competitive advantage.

Zaman et al. (2025) discuss that digital technologies alone do not directly improve performance. Their positive effect on performance depends on how well they are managed within the organization, including aligning technologies with business goals, optimizing resources, managing change, and stimulating innovation. Management approach mediates the relationship between technology adoption and performance outcomes, indicating that managerial practices are essential for transforming digital investments into positive performance outcomes. This emphasizes the importance of managerial leadership in guiding digital transformation, as managers must develop the capabilities to integrate technologies thoughtfully, adapt organizational processes, and cultivate a culture that supports continuous learning and technological adaptation to achieve efficiency gains and competitive advantage.

These findings are in line with the Orkamo et al. (2025) study, which shows the important role of leadership. The study shows that a mix of behaviors drives performance outcomes, influencing critical performance dimensions such as effective leadership, employee acceptance of digital technologies, development of digital competencies, and digital innovation. They contribute to enhanced organizational performance when appropriately integrated with digital transformation efforts. Interestingly, emotional intelligence is identified as an important attribute that helps leaders be more effective, supporting employees through change and supporting a culture that sustains transformation and performance improvements.

Research indicates that human resource management plays an important role in turning digital transformation into enhanced performance. Chali and Lakatos (2024) found that strategic team management practices are positively associated with financial outcomes in cooperative enterprises. Vogt (2020) showed that high-performance work practices, including employee engagement and merit-based rewards, enhance financial performance. Together, these findings suggest that aligning digital transformation initiatives with strategic human resources management practices and effective team management is essential to maximizing organizational performance while ensuring innovation, productivity, and risk management.

At the same time, Belkhamza (2023) emphasized that digital transformation can boost efficiency and productivity. It also introduces cybersecurity challenges that must be managed to safeguard organizational outcomes. The rapid DT of contemporary businesses has increased their dependence on digital infrastructures, exposing them to a wide range of cyber threats. Consequently, organizations should adopt comprehensive CS measures to protect sensitive data, maintain business continuity, and sustain customer trust. Additionally, understanding the financial impact of cyber incidents helps organizations assess their exposure and prioritize cybersecurity investments.

Integrating digital transformation and cybersecurity brings several significant challenges. Sarcea (2024) highlights cybersecurity as a key driver of digitalization, noting its essential role in protecting sensitive data, managing risks, and strengthening organizational resilience. The study shows that without a strong focus on cybersecurity, organizations may struggle to fully realize the benefits of digital transformation.

CS has become a key component in safeguarding both business and customer information. As cyber risks continue to grow, ranging from ransomware attacks to insider threats, organizations must adopt effective data protection measures to reduce their exposure (Smith, Green, & Carter, 2023). The use of established security standards, such as ISO 27001 and the NIST Cybersecurity Framework, helps organizations align with recognized best practices and improve their overall security posture (Jones & Brown, 2022).

In addition, companies that place a strong emphasis on cybersecurity are better positioned to earn customer trust, an essential factor in preserving brand reputation and long-term customer loyalty (Johnson & Lee, 2021).

A proactive approach to risk assessment plays a critical role in identifying vulnerabilities and addressing cyber risks before they develop into serious incidents (Miller & Davis, 2020). Well-designed incident response plans further support this process by enabling organizations to detect, contain, and recover from security breaches promptly, thereby limiting operational disruption and financial impact (Taylor et al., 2022). Evidence shows that organizations with clearly defined incident response frameworks tend to experience reduced downtime and stronger business continuity following cyberattacks (Garcia & Patel, 2023).

Digital technologies have fundamentally transformed business operations, driving greater efficiency and enabling innovation across industries. At the same time, the integration of technologies such as cloud computing, artificial intelligence, and the Internet of Things (IoT) has expanded the cyber threat landscape and introduced new security challenges (Williams & Carter, 2023). To ensure that digital transformation delivers sustainable value, organizations must implement robust security controls that protect systems and data while supporting operational performance (Nguyen et al., 2022). Firms that successfully address these challenges are better positioned to achieve long-term profitability and maintain a competitive edge (Chen & Zhao, 2021). In this context, cybersecurity investment should be viewed not only as a protective measure but also as a contributor to financial performance, as it helps reduce the costs associated with breaches, downtime, and system failures (Harris et al., 2021).

The relationship between CS and organizational performance is further emphasized by Alenezi et al. (2023), who highlight the importance of appropriate security measures to safeguard digital assets and sustain performance during digital transformation initiatives. However, the adoption of cybersecurity strategies is influenced not only by internal organizational priorities but also by the broader regulatory and policy environment.

Within the European Union, cybersecurity regulations and directives aim to enhance cyber resilience and data protection across member states. However, they can also impose substantial compliance and operational demands on businesses. These frameworks require organizations to adjust internal processes and invest in governance structures to meet regulatory expectations. Despite these challenges, Sarcea, Costea, and Zbuchea (2024) argue that the enforcement of EU cybersecurity standards strengthens firms' risk management capabilities and shapes strategic decision-making. By embedding security considerations into digital operations, organizations can improve trust, resilience, and competitive positioning. As a result, firms that align effectively with EU cybersecurity requirements are more likely to prevent breaches, retain stakeholder confidence, and support sustainable growth through secure digital transformation.

The financial consequences of cybersecurity practices are significant. Strong security measures can help organizations avoid costly data breaches that

often lead to direct financial losses, regulatory penalties, and long-term reputational harm. The Gordon–Loeb model offers an economic perspective on cybersecurity investment, suggesting that firms should invest up to 37% of the expected loss from a potential breach to achieve an optimal level of protection (Gordon & Loeb, 2002). This model highlights the importance of balancing security spending with potential risk exposure. In practice, effective CS requires a comprehensive approach that includes regular risk assessments, employee awareness and training, and the implementation of advanced security technologies. Increasingly, organizations are adopting zero-trust architectures, which require continuous verification of all access requests, regardless of source, thereby strengthening their overall security posture (Scott, 2025).

