International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

The Digital Evolution Strategies for Overcoming Cybersecurity and Adoption Challenges in French SMEs

Rachid Ejjami

Doctoral Candidate, Ecole des Ponts Paris Tech, France

Abstract

French Small and Medium-sized Enterprises (SMEs) face a crucial juncture in their path towards digital transformation. They encounter notable obstacles in embracing digital technologies and bolstering cybersecurity measures. This integrative literature review examines the complex relationship between digitalization and cybersecurity, highlighting their importance for enterprises' ongoing competitiveness and operational security. The study is focused on two primary areas: the integration of digital technologies and the establishment of robust cybersecurity frameworks. This review thoroughly examines existing research to offer strategic insights for leaders of French SMEs and IT policymakers. It employs rigorous inclusion and exclusion criteria, detailed data extraction, and comprehensive synthesis to ensure a systematic analysis. The findings emphasize the critical roles of organizational culture and innovation diffusion in shaping the adoption of technology and the implementation of security practices. The review puts forward practical suggestions to address the digital divide, strengthen cybersecurity readiness, and promote a digital environment accessible to all sectors of French SMEs. These recommendations focus on enhancing operational efficiency, minimizing expenses, and fortifying the security framework to bolster a solid national digital transformation. The study's conclusions highlight the significance of these findings for future research and practice, providing a thorough guide for incorporating digital transformation and cybersecurity in the context of French SMEs.

Keywords: Digital transformation, Cybersecurity, French SMEs, Organizational culture, Innovation diffusion, Technology adoption, Operational security

Introduction

Some French SMEs are transitioning considerably in the dynamic digital era, embracing new technology to redefine their operations and strategic goals [1]. This progress is critical for remaining competitive in a global economy that places an increasing value on adaptability, innovation, and technological knowledge. As these small and medium-sized businesses implement digital tools into their everyday operations, they increase efficiency and discover new prospects for growth and client engagement. However, the introduction of digital technology increases vulnerability to cyber threats, necessitating rigorous measures to deal with the complexities of digital transformation and protect operations from developing hazards [2]. The proliferation of interconnected devices during the Internet of Things (IoT) era amplifies the potential avenues malicious actors can infiltrate, thereby underscoring the criticality of robust and efficient cybersecurity measures.

Cybersecurity presents significant issues for SMEs as they adopt disruptive technologies like cloud computing, IoT, and AI-driven analytics [3]. Although these technologies offer considerable benefits, they expose businesses to new vulnerabilities and increasingly sophisticated and deadly cyber threats. As a result, strong cybersecurity measures have become an essential component of many firms' digital strategies, protecting them from the ever-changing world of cyber threats while maintaining their operations' robustness [4]. Maintaining a careful balance between innovation and risk management, critical to the resilience and profitability of digital transformations, highlights the importance of identifying and mitigating vulnerabilities so that possible downsides do not overshadow the benefits of digitization. The use of technology among French SMEs varies significantly, depending on factors such as industry-specific patterns, firm size, and regional infrastructure [5]. While some firms have eagerly embraced digital tools, rapidly updating their operations to boost their market positions, others cautiously approach the digital landscape due to limited resources and variable levels of digital literacy. SMEs must adjust their strategies to effectively address the difficulties created by significant differences in digital access, which affect technology adoption rates and cybersecurity efficacy [6]. They should carefully align their approach to technology and cybersecurity with their requirements and abilities and be willing to change their techniques as needed. That is consistent with France's overall digital strategy, which includes significant investments in digital platforms and talent development.

The cultural context within small and medium-sized enterprises plays a vital role in determining the level of adoption of digital technologies and the effective management of cybersecurity. The success of digital projects and the effectiveness of cybersecurity measures heavily rely on the prevailing business culture, given the limited resources available compared to more giant corporations [2]. Organizations that place high importance on proactive risk management, ongoing learning, and the flexibility to adapt to new technologies are more likely to succeed in overcoming the difficulties associated with digital transformation. Comprehending and accepting these cultural elements is essential for creating a workplace that effectively integrates digital tools while prioritizing security. Therefore, small and medium-sized firms should prioritize the development of a supportive and forward-thinking corporate culture to leverage digital technology and manage associated risks with efficiency effectively [7]. The emphasis is on cultivating a setting that promotes continuous innovation and safely incorporates digital technologies.

