ABSTRACT

In recent times, digital transformation and cybersecurity have become important aspects for the success of organizations. With a constant increase in cybersecurity incidents and growing pressure on organizations to adopt digital technologies, organizations have an increased need to explore in depth how they interact and specifically affect organizational outcomes. Existing literature offers varied perspectives on the concepts of cybersecurity and digital transformation, but remains insufficiently researched within organizations when it comes to the influence of these factors on company performance.

The present doctoral thesis investigates the complex relationships between digital transformation, cybersecurity, and organizational performance within private companies operating in Romania, situating the analysis within the broader context of European regulatory frameworks and the emerging relevance of Big Data analytics. The importance of this topic lies precisely in addressing an evident gap in the literature, providing an integrated analysis of domains that have previously been treated predominantly in isolation. As digitalization increasingly permeates organizational processes, strategies, and business models, understanding the link and balance between technological innovation, information security, and legal regulatory compliance has become critical for both academia and professionals. The research is designed to provide a comprehensive and interdisciplinary perspective on how technological and security-related initiatives, when effectively managed and aligned with EU regulatory requirements, can enhance the organizational resilience, operational efficiency, and strategic performance of companies.This doctoral research endeavor is motivated by the need to acquire a deeper understanding of the long-term impact that technological and security-related decisions exert on organizational performance. Digital transformation has emerged as a major driver of organizational competitiveness and sustainability, often encompassing the adoption of advanced technologies, the redesign or recalibration of internal business processes, and the cultivation of an organizational culture oriented toward digitalization and automation. Organizations that fail to integrate digital capabilities risk becoming irrelevant in markets already undergoing rapid evolution. However, while digitalization offers countless opportunities for better efficiency, higher degrees of innovation, and broader market expansion, it simultaneously increases risk through exposure to cyber threats, data breaches, or operational disruptions. In this context, cybersecurity is no longer a purely technical or defensive concern; it has become a strategic enabler that safeguards organizational assets, fosters stakeholder

trust, and ensures business continuity.Furthermore, the European Union, through initiatives such as GDPR, NIS2, and DORA, has established a complex regulatory environment to which organizations must adapt during their digital transformation. Compliance with these frameworks entails not only legal obligations but also shapes strategic decision-making, data governance, and the integration of emerging technologies, such as Big Data analytics. Consequently, this research investigates how digital transformation, cybersecurity practices, Big Data capabilities, and EU regulatory compliance interact to influence organizational performance, encompassing both tangible outcomes, such as financial and operational performance, and intangible outcomes, such as reputation, trust, and innovation capacity.The architecture of this research is guided by five fundamentally and structurally interconnected objectives, designed to provide an overview of the phenomena studied. The first objective aims to rigorously evaluate the impact that digital transformation initiatives exert on global organizational performance. The second seeks to determine the influence of cybersecurity capabilities on corporate resilience and operational outcomes. Subsequently, the endeavor focuses on analyzing the contribution of Big Data analytics to grounding the decision-making process and obtaining a sustainable competitive advantage. Finally, the research examines the strategic implications of European Union regulatory frameworks on digital and security policies, culminating in the development and validation of an integrated model capable of explaining the causal mechanisms through which these factors interact in shaping business success. To ensure methodological rigor, these general objectives are operationalized through three central research questions articulated around distinct thematic cores. The first question explores the extent to which the digital transformation process reconfigures and strains the cybersecurity defense systems of organizations. The second line of investigation evaluates the direct impact of information security investments on organizational performance indicators. Lastly, the third question aims to identify and rank the structural elements essential for designing a resilient and efficient cybersecurity framework tailored to the specific needs of entities undergoing technological transition.The theoretical foundation of this research draws perspectives from multiple areas of literature. Digital transformation is conceptualized as a socio-technical process that integrates technology adoption with organizational strategy, process optimization, and cultural change. Insights from the qualitative phase revealed that while advanced technologies, such as AI, IoT, and data analytics, are central to transformation efforts, human, organizational, and regulatory factors are equally critical, confirming that digital transformation is a multidimensional, strategic phenomenon. Cybersecurity is positioned as both a strategic and operational imperative that allows organizations to manage risks, protect intellectual property, maintain