3. Methodology of the Research

The investigation has two main objectives: (Ob.1) understanding the implementation and impact of digital transformation, with a stress on business performance, and (Ob.2) understanding cybersecurity integration and its influence on organizational performance. Both objectives are important for any business organization that aims to increase performance by safely integrating the latest technological developments.

The first objective identifies strategies for digital transformation, examines specific challenges, and considers how technological adoption influences business models. It also assesses business performance across operational efficiency, customer engagement, competitive advantage, and financial outcomes. The second objective maps cybersecurity approaches and challenges. It also examines the integration of cybersecurity and digital transformation. The third line of investigation is the impact of cybersecurity on performance, competitive positioning, and trust.

Qualitative research is the most appropriate method for ensuring a deep, contextual understanding of the investigated topic and achieving the set objectives. In-depth individual interviews allow managers to explain their experiences, challenges, and approaches freely. Managers often face unique challenges and opportunities, and interviews allow for exploring these in their real-life contexts (Yin, 2018). They allow greater flexibility in exploring the approached theme, with the possibility of discussing uncovered insights. It is especially appropriate since both digital transformation and cybersecurity are highly dynamic and complex phenomena. Individual interviews allow the collection of a rich data set, capturing perceptions, attitudes, and nuanced detail that can be the subject of complex analysis. Piperopoulos (2010) emphasizes the value of qualitative research methods, particularly case study research, in understanding experts and the special role of owner-managers. Thus, semi-structured interviews provide a balance between structure that ensures consistency across interviews and flexibility that allows exploration of emerging themes.

To identify suitable participants for the interview, purposive sampling was considered. Subject-matter expert managers were primarily targeted because they

bring relevant experience and insights. The individual interview format, along with the ethical approach adopted, ensures confidentiality and informed consent, as managers may discuss sensitive business issues (Kvale & Brinkmann, 2015). Nine in-depth interviews with managers and subject-matter experts in digital transformation were conducted in October 2025 (Table 1).

The Participants in the Interviews

Table 1

Participant ID	Industry	Position	Years of managerial experience
I1	Cybersecurity	Expert	20
I2	Banking	Top management	15
I3	FMCG	Middle management	20
I4	Cybercrime	Expert	15
I5	Banking	Middle management	15
I6	Cybersecurity/IT	Top management	15
I7	Automation/IT	Top management	10
I8	Data Science/Automation	Expert	10
I9	Banking	Middle management	20

Source: Authors' own research results.

Before the interview, participants signed a consent form agreeing to the audio/video recording of their interview for the purpose of supporting objective analysis and that the recording would not be shared without prior consent. All personal data will be kept confidential, securely stored, anonymized in publications, and handled in compliance with the GDPR, with the participant retaining the right to access, correct, or request the deletion of their data.

The results were analyzed using ATLAS.ti, a qualitative data analysis tool that offers features for coding, analysis, and visualization. Networks can be built to visualize relationships among concepts, which helps understand complex phenomena such as SME management. ATLAS.ti query tool allows asking questions of coded data, such as identifying co-occurring themes or testing hypotheses (Friese, 2019).

After conducting the in-depth interviews, for analysis purposes, the quotation codes in ATLAS.ti used were: Additional details, Background, Company info, Cybersecurity (CS), Digital Transformation (DT), DT & CS, and Performance (Figure 1).

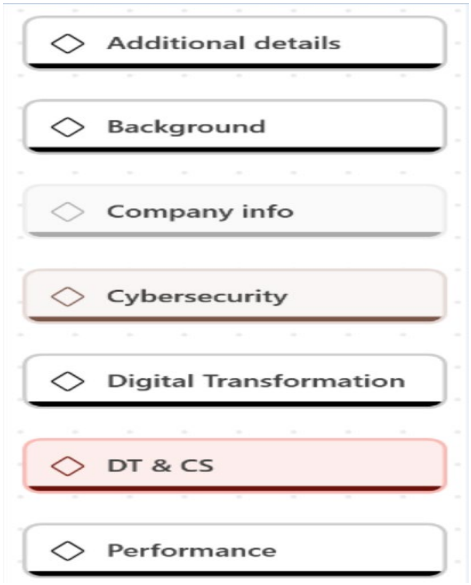

Figure 1. ATLAS.ti Code System
Source: Authors' own research results.

The main quotation codes used for analysing the in-depth interviews are presented in Figure 2. These directly correspond to the central research questions and capture the interviewees' insights on the theme. The DT & CS code was introduced to explicitly capture perspectives addressing the integration, alignment, or tension between digital transformation and cybersecurity. This code is particularly important given the study's objective to explore whether cybersecurity is perceived as an enabler or a constraint within digital transformation strategies, and how early integration of cybersecurity influences organizational outcomes.

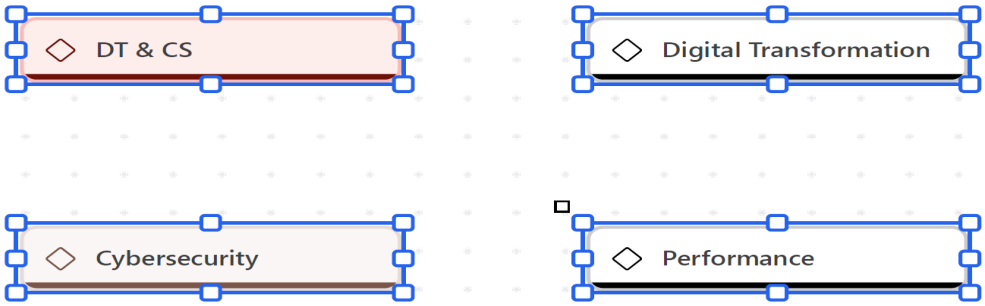

Figure 2. ATLAS.ti Main Codes
Source: Authors' own research results.