External factors such as the legal framework and government policies significantly impact French SMEs' digital and cybersecurity environment [8]. Government measures to stimulate digital growth and strengthen cyber resilience are essential in assisting these enterprises as they embark on their digital transformation path. These programs go beyond satisfying legal criteria, providing critical financial and technical assistance to SMEs as they face the myriad obstacles of digital transformation. This assistance is critical in creating a secure and forward-thinking business environment that facilitates the seamless integration of digital technology. Compliance with external regulatory and policy frameworks is critical for small and medium-sized businesses seeking to capitalize on digital benefits while effectively managing associated risks [9]. This alignment reflects France's overarching goal to encourage industry digital transformation, emphasizing developing a solid infrastructure and providing a favorable policy climate that fosters the development of small and medium-sized businesses in a digital economy.

The integration of digital transformation and cybersecurity in French SMEs represents a complex interplay of technological adoption, cultural adaptation, and compliance with regulatory standards [10]. By delving deeply into these dynamics, SMEs can more effectively strategize their approaches to

digitalization and cybersecurity. It is not sufficient for SMEs to simply survive in the digital era; rather, they must thrive by leveraging technology as a pivotal force for growth and innovation. Embracing a comprehensive and strategic approach that encompasses technological advancements, cultural shifts, and regulatory compliance will empower French SMEs to fully realize their potential in a manner that is both secure and sustainable [6].

Researchers emphasize the need for organizational agility and efficient human-digital system interactions as French SMEs manage digital transformation [11]. Extensive education is required to reduce fears connected with new technology, allowing French SMEs to gain the necessary skills for competitive digital transformation. They should also take a thorough approach to data privacy and cybersecurity concerns. Understanding the approaches and factors that influence digital technology adoption among French business leaders is critical. Improving stakeholder communication can encourage leaders to invest in technological breakthroughs that modernize France's digital infrastructure, improve operational security, and boost global competitiveness. That is consistent with France's national initiatives, which support SMEs by investing heavily in digital platforms and skills development to increase SME competitiveness and adaptability in a supportive environment for digital transformation, as detailed in the country report on France's digital strategy [12].

The involvement of French SMEs in digital technologies and cybersecurity is diverse, necessitating strategic innovation and proactive change management [13]. Analyzing adoption methods and the elements influencing their acceptance in the French business landscape could yield valuable insights. Gaining a better understanding of these processes helps close the gap between existing tactics and the potential benefits of adopting technology. That may encourage SME CEOs to invest strategically to develop their digital ecosystems. These types of investments are critical for successfully navigating the difficulties of digital transformation and building a flexible, future-oriented business environment. That necessitates a concerted effort to educate and empower workers, align digital initiatives with business objectives, and seamlessly integrate cybersecurity safeguards from the start of technology installation procedures [14]. This move will preserve the data and digital technology that enable French SMEs to maintain their strength and competitiveness in the digital era.

Background

The digital transformation journey for SMEs in France is distinguished by innovation and significant hurdles as these organizations struggle to remain competitive in a quickly changing technology world [15]. SMEs embrace cutting-edge technology like cloud computing, the Internet of Things (IoT), and robust data analytics, which transform their business operations, increase productivity and allow them to develop creative client interactions and service alternatives. This transition entails more than just using new technology; it also includes a considerable shift in their business models, operational methods, and organizational culture. These transformations are underpinned by France’s strategic aims of boosting digital performance and increasing competitiveness at home and internationally [16]. These initiatives are part of a national strategy to foster digital transformation and enhance digital infrastructure across industries within legislative frameworks in collaboration with European partners.Yet, their implementation requires significant expenditures in digital platforms and talent development, focusing on fostering an innovative and adaptable culture.