operational resilience, and preserve stakeholder trust. Effective cybersecurity requires technical protection measures, formal policies, incident response mechanisms, and employee awareness programs. In the context of SMEs, managerial decision-making is influenced by resource constraints, evolving threats, and regulatory pressures. Big Data analytics is framed as an enabler of both digital transformation and cybersecurity, supporting informed decision-making, predictive insights, and proactive risk management. Regulatory compliance, particularly within the European context, is treated as both a constraint and an opportunity, shaping organizational behavior, risk management, and the strategic implementation of digital initiatives. The conceptual model integrates these constructs, hypothesizing direct, indirect, and mediating relationships among digital transformation, cybersecurity, Big Data, EU compliance, and organizational performance.Methodologically, the study adopts a mixed-methods research design that integrates qualitative and quantitative analysis techniques to provide a comprehensive understanding of the investigated phenomena. The research begins with a systematic review of the academic literature, aimed at clarifying the conceptual foundations of digital transformation, cybersecurity, and organizational performance, as well as identifying theoretical inconsistencies and insufficiently explored relationships among these constructs. This stage is complemented by a bibliometric analysis conducted using VOSviewer, which maps the intellectual structure of the relevant research fields. The bibliometric results identify dominant research themes, influential publications, and leading authors, while also revealing the evolution of research interest and the degree of convergence over time between digital transformation and cybersecurity studies. However, as an inherent limitation, the bibliometric analysis relied primarily on publications indexed in Scopus, potentially excluding relevant contributions from non-English sources or industrial reports (white papers).The qualitative stage of the study involved nine in-depth semi-structured interviews with managers and SME representatives from various economic sectors. Participants were purposefully selected based on their professional experience, expertise in digital transformation or cybersecurity, and organizational context, ensuring diverse perspectives and comprehensive coverage. The interviews were conducted through face-to-face meetings, telephone conversations, and email correspondence (which constitutes a methodological limitation due to the variation in collection formats), and the resulting data were analyzed using ATLAS.ti to identify recurent patterns, emerging themes, and interrelationships. The qualitative findings indicated that digital transformation is recognized as a multidimensional phenomenon involving technology adoption, process optimization, strategic leadership, and cultural adaptation. Managers highlighted the critical role of cybersecurity measures and regulatory compliance in successfully implementing digital initiatives, confirming that digital

transformation is a socio-technical and strategically embedded process. The insights derived from this phase grounded the development of the quantitative survey instrument, the operationalization of the key constructs, and the refinement of the conceptual model.The quantitative stage utilized a structured questionnaire distributed to a sample of 125 private companies in Romania. The survey captured both respondent demographics and organizational characteristics, as well as measures regarding digital transformation, cybersecurity practices, Big Data analytics, EU regulatory compliance, and organizational performance. The constructs were operationalized using reflective items developed based on the literature and qualitative insights, ensuring content validity and contextual relevance. Data were analyzed using Partial Least Squares Structural Equation Modeling (PLS-SEM) in SmartPLS 4.0. The measurement model was rigorously evaluated for reliability and validity using Cronbach's Alpha, Composite Reliability, Average Variance Extracted (AVE), the Fornell-Larcker criterion, and the Heterotrait-Monotrait ratio (HTMT). All constructs demonstrated strong internal consistency, convergent validity, and discriminant validity, supporting the robustness of subsequent structural analyses. The model proved to be statistically robust, registering optimal fit indices. The collected empirical results demonstrate that the proposed conceptual model possesses moderate to strong explanatory power, accounting for 24.4% of the variance in Digital Transformation, 27.9% in Cybersecurity, and 43.6% in Company Performance.