After conducting in-depth interviews and coding data into categories such as "Background," "Company Info," "Cybersecurity," "Digital Transformation,"

"DT&CS," and "Performance," the Quotation Manager side helped systematically review and analyze the data, ensuring that insights are well documented and accessible. The quotation manager function in ATLAS.ti displays all the quotations extracted from the dataset. It also allows renaming, modifying, or deleting quotations. Assigning or reassigning codes to specific quotations and adding memos or comments to provide additional context are also part of the function. Filtering and sorting by document, code, author, or creation date, and focusing on specific themes or categories, are included in the filtering and sorting functionality.

4. Findings and Discussions

4.1 The Implementation and Impact of Digital Transformation

The qualitative analysis identified six key concepts related to the digital transformation (DT) paradigm, as illustrated in Figure 3. This paradigm is not viewed merely as a technological upgrade but as a comprehensive shift that inherently includes performance discussions. Some participants (I2, I6, and I7) frame digital transformation as a vehicle for achieving superior organizational outcomes, with the successful integration of technology serving as the primary driver of operational excellence and long-term viability.

One of the central elements of this approach is Business Process Reengineering, which many view as essential for achieving strong performance. Participants note that simply adding digital tools to outdated or inefficient processes rarely produces meaningful results. Instead, organizations need to streamline and optimize their workflows first. This not only eliminates bottlenecks and reduces human errors but also enables the organization to operate more flexibly and accurately.

The approach also relies heavily on Strategic Leadership and Cultural Change. Several respondents emphasize that a management culture of openness is crucial for ensuring that digital initiatives align with broader organizational goals. In this view, strong performance emerges naturally from a culture that encourages innovation and adaptability. Without this mindset at the leadership level, technology adoption tends to remain superficial, limiting benefits such as higher customer engagement or improved financial performance.

Finally, the integration of Emerging Technologies and Data Analytics serves as the technical engine of this paradigm. Several tools, such as AI and real-time data science, allow firms to move from reactive to proactive strategies (I2 and I6). This shift is critical for resilience, enabling organizations to maintain high performance levels even in regulated or volatile environments. By prioritizing the maintenance of legacy systems alongside innovations, managers ensure that the digital transformation journey remains a sustainable process that continuously adds value to the organization.

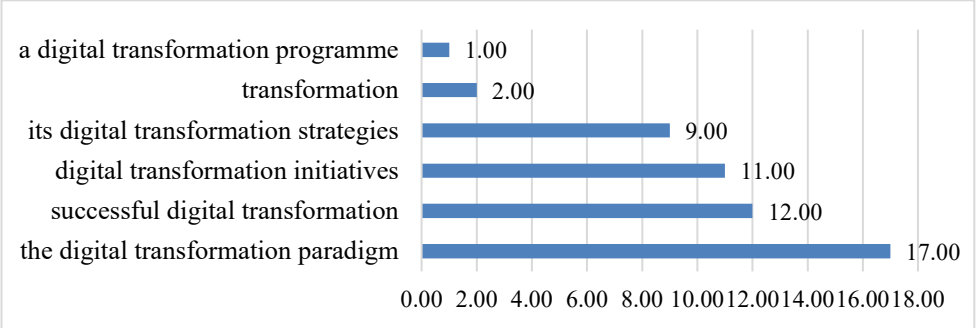

Figure 3. Digital Transformation Highlights in ATLAS.ti
Source: Authors' own research results.

Interviews consider that an effective digital transformation strategy requires integrating technological innovations with business goals to boost performance and competitiveness. They align with Henriette et al. (2015), who highlight that digital transformation means more than technological shifts, impacting business models, operational processes, and customer experiences. Implementing digital transformation programs involves structured initiatives that help organizations transition into the digital age. These programs encompass adopting new technologies, process reengineering, and cultural change management.

The connection between the theoretical framework and the practical elements from the interviews is especially clear when examining the factors that contribute to competitiveness. For instance, technology is seen as a secondary layer that must be preceded by structural and mental shifts: "For me, before any technology is applied, digital transformation involves the process of design thinking and business process reengineering… Digital transformation cannot be achieved without cultural change." (I9) This perspective confirms that the impact on business models and operational processes described by Henriette et al. (2015) is fundamentally rooted in the organization's ability to first redesign its internal logic and culture.

Similarly, the role of leadership in converting digital initiatives into actual business performance, connecting productivity directly to strategic oversight: "Yes, [digital transformation] sits at the core of transforming businesses and productivity... [but] the biggest challenge sits within lack of strategy and initiatives from the management team" (I5). These findings show the practical importance of having a structured approach to digital transformation programs, indicating that even the most sophisticated technologies may fall short of delivering the anticipated competitive advantage and performance improvements without an active and strategic management team.