Scholarly research into French SMEs' digital transformation is still in its early stages, providing potential for more investigation and knowledge of the various variables affecting these businesses' digitalization

adaptation [13]. This transformation enhances competitiveness and the capacity to adapt to evolving consumer expectations, driven by insights derived from data beyond the scope of company operations. An in-depth understanding of the complex relationship between human and technical systems, adapting business strategies, dealing with ever-changing labor markets, and creating value in various industries play a crucial role for SMEs to fully maximize the effectiveness of their digital tactics [17]. Such initiatives result in higher productivity and decreased costs; with automation and digitization, SMEs can enhance customer satisfaction, expand profitability, and establish a more competitive market position [18].

Cybersecurity has evolved as an essential component of digital transformation, especially as SMEs gradually integrate digital technologies into their operations [19]. As integration proceeds, cyber dangers become more prevalent, emphasizing the importance of cybersecurity in managing the quickly changing digital ecosystem while protecting sensitive data and customer confidence. In the face of a constantly changing cyber threat landscape, French SMEs should maintain vigilant system monitoring by integrating cybersecurity solutions to protect their digital and operational infrastructure [20]. Implementing a comprehensive security strategy allows them to mitigate and withstand evolving cyber threats effectively, ensuring their long-term growth and success in the digital market. This forward-thinking approach ensures that businesses not only overcome the challenges of the digital age but also have the flexibility and strength required to quickly adapt to shifting technological landscapes, allowing them to thrive in an ever-changing digital environment [21].

There is an urgent need for additional research into the impact of organizational culture on the effective adoption of digital technologies and cybersecurity measures in small and medium-sized firms (SMEs) in France [10]. Understanding the influence of organizational culture can identify how attitudes towards innovation and risk affect technology integration and security practices, thereby guiding SMEs in creating more adaptive and resilient business models. The organization's emphasis on security procedures and protocols reflects its recognition of the need to safeguard sensitive information, systems, and assets from various threats, including cyberattacks, data breaches, and illegal access [22]. The problem is the difficulties facing the implementation of cybersecurity within SMEs undergoing digital transformation. Due to resource restrictions, it can be hard for SMEs to build a work environment that integrates technology with daily operations and company goals; nonetheless, it is critical to implement security measures to protect against cyber assaults. Many SMEs need help implementing security measures, which impedes the critical cultural shift required for faster adoption of new technology and more robust cybersecurity defenses. Creating an atmosphere that promotes constant digital innovation and strong security standards is both challenging and necessary for these companies to remain competitive and resilient in the digital age [23].

Given their critical economic role, French SMEs should strengthen their digitalization and cybersecurity efforts to enhance competitiveness, increase security and risk management, ensure sustainability and growth, and remain relevant in the market [13]. Current literature emphasizes the need for a well-planned approach that allows SMEs to efficiently manage the integration of cutting-edge technologies while maintaining solid cybersecurity measures [16]. By doing so, businesses can leverage the full potential of digital transformation without compromising their operational integrity or customer trust. The purpose of this integrative literature review is to investigate how French SMEs can successfully implement digital transformation while taking cybersecurity measures to improve organizational resilience and competitiveness. The integrative literature review method used in this

study combines information and practical insights from critical studies to evaluate existing knowledge and provide paths for future research in the quickly expanding digital ecosystem. This approach is suitable for studying the digital transformation of French SMEs as they manage the complexities of technology adoption and cybersecurity to ensure long-term growth in the digital era.