A central conclusion of the study is that Digital Transformation acts as a key driver of Company Performance (confirming hypothesis H1). The digitalization of processes, combined with the integration of data-driven decisions and automation, leads to superior operational efficiency and increased market responsiveness. Hypothesis H2 was also confirmed, revealing that mature cybersecurity does not represent merely a defensive barrier or a cost, but a direct strategic enabler of performance and business partner trust.Regarding Big Data capabilities, the results validated hypothesis H3 and partially H4, confirming that these analytical competencies are essential for the success of Digital Transformation and contribute significantly to the effectiveness of Cybersecurity, providing support for proactive risk management. The influence of EU regulatory compliance (H5) was validated as a major structural determinant. Alignment with regulations exerts a positive and highly significant influence on both Digital Transformation and Cybersecurity. This finding provides an important counter-narrative to the criticisms raised by major technology companies (Big Tech), demonstrating that European regulations (GDPR, NIS2, DORA, DSA) do not block innovation, but rather institutionalize best practices and create an equitable competitive advantage for smaller actors, such as SMEs.The mediation hypothesis H6, which proposed that Big Data and EU regulations mediate

the relationship between Digital Transformation, Cybersecurity, and Company Performance, was partially supported. The indirect effects indicate that both constructs have significant mediating roles, intensifying the pathways through which technology translates into measurable results; specifically, the indirect relationships and show that organizations that extract value from data and adhere to EU standards achieve superior financial and operational results.

Conversely, insufficient maturity in cybersecurity amplifies the negative consequences of digitalization, exposing organizations to operational disruptions, financial losses, and reputational risks. At the same time, the findings allow for the identification of both the benefits and limitations of digital transformation within the context of cybersecurity requirements and contribute to the validation of the proposed model. Organizations that integrate cybersecurity considerations into their digital transformation strategies achieve superior performance outcomes and manifest greater resilience against cyber threats. Based on the combined results of the bibliometric and empirical analyses, the thesis develops and empirically validates a structural and conceptual model that explains how digital transformation and cybersecurity interact to influence organizational performance, thereby extending existing theoretical frameworks in the fields of information systems and organizational studies.

The study recognizes a series of important methodological limitations. From a temporal standpoint, the qualitative phase was conducted between August and October 2024, whereas the quantitative phase took place in July 2025, which might have overlooked interim changes in dynamics. Furthermore, the use of cross-sectional data restricts the ability to infer strict long-term causal relationships, making longitudinal designs highly recommended for future research. The reliance on self-reported data may introduce a social desirability or perceptual bias, an element that could be corrected in future studies by integrating objective financial metrics or external audits. Likewise, the geographical specificity (focusing on companies in Romania/UE) limits the direct transferability of the results to regions with different levels of institutional maturity (such as North America or Asia-Pacific). Conceptually, the model was limited to 5 major constructs, leaving room for future research to include variables such as organizational culture or leadership style.The study provides both theoretical and practical contributions. It extends the understanding of digital transformation by integrating cybersecurity, Big Data analytics, and EU regulatory compliance into a coherent conceptual framework, empirically validated in the Romanian context through the lens of the Resource-Based View (RBV), Dynamic Capabilities, and Institutional Theory.

From a managerial perspective, the findings suggest that organizations should adopt an integrated approach that combines technology adoption, security measures, data analytics, and regulatory

awareness to maximize organizational performance. Additionally, cultivating a culture of cybersecurity awareness and providing continuous training are essential, particularly for resource-constrained SMEs.The originality of this doctoral research lies in its interdisciplinary approach and in the development of an empirically grounded model that integrates digital transformation and cybersecurity within a performance-oriented analytical framework. By correlating theoretical perspectives with empirical evidence, the thesis contributes to the advancement of knowledge in the fields of digital strategy and cybersecurity management.

From a practical perspective, the findings offer concrete and applicable insights for managers and policymakers, supporting an evidence-based decision-making process regarding digital investments and cybersecurity governance. The proposed model serves as a strategic tool for organizations aiming to optimize their performance while mitigating cyber risks in an increasingly complex digital environment.In conclusion, this doctoral research illustrates that digital transformation and cybersecurity are mutually reinforcing strategic capabilities, whose effectiveness is enhanced by Big Data practices and compliance with EU regulations. The study confirms that technology alone is insufficient to ensure organizational success; human, organizational, and regulatory dimensions play a decisive role. By employing a mixed-methods design, the research blends contextual depth with empirical rigor, offering a comprehensive framework for understanding how digitalization, cybersecurity, data, and regulation jointly shape organizational outcomes. The results obtained can be utilized in practice by managers, can further develop and enrich the academic discourse on socio-technical transformation and regulatory impact, and simultaneously lay the groundwork for future studies examining cross-country comparisons, sector-specific dynamics, and the evolution of legislative frameworks.