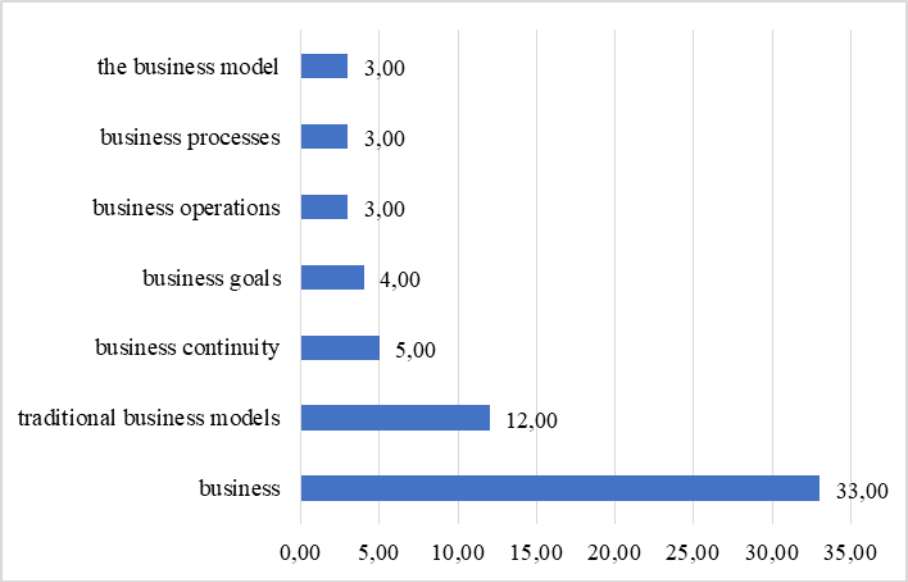

Figure 4. DT and BUSINESS Correlations Identified in ATLAS.ti
Source: Authors' own research results.

Business models show how an organization creates, delivers, and captures value. Traditional business models rely on established frameworks, in which value is generated through the production and distribution of goods or services in a linear supply chain. They are focused more on preserving existing processes and resources (Niemimaa et al., 2019).

How these traditional business models work in the context of digital transformation is of high concern among the respondents, who emphasize that the shift is no longer optional but a matter of survival. For instance, some interviewees pointed out that in highly regulated sectors like banking, the traditional model, once centered on physical infrastructure and face-to-face interaction, is being radically replaced by "platform-centric" models. In this new logic, value is captured through 24/7 digital accessibility and the ability to offer personalized services based on real-time data, rather than through the mere preservation of existing resources.

This evolution is further detailed by participants, who observed a significant shift from "product-centric" to "service-oriented" business models. In their view, digital transformation enables companies to move beyond linear distribution of goods toward capturing value through continuous, data-driven insights and predictive maintenance. This suggests a necessary modification of the business model where the value proposition is no longer a static product, but a dynamic, interconnected service. Such a transition requires organizations to rethink their revenue streams, moving from one-time transactions to subscription-based or usage-based models that leverage the constant connectivity of digital assets.

However, participants observed that the success of these modifications is intrinsically linked to organizational agility. The experts suggest that for a traditional business model to adapt successfully, it must transition into a "digital ecosystem" where value is co-created with customers through continuous feedback loops. This proposed modification requires a departure from the rigid, linear supply chain toward a more networked approach, allowing firms to manage the risks associated with market volatility. Consequently, respondents agree that a truly transformed business model is one that prioritizes digital scalability and integrates cybersecurity as an enabler of trust, ensuring that the value captured is both sustainable and resilient.

Participants in the interviews consider that business continuity in the digital age is inseparable from the proactive adaptation of these models. One participant stresses that structural and cultural readiness is a prerequisite for value creation: “For me, before any technology is applied, digital transformation involves the process of design thinking and business process reengineering… Digital transformation cannot be achieved without cultural change.” (I9) This reinforces the idea that modification is not just technical, but a fundamental shift in organizational logic. The strategic importance of this evolution is further highlighted: “[digital transformation] sits at the core of transforming businesses and productivity,” (I5). Together, these insights validate the need for an evaluative approach. Management must actively lead the evolution of the business model to ensure it remains resilient and able to capture value in a volatile digital landscape.

Additionally, participants emphasized that adopting suitable business models influences an organization’s long-term viability, with digital maturity a critical factor for survival. This view aligns with the argument of Lester et al. (2003) that organizations need to move beyond traditional approaches to remain competitive, requiring a reassessment of their current position in the organizational life cycle. Some participants further highlighted that companies that fail to innovate their business models risk becoming obsolete as they progress through the later stages of the life cycle (I2 and I6). Overall, the participants agreed that sustained performance and longevity are achievable only when organizations actively transition from rigid structures to agile, digitally integrated models capable of navigating the challenges of today’s economy.

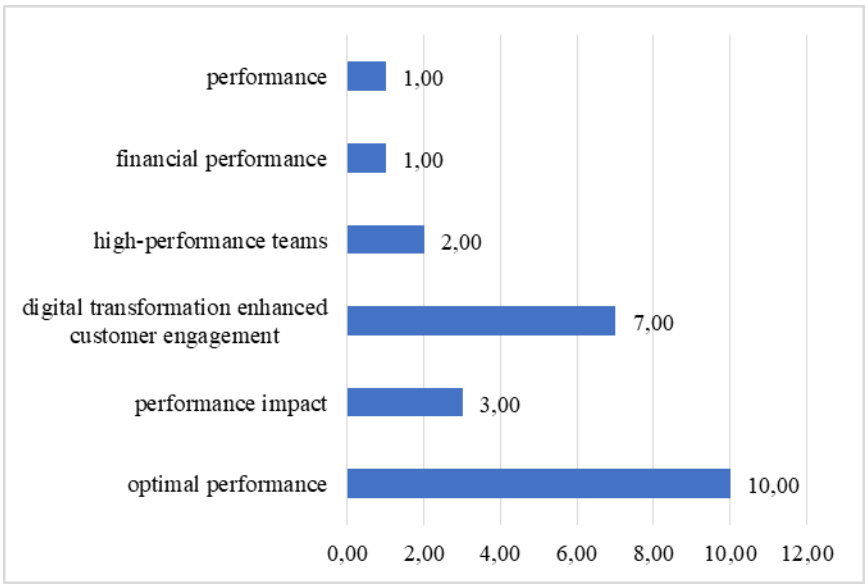

Figure 5. Performance Dimensions Identified in ATLAS.ti
Source: Authors' own research results.