This study is significant because it emphasizes the critical need for French SMEs to integrate cybersecurity procedures into their operational strategies, enabling them to leverage digital transformation and remain competitive and secure in the global market. The existing literature recognizes the pivotal role of cybersecurity in allowing digital technologies to significantly enhance operational efficiency and broaden market reach [19]. The adoption of new technologies introduces complex cybersecurity issues that demand strong management to safeguard sensitive data and preserve consumer confidence. Simultaneously, implementing data security measures enables SMEs to streamline their processes and automate routine tasks, thereby reducing labor costs and enhancing efficiency [24]. This dual approach ensures the protection of valuable information while positioning SMEs for sustainable growth by increasing productivity and operational effectiveness in a secure digital environment. Additionally, robust cybersecurity measures provide strong protection for digital systems against potential threats, ensuring that productivity enhancements achieved through digitalization are not only maintained but also secure over the long term. Therefore, it is imperative for SMEs adopting digitalization to continuously update their cybersecurity strategies to handle evolving threats and maintain a competitive edge in an increasingly unsafe digital world [7].

This integrative literature review attempts to tackle a crucial research question: What recommendations may be provided to assist French SMEs in efficiently leveraging digital technology while upholding robust cybersecurity measures to enhance their competitiveness and operational security? This inquiry investigates strategic perspectives that can assist French SMEs in effectively navigating the complexities of securely adopting digitalization. This ILR strengthens the digital framework and enhance cybersecurity measures that are crucial for the success of these businesses, as it provides a comprehensive analysis of existing knowledge, identifies areas needing further research, and suggests practical strategies [25].

Theoretical/Conceptual Framework

This integrative literature review delves into French SMEs' challenges in adopting cybersecurity measures amid their digital transformation. Organized around two pivotal concepts—digital evolution strategies and cybersecurity—the review explores how French SMEs practically integrate cybersecurity into their operational and strategic frameworks during their digital transformation journey. It delves into the obstacles encountered, including resource constraints, knowledge gaps, and organizational resistance, while proposing practical solutions to overcome these hurdles. Moreover, the review sheds light on the operational impacts of cybersecurity solutions, emphasizing enhancements in data protection, risk management, and regulatory compliance.

Cybersecurity technologies play a vital role in the digital transformation journey of SMEs, particularly in safeguarding data, securing online transactions, and verifying identities—essential elements for upholding business integrity and fostering customer trust [26]. As SMEs increasingly rely on digital tools, the infrastructure provided by digital transformation initiatives becomes indispensable, facilitating the implementation of cybersecurity solutions and seamlessly integrating them into existing business operations. Adopting advanced cybersecurity measures, such as encryption, multi-factor authentication,

and intrusion detection systems, is paramount for mitigating cyber threats, averting data breaches, fortifying network access, and ensuring compliance with privacy regulations [27]. Furthermore, by fortifying their digital environments, SMEs can confidently harness their digital capabilities to explore new market opportunities, innovate, enhance operational efficiency, and establish themselves as reliable entities in an increasingly privacy-conscious digital marketplace.

However, SME leaders and policymakers in France confront considerable barriers to deploying cutting-edge cybersecurity solutions in small and medium-sized firms. These issues stem from various factors, including the complexity of security technology, organizational resistance to change, and a need for interoperability between new technologies and old business processes [28]. A comprehensive approach is required to effectively manage cybersecurity adoption in SMEs, ensuring that technologies are readily available, comprehensible, and seamlessly integrated across all organizational levels. Clear communication, training, employee involvement in the change process, and emphasizing the benefits of new security measures can all help to overcome opposition within an organization's culture. Interoperability between new technology and existing business processes is critical for ensuring seamless integration, improving operational efficiency, and fully leveraging the benefits of digital transformation. In light of these practical issues, theoretical insights from Diffusion of Innovations Theory and Socio-Technical Systems Theory are especially pertinent. The former emphasizes the challenges of embracing cybersecurity developments due to their complexity or incompatibility with existing systems [29]. The latter underlines the need to integrate technology solutions with an organization's social structures. Effective adoption goes beyond technology advancements and requires comprehensive cultural and operational adjustments inside the company to achieve successful integration and long-term advantages [30].

The study's conceptual framework is rooted in the significant challenges French SME leaders and policymakers encounter when implementing sophisticated cybersecurity measures. These obstacles encompass the intricacy of security technologies, organizational resistance to change, and the integration difficulties between new technology and existing business processes [13]. Moreover, the reluctance of organizational cultures to embrace new technology can significantly hinder the successful implementation of crucial security measures. Overcoming these challenges requires a comprehensive approach that facilitates access to and understanding of cybersecurity technology and ensures seamless integration across all organizational levels. This approach entails employing adaptive strategies to adjust existing procedures and foster a culture prioritizing security within businesses. Such strategies may include establishing internal cybersecurity protocols, enhancing system compatibility, and nurturing an environment that recognizes security as an indispensable component of corporate operations [31]. This integrative literature review underscores the intricate dynamics involved, emphasizing the importance of a holistic strategy for cybersecurity implementation in SMEs that aligns technology upgrades with organizational restructuring, particularly within the context of French small and medium-sized firms.

The study's theoretical framework is based on the fusion of Diffusion of Innovation Theory and Socio-Technical Systems Theory, serving as a lens to investigate the factors influencing the acceptance and implementation of advanced cybersecurity measures in French SMEs. Diffusion of Innovation Theory is instrumental in understanding how perceived attributes of cybersecurity solutions shape their adoption across different organizational levels [32]. It underscores the importance of innovation characteristics and the role of change agents in facilitating the adoption process. In contrast, Socio-Technical Systems Theory illuminates how these technologies are integrated into small and medium-sized enterprises'

social and organizational structures, emphasizing the need to align technological solutions with human factors to ensure seamless integration and improved organizational activities [33]. This dual-framework approach enables a comprehensive analysis of both the technological and social dimensions influencing cybersecurity adoption in SMEs and developing targeted strategies to overcome technology acceptance barriers and maximize the effectiveness of cybersecurity implementations.

There is a notable gap in the literature concerning the concurrent implementation of cybersecurity measures alongside the digital transformation of small and medium-sized enterprises [8]. While existing research often focuses on either the technological aspects of cybersecurity or theoretical frameworks related to organizational change, there remains an urgent need for more comprehensive studies examining the intersection of these elements within the SME context [34]. This gap underscores the necessity for further research into the simultaneous application of cybersecurity technologies and organizational change management. Addressing this gap is paramount as it offers a holistic understanding of the challenges and best practices involved, providing essential insights into practical methods for integrating cybersecurity measures into SMEs' digital operations [35]. Bridging this research deficit is pivotal for enhancing SMEs' security frameworks, bolstering technical robustness, and fostering seamless cultural and procedural integration during digital transformation. Such endeavors are indispensable for significantly enhancing SMEs' resilience and competitiveness in the digital landscape, as well as ensuring their sustainability and safety amidst the rapidly evolving cyber environment [14].

When considering future studies on the integration of cybersecurity during digital transformation, it is critical to extensively investigate the unique issues faced by SMEs in various industrial sectors in France. Future research should prioritize providing practical help to SMEs in developing and implementing cybersecurity plans adapted to their specific operational, cultural, and technological contexts. Assessing how cybersecurity measures affect an organization's agility, competitiveness, and innovation skills is vital to ensure that security protocols do not impede growth and adaptation while protecting against attacks [36]. Analyzing these components will improve our understanding of how cybersecurity may be used not only as a defensive mechanism but also as a competitive advantage that promotes long-term business growth. Future research in these areas could considerably improve the practical use of integrated cybersecurity solutions, enabling French SMEs to confidently manage the problematic issues of digital transformation while retaining security and efficiency. Such a management style is crucial for combining insights from many sectors and addressing the complex challenges of protecting modern businesses in an increasingly digital world [37].