Six main concepts were extracted for the analysis in Figure 5. These concepts suggest that in the modern business environment, performance is no longer measured solely by financial output, but by the organization's ability to maintain digital resilience and stakeholder trust. Respondents framed cybersecurity not as a cost center, but as a strategic element that protects the value created through digital transformation.

The findings indicate that Operational Continuity and Risk Mitigation are the most direct links to performance and cybersecurity. “Yes, [cybersecurity] sits at the forefront of my day-to-day and leads the decisions I have to make... ensuring our processes are not impacted, and business functions smoothly.” (I5) This perspective highlights that performance is inherently tied to the absence of disruptions. A secure environment allows the organization to focus on growth and innovation without the threat of large operational losses.

Furthermore, the concepts of Customer Trust and Competitive Positioning emerged as drivers for long-term sustainability. The interviews revealed that a "security-by-design" approach directly influences a firm's market reputation. Technology is important, but the true impact on performance comes from the discipline of human and procedural factors: “Cybersecurity is mostly in following the strict development lifecycle... managing legacy solution, maintenance, support, and making cost-conscious prioritization decisions.” (I9). This highlights that strategic performance is achieved when cybersecurity is integrated into the very fabric of the organizational culture, ensuring that the company remains resilient against evolving threats while maintaining its competitive edge.

Customer-oriented strategies are identified by respondents as beneficial for organizational performance, supporting other studies that play a crucial role in financial success. The interviews confirm that customer-oriented strategies are no longer just about service quality, but about the seamless integration of digital accessibility and security. Respondents view the digital experience as the primary context for value creation, where performance is directly measured by the organization's ability to meet evolving consumer expectations in a secure environment. Some participants particularly highlighted that in the financial sector, a customer-oriented approach necessitates a transition from traditional physical interactions to robust digital platforms that prioritize user convenience and data protection.

"Yes, it [digital transformation] sits at the core of transforming businesses and productivity, in particular in an organization which places clients' needs at its forefront." (I5) This insight demonstrates that for the interviewed managers, financial success and productivity are natural outcomes of a strategy that uses technology to simplify and secure the customer journey. Furthermore, interviewees noted that gaining valuable consumers' insights through digital platforms is what eventually results in "higher revenues and better customer satisfaction" (I3), effectively closing the loop between a customer-centric mindset and tangible organizational performance.

Participants argue that the technical success of any digital initiative is predicated on the quality and cooperation of the people involved. The role of leadership in developing high-performance teams to drive strategic change suggests that financial resilience is a direct result of how human capital is managed and motivated. These experiences and opinions are aligned with Chali and Lakatos (2024) and Vogt (2020) studies, showing the connection between proper management of human resources, high-performance teams, and financial performance.

There are also explicit links between the effectiveness of cybersecurity and digital processes to human discipline and continuous professional development: "Cybersecurity does not start with technology… Human factors are the most important factor." (I9) Therefore, long-term performance is not just a matter of purchasing software, but of fostering a culture where experts and managers collaborate effectively. By investing in subject-matter experts and addressing change resistance, organizations ensure that their human resources become a strategic asset rather than a barrier, ultimately securing the firm's competitive positioning and operational efficiency.

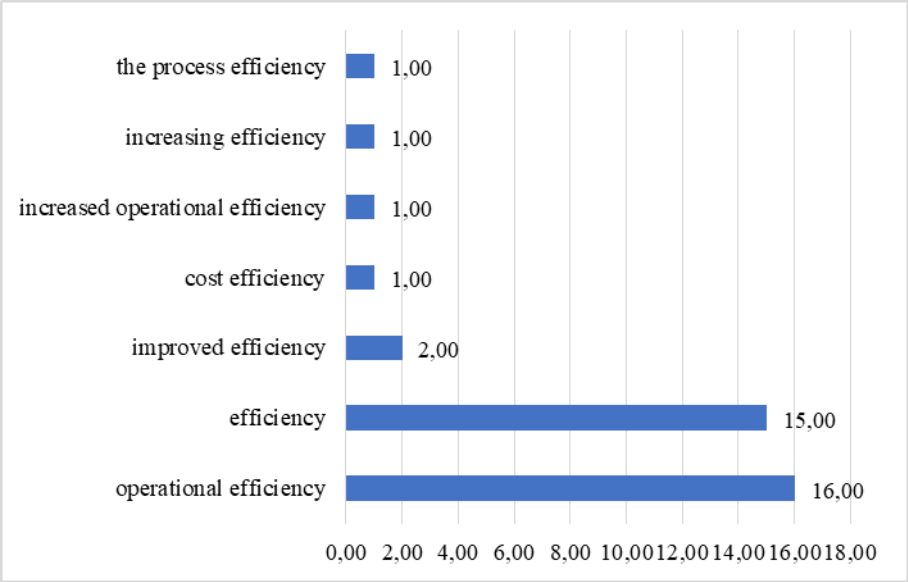

Figure 6. DT-Performance-Efficiency Correlations Identified in ATLAS.ti
Source: Authors' own research results.

Seven correlations were extracted regarding the Efficiency sub-section of the Performance section (Figure 6). The respondents framed efficiency as a direct result of streamlining operations and the strategic use of technology.