Research Method and Design

An integrated literature review (ILR) merges theoretical and empirical literature to enhance comprehension of a specific event or scenario by collecting information from diverse academic sources, synthesizing, evaluating, and critically analyzing current knowledge on a particular research issue [38]. The objective is to comprehensively understand the issue by integrating insights from various studies, theories, and perspectives, laying the groundwork for a conceptual framework and guiding future research endeavors. An ILR draws upon various sources, including peer-reviewed publications, books, conference papers, reports, grey literature, and reputable web sources, actively contributing to developing concepts that inform field policies and practices [39]. Its primary aim is to identify patterns and recurring themes while juxtaposing different viewpoints to comprehensively understand the research topic. Through this meticulous evaluation, ILR assesses the quality, methodology, and rigor of studies,

highlighting areas warranting further investigation to offer valuable insights into future research opportunities. Ultimately, the ILR method presents a coherent and valuable narrative that provides a distinct perspective on the research landscape [40].

Researchers approach literature review themes by identifying emerging research interests, keeping up with crucial area breakthroughs, and pursuing new research avenues [41]. They underline the significance of actively engaging with emerging breakthroughs and evaluating potential future orientations, as well as the critical function of keeping stakeholders informed. They emphasize the importance of conducting thorough literature evaluations that evaluate policy implications, future practices, and developmental repercussions. Researchers also emphasize the need to specify sample criteria clearly to ensure representativeness and underline the importance of undertaking a thorough and systematic data collection phase that matches the study's objectives [42]. They use a methodological framework to make sure that their research is rigorous and unbiased. A literature evaluation that does not thoroughly examine policy implications, future practice, and development is unlikely to elicit further inquiry into the issue [43]. Experts also advocate using vast academic search engines like Google Scholar to identify relevant papers and consult various sources to understand the topic at hand.

The Integrative Literature Review (ILR) method conducts a comprehensive analysis by combining varied perspectives and findings from various sources, including academic articles, reports, case studies, and industry publications. The ILR approach is beneficial for a study looking into the digital revolution and the cybersecurity and adoption difficulties that French SMEs confront [6]. Examining scholarly works on this topic enables a complete understanding of the elements contributing to these challenges and formulating ways to solve them. Addressing French SMEs' challenges during their digital transformation necessitates integrating expertise from several disciplines, such as technology, business, cybersecurity, and organizational change [7]. This strategy is critical for identifying and synthesizing best practices and insights to assist these firms in navigating the complexity of digital and cybersecurity integration. Using the ILR technique, researchers may uncover effective strategies and provide significant advice for improving the resilience and competitiveness of French SMEs in the digital age [1].

The research question seeks to investigate the critical elements that influence the successful implementation of digital transformation practices, focusing on a diverse range of applications across industries, regulatory challenges, and potential consequences for the French business environment. This ILR seeks to identify common themes, patterns, and areas of knowledge that deserve further investigation through a thorough and structured examination of existing literature. Identifying common patterns and areas of knowledge that deserve further investigation is critical for tackling the research topic and improving our understanding of overcoming cybersecurity and adoption barriers in French SMEs, and it allows for investigating numerous hypotheses and data, leading to a better and more complete comprehension of the issue [5]. That involves precisely aligning the selection criteria with the driving question, taking into account the participants, interventions, and desired outcomes. The ILR method is particularly well-suited for this study because it allows for constructing a solid theoretical basis and conceptual framework, both critical for developing effective strategies and policies to promote the digital growth of French SMEs. This technique enables the analysis of previous studies' theoretical approaches, models, and frameworks, providing guidance for current research and contributing to developing a robust analytical framework [32].

A complete methodological framework for an Integrative Literature Review includes five critical stages: problem formulation, data collection, data assessment, data analysis and interpretation, and presentation of results [25]. This ILR on digital transformation and associated cybersecurity challenges in French SMEs adopts a comprehensive approach to gathering relevant information from numerous sources so that its integrity and the depth of the analysis undertaken throughout its realization are significantly enhanced. This evaluation began by stating the study's objectives, scope, and focus on integrating digital technologies and managing cybersecurity concerns in French SMEs to identify the significant concerns and challenges in this approach. Subsequently, key terms, keywords, and phrases such as "digital transformation," "cybersecurity," "French SMEs," and similar variations were identified to guide the data collection process. A comprehensive search string was then constructed using these terms and logical operators such as AND and OR were used to refine the search, and the literature search involved carefully selecting appropriate academic databases, journals, digital libraries, and repositories. A well-structured data collection format aligned with the study's goal and key research question was crucial for obtaining consistent and meaningful information from all sources. The integrity of a research paper and the meticulousness with which the author carries out literature and data analysis are critical in producing reliable and noteworthy results [44].

Following the establishment a specific search phrase, a thorough review of various articles, conference papers, reports, and academic publications was conducted. Each title and abstract was painstakingly examined against predetermined inclusion and exclusion criteria to discover relevant literature on digital transformation and cybersecurity in French SMEs. The content of selected papers was consolidated, with conclusions organized around themes including methodology, significant insights, difficulties, and opportunities. This investigation found patterns and insights into how French SMEs handle digital transformation and cybersecurity, significantly affecting strategic decision-making. The review finished with a complete synthesis, which provided a detailed panorama of current practices and potential directions. Backward and forward citation searches were also undertaken to improve the review's rigor and reproducibility. They play an essential role in ensuring comprehensive literature coverage, increasing the study's rigor, and identifying relevant studies that may contribute to the durability and validity of the research findings [45].

One issue relevant to the topic of this study that must be addressed is the possibility of inconsistencies between the research undertaken and the population under investigation. Several practical methods were implemented to mitigate this potential risk including a thorough data collection strategy to guarantee that all relevant material was collected. The collected data was thoroughly recorded, including information on sources, publication years, and critical study terms like "digital transformation," "cybersecurity," and "French SMEs." A thorough synthesis technique was used to ensure the findings' integrity and address potential selection biases. This study used a variety of library databases and search engines, including Google Scholar, IEEE Xplore, ACM Digital Library, PubMed, Web of Science, and Scopus. Google Scholar's ample scope and widespread use in academics demonstrate its importance as a primary resource for finding relevant papers [46]. After discovering notable works and themes, the search strategy included vital phrases and was modified to focus on specific aspects of digital transformation and cybersecurity in French SMEs, ensuring that only the most relevant and impactful research was included, increasing the findings' robustness and applicability.

Given the scarcity of recent research, dissertations, and conference proceedings on "The Digital Evolution Strategies for Overcoming Cybersecurity and Adoption Challenges in French SMEs," I made

the most of the available literature. I meticulously researched peer-reviewed journal articles, books, and credible web sources to gather relevant data, insights, and hypotheses for the study. The Integrative Literature Review (ILR) technique was chosen because it amalgamates a diverse body of literature from numerous sources, allowing for a thorough examination of technology, business, policy, and economics in relation to French SMEs. This technique was instrumental in identifying patterns, trends, and gaps in the literature, providing a comprehensive understanding of the digital transformation and cybersecurity concerns these businesses face. The ILR technique enhanced the analysis, enabling a detailed evaluation of the complexities involved in effectively safeguarding and digitizing French SMEs. This approach facilitated a holistic perspective on the challenges and strategies pertinent to the digital evolution of these enterprises, ensuring a robust and well-rounded investigation [6].

Tables 1, 2, and 3 categorize and organize the selected papers according to their citation count, providing insight into each article's significance and impact within the current literature on "The Digital Evolution Strategies for Overcoming Cybersecurity and Adoption Challenges in French SMEs." This rating highlights the most reliable sources and arguments in the current research, advising readers on the significance of each piece of evidence discussed regarding digital transformation and cybersecurity in French SMEs.