A primary driver identified was the transition from manual to automated processes to minimize human error. “It means leveraging advanced technologies like IoT, AI, and data analytics to optimize manufacturing processes, enhance productivity, and drive innovation in industrial operations.” (I8) By automating these workflows, organizations achieve a level of precision and speed that traditional models cannot.

Discussions show that efficiency was strongly correlated with Operational Continuity. The experts noted that a process is only truly efficient if it remains uninterrupted by external threats and that linked security governance is essential to the smooth functioning of business units. I5 states that companies have to “...ensure our processes are not impacted and business functions smoothly.” I3 highlights that digitalization translates into "finding ways to simplify how we operate, by streamlining business processes." These findings suggest that the most efficient organizations are those that successfully connect digital tools with a "security-by-design" mindset, enabling a scalable business model in which increased output does not lead to greater risk.

4.2 Cybersecurity and organizational performance

In an era of escalating cyber pressures, businesses must assume strong cybersecurity measures to safeguard their digital assets, ensure business continuity, and

maintain customer trust. Effective incident response plans, risk assessment, and data protection strategies are essential for facing financial and operational risks, according to the interviews. Additionally, organizations that consider cybersecurity along with their digital transformation efforts can enhance efficiency, innovation, and profitability, thereby ensuring a sustainable competitive advantage in the digital economy (Figure 7). The Quotation Manager figure was broader, but we extracted the most used ones. The other key concepts will be extracted and analyzed later in this report through sections and subsections.

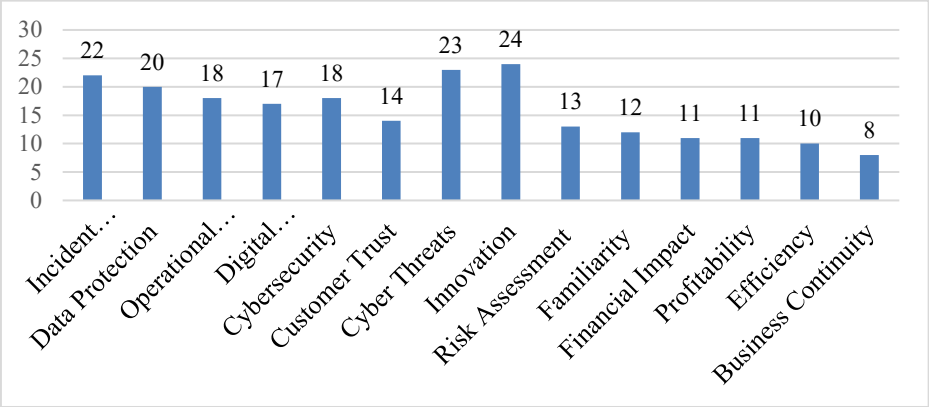

Figure 7. Most Frequently Quoted Cybersecurity and Performance Concepts from ATLAS.ti Analysis

Source: Authors' own research results.

Initially, 15 of the main quotations were extracted, but four were merged: "Cybersecurity Threats" with "Cyber Threats", and "Performance-Innovation" with "DT-Innovation", so now we totalize 13 main quotations (key words). We can observe specific terms in the Cybersecurity area, as well as in Business and Digital Transformation, along with Performance concepts. An incident response plan, along with data protection from CS's side, operational efficiency and profitability from Performance's side, and innovation from DT's area, are the most powerful highlights. Key words extractions by section and correlations with the main concepts (DT, CS, P) will be explored in the next sub-section.

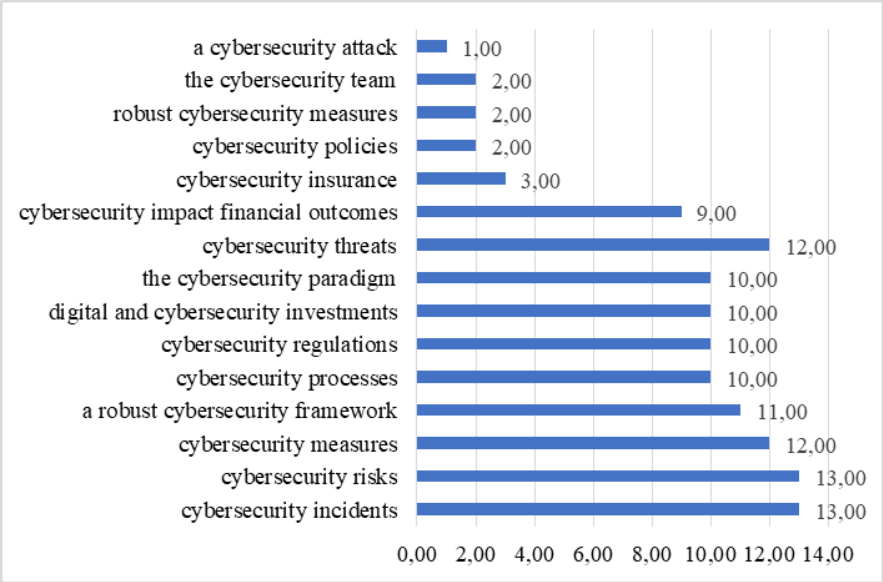

Figure 8. Cybersecurity Dimensions Highlighted in ATLAS.ti
Source: Authors' own research results.

Out of 16 main concepts extracted from the Cybersecurity area after conducting in-depth interviews, we decided to proceed with 15 of them, as two were merged: "the most significant cybersecurity threats" was merged with "cybersecurity threats". Incidents, risks, and measures, as well as a robust cybersecurity framework, were the most commonly used key concepts. Cybersecurity processes and regulations, along with the digital investments, were also highlighted during the review of the extracted and analyzed data.

The qualitative analysis of the Cybersecurity area revealed a paradigm shift in which security is no longer viewed as a purely technical barrier but as a fundamental element of business resilience. The 15 core concepts identified, ranging from threat management to regulatory compliance, suggest that an effective security posture is now a primary indicator of organizational health. Participants consistently emphasized that as digital footprints expand, the complexity of managing incidents and risks grows proportionally, requiring a shift from a reactive to a proactive approach.

A central theme in these discussions was the integration of security into the very core of business operations. "[Cybersecurity] sits at the forefront of my day-to-day and leads the decisions I have to make... ensuring our processes are not impacted and business functions smoothly." (i5) This highlights that for modern managers, security is the "guardian" of productivity, where the primary goal is the preservation of operational continuity against an increasingly sophisticated threat landscape.

Furthermore, the interviews show that technology alone is insufficient without the discipline of standardized processes and human expertise. Effective security is rooted in the lifecycle of the systems themselves: "Cybersecurity is mostly in following the strict development lifecycle... managing legacy solution, maintenance, support, and making cost-conscious prioritization decisions." (I9) This indicates that digital investments must consider acquiring new technologies and rigorously maintaining existing ones. Consequently, respondents' consensus is that a truly secure organization is one that harmonizes regulatory compliance with a strong internal security culture, ensuring that value is protected at every level of the digital ecosystem.

Interestingly, several respondents noted the emergence of cybersecurity insurance as a strategic tool for risk transfer. Although relatively new in the local market compared to the United States, it is increasingly seen as a necessary layer of financial protection. Participants suggested that having cyber insurance not only covers potential losses from ransomware and data breaches but also acts as a catalyst for improving internal security standards, as insurers often require a baseline level of maturity before providing coverage.

Additionally, respondents are concerned about regulations and policies. Regulations aim to standardize cybersecurity practices, ensuring organizations implement adequate safeguards against evolving cyber threats. Respondents view regulations not merely as a legal burden, but as a critical framework for standardizing security and ensuring business survival. While they acknowledge that mandates like NIS2 or GDPR provide a necessary baseline, they emphasize that true performance comes from integrating these rules into the organizational culture rather than just "checking a box."

The interviewees highlighted that the real challenge lies in the disciplined execution of these policies. “Cybersecurity is mostly in following the strict development lifecycle... managing legacy solution, maintenance, support and making cost-conscious prioritization decisions.” (I9) This suggests that regulations serve as a strategic guide for resource allocation. Similarly, I5 views policy adherence as a prerequisite for operational stability, stating that it “leads the decisions I have to make... ensuring our processes are not impacted and business functions smoothly.” Ultimately, for the participants, a strong regulatory system is what transforms cybersecurity from a technical requirement into a reliable enabler of trust and longevity.

The perceived risks identified by interviewees focus on the systemic disruption of business functions and the erosion of trust. Beyond technical glitches, respondents are primarily concerned with sophisticated threats like ransomware and the vulnerabilities inherent in "legacy" systems. These managerial practices directly support Aven’s (2016) recommendation that risk assessment be a driver of better decision-making. I9 supports this by noting that resilience comes from “making cost-conscious prioritization decisions” regarding maintenance and support. By integrating risk evaluation into their daily operations, the participants

ensure their organizations remain adaptive and maintain continuity in an increasingly uncertain digital environment.

Figure 9. Concepts Cloud ATLAS.ti web
Source: Authors' own research results.

The view in ATLAS.ti web is an accumulation of the keywords used in the in-depth interviews, without any AI codes applied (only based on the raw data). Figure 9 shows that respondents place the highest importance on cybersecurity, which is closely connected to business risks.

5. Conclusions

The qualitative analysis reveals that digital transformation and cybersecurity are no longer disparate technical functions but are deeply integrated into the core of organizational performance. Managers do not see digital transformation as pure technology, but as an engine for sustainable performance. The insights gathered from experts and managers demonstrate that a successful business model in the digital age must be fluid, going from rigid structures to agile ecosystems where value is co-created and protected simultaneously. Process reengineering is fundamental for achieving significant results and further adoption of digital innovation.

The findings show that human capital remains the most important variable; without a shift in organizational culture and the development of high-performance teams, even the most advanced digital investments fail to deliver their full potential. Both leadership and organizational culture contribute to the valorization of digital technologies and to an effective and safe digital transformation.

Furthermore, efficiency is redefined through the lens of resilience, true operational speed is only achieved when processes are both automated and secured against disruption. The study validates that risk-based decision-making and regulatory compliance serve as the guardians of longevity. As articulated by the participants, the path to sustainable performance lies in harmonizing innovation with a "security-by-design" mindset, ensuring the organization remains competitive, trustworthy, and resilient in an increasingly volatile global landscape.

References

1. Alenezi, M., Tarhini, A., Masa'deh, R. & Alalwan, A., 2023. *Digital transformation and cybersecurity challenges for business resilience: issues and recommendation*s. *Sensors,* 23(15), p.6666. https://doi.org/10.3390/s23156666
2. Belkhamza, Z., 2023. Cybersecurity in Digital Transformation Applications: Analysis of Past Research and Future Directions. *International Conference on Cyber Warfare and Security,* 18(1), pp.19-24. https://doi.org/10.34190/iccws.18.1.1005
3. Chali, B. D. & Lakatos, V., 2024. The impact of human resource management on financial performance: A systematic review in cooperative enterprises. *Journal of Risk and Financial Management*, 17(10), art. 439. https://doi.org/10.3390/jrfm17100439
4. Chen, L. & Zhao, M., 2021. Digital transformation and cybersecurity: a balancing act. *Journal of Business Technology*, 29(2), pp. 112-128.
5. Friese, S., 2019. *Qualitative Data Analysis with ATLAS.ti* (3rd ed.).
6. Garcia, R. & Patel, S., 2023. Business continuity strategies in cybersecurity frameworks. *Information Security Review*, 18(1), pp. 22-39.
7. Gordon, L. A. & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security (TISSEC),* 5(4), pp. 438-457.
8. Harris, T., Li, X. & Kim, J., 2021. The economic impact of cybersecurity investment on business performance. *Journal of Risk Management*, 12(4), pp. 78-95.
9. Henriette, E., Feki, M. & Boughzala, I., 2015. The Shape of Digital Transformation: A Systematic Literature Review. In *Proceedings of the 9th Mediterranean Conference on Information Systems* (pp. 431-443). AIS. https://aisel.aisnet.org/mcis2015/10/
10. Johnson, K. & Lee, P., 2021. Consumer perception of cybersecurity and its impact on brand trust. *Journal of Consumer Research*, 27(3), pp.89-105.
11. Jones, R. & Brown, A., 2022. Cybersecurity frameworks: Adoption and effectiveness in enterprise settings. *Security & Compliance Review*, 9(2), pp. 33-51.
12. Kvale, S. & Brinkmann, S., 2015. *Interviews: Learning the Craft of Qualitative Research Interviewing* (3rd ed.). Sage Publications.
13. Miller, D. & Davis, W., 2020. *Risk assessment methodologies for cyber threats*. Journal of Information Security, 16(2), pp. 55-73.
14. Nguyen, A., Patel, R. & Thompson, S., 2022. Cyber resilience in digital transformation strategies. *Business and IT Journal*, 22(5), pp. 120-138.
15. Niemimaa, M., Heikkilä, M. & Heikkilä, J., 2019. Business continuity of business models: Evaluating the resilience of business models for contingencies. *International Journal of Information Management*, 46, pp. 149-160.

16. Orkamo, M., Ukko, J., Rantala, T. & Saunila, M., 2025. Leadership behaviours to promote organisational performance in private sector digital transformation - A systematic literature review. *Digital Business*, 100155.
17. Piperopoulos, P., 2010. Qualitative research in SMEs and entrepreneurship: A literature review of case study research. *International Journal of Economics and Business Research*, 2(6), pp. 494-509.
18. Rahman, A. A., Esa, Y. N. E. & Ahmad, N. A., 2024. The Effectiveness of Digital Transformation on Organizational Performance: A Literature Review. *International Journal of Entrepreneurship and Management Practices*, 7(25), pp. 215-224. https://doi.org/10.35631/IJEMP.725018
19. Sarcea, O.A., 2023. How digital transformation and cybersecurity affect companies' performance? In: F. Anghel, B. Hrib, A. Mitan, V. Stoica and A. Zbuchea (eds.), *STRATEGICA. Managing Business Transformations during Uncertain Times*. Bucharest: Tritonic Publishing. https://doi.org/10.25019/STR/2023.039
20. Sarcea, O.A., 2024. Artificial intelligence & cybersecurity – connection, impacts, way ahead. In: *Proceedings of the International Conference on Machine Intelligence & Security for Smart Cities (TRUST)*, vol. 1, pp. 17-26.
21. Sarcea, O.-A., Costea, A.M. & Zbuchea, A., 2024. Examining the EU Policies and Corporate Relations Through a Cybersecurity Lens. *Europolity: Continuity & Change in European Governance, 18*(2).
22. Sarcea, O.A., Zbuchea, A. & Pinzaru, F., 2024. Mapping organizational performance using digital technologies. In: *Proceedings of the International Conference on Business Excellence* (Vol. 18, No. 1, pp. 3530-3542). Sciendo.
23. Scott, M. (2025). *ESG Watch: Companies 'complacent about cybercrime', despite rise in risk from AI*. Reuters, Sustainability, Sustainable finance reporting.
24. Shah, S. H. A., Shah, S. M. A. & Khan, Z., 2019. Impact of customer-oriented strategy on financial performance with mediating role of HRM and innovation capability. *Journal of Business & Economics*, 11(1), 1-20. https://doi.org/10.34260/jaebs.111.1
25. Smith, J., Green, L. & Carter, M., 2023. *Data protection in the age of increasing cyber threats*. Cybersecurity & Privacy, 10(1), pp. 41-58.
26. Taylor, B., Wilson, J. & Adams, C., 2022. *Incident response planning: Best practices for minimizing cyber risk*. Risk Management Journal, 14(3), pp. 72-88.
27. Vial, G., 2019. Understanding Digital Transformation: A Review and a Research Agenda. *Journal of Strategic Information Systems*, 28(2), pp. 118-144. https://doi.org/10.1016/j.jsis.2019.01.003
28. Vogt, S. (2020). The financial impact of high-performance work practices. *Contemporary Management Research,* 16(4), pp. 245-268. https://doi.org/10.7903/cmr.19623
29. Williams, M. & Carter, D., 2023. Operational efficiency and cybersecurity in cloud computing environments. *Journal of Digital Security*, 19(4), pp. 88-102.
30. Yin, R. K., 2018. *Case Study Research and Applications: Design and Methods* (6th ed.). Sage Publications.
31. Zaman, S. A. A., Vilkas, M., Zaman, S. I. & Jamil, S., 2025. Digital technologies and digitalization performance: the mediating role of digitalization management. *Journal of Manufacturing Technology Management*, 36(2), pp. 307-333.