Table 1: Representative Literature on Adaptation to Technological Advances and Cybersecurity Integration Selected for Review

Rank	Title	Year	Author(s)	Type of Document	Citations
1	Barriers to digital servitization in French manufacturing SMEs	2023	Peillon & Dubruc	Journal article	131
2	Grasp the challenge of digital transition in SMEs—A training course geared towards decision-makers	2021	Azevedo & AH Almeida	Journal article	66
3	The contribution of organizational culture, structure, and leadership factors in the digital transformation of SMEs: a mixed-methods approach	2023	Leso, Cortimiglia, & Ghezzi		48

Table 2: Representative Literature on Cultural and Organizational Readiness for Digital Transformation Selected for Review

Rank	Title	Year	Author(s)	Type of Document	Citations
1	Digital transformation: A multidisciplinary reflection and research agenda	2021	Verhoef, Broekhuizen, Bart, Bhattacharya, Dong, Fabian, & Haenlein	Journal article	3332

2	Internationalization and Digitalization: Applying digital technologies to the internationalization process of small and medium-sized enterprises	2021	Hervé, Schmitt, & Baldegger	Journal article	110
3	Understanding how digital transformation can enable SMEs to achieve sustainable development: A systematic literature review	2022	Philbin, Viswanathan, & Telukdarie	Journal article	31
4	Enhancing Sustainable Business by SMEs' Digitalization	2022	Korez-Vide, Hunjet, & Kozina	Journal article	5
5	Promesses et défis de la transformation numérique du secteur public	2022	Jacob, Defacqz, & Agossou	Journal article	4
6	Adoption and performance outcome of digitalization in small and medium-sized enterprises	2024	Kallmuenzer, Mikhaylov, Chelaru, & Czakon	Journal article	1
7	La transformation digitale dans les entreprises : attentes et retombées	2020	Gevorgyan & de Rocca Serra	Journal article	0
8	The Contribution of Agility to an Organization's Digital Transformation.	2023	Ibrahimi & Benchekroun	Journal article	0
9	Digitalization And Its Impact on Small and Medium-Sized Enterprises (SMEs): An Exploratory Study of Challenges and Proposed Solutions	2023	Ji & Singh	Journal article	0
10	Digital and Sustainable (Twin) Transformations: A Case of SMEs in the European Union	2024	Burinskienė & Nalivaikė	Journal article	0

Table 3: Representative Literature on Impact of External Factors on Digital and Cybersecurity Strategies Selected for Review

Rank	Title	Year	Author(s)	Type of Document	Citations
1	A Framework for GDPR Compliance for Smalland Medium-Sized Enterprises	2019	Brodin	Journal article	63
2	Sustainable digital transformation in small and medium enterprises (SMEs): A review on performance	2023	Melo, Queiroz, Junior, de Sousa, Yushimito, & Pereira		54
3	The opportunities and challenges of digitalization for SME's	2023	Telukdarie, Dube, Matjuta, & Philbin	Journal article	43
4	La cybersécurité : contexte, enjeux, constats et perspectives Cybersecurity: context, issues, findings and outlook	2023	Damiano	Journal article	1

Findings

Strategic Integration of Digital Transformation and Cybersecurity

The strategic integration of digital transformation and cybersecurity is a significant goal for French SMEs as they attempt to use digital technology to drive growth and increase their competitive edge while dealing with rising cyber risks that could stymie their progress. Connecting cybersecurity efforts to digital transformation objectives has been highlighted as one of the most challenging issues. Many small and medium-sized firms prioritize technological upgrades and process optimization when launching a digital initiative. Unfortunately, this frequently leads to firms ignoring cybersecurity, leaving them open to cyber threats and potential assaults [33]. This fragmented strategy can cause significant disruptions, financial losses, and reputational harm. Furthermore, the rapid pace of technological advancement frequently outpaces the development of appropriate security measures, complicating the problem [4]. As a result, it is critical to implement a well-thought-out and comprehensive approach that includes cybersecurity as a core component of digital strategy. This approach protects every step toward digital growth from cyber risks, ensuring the organization's success and stability [36].

The literature underlines the significance of organizational culture in successfully managing cybersecurity and digital transformation. A proactive, inventive, and security-conscious culture is required for the seamless adoption of new technology and strong cybersecurity measures [35]. Leadership, in particular, plays a critical role in building such a culture by engaging and educating people about cybersecurity risks and practices. The current regulatory framework also plays an important role, with government policies offering critical assistance and advice while enforcing severe compliance standards that might be difficult for SMEs to satisfy. Effective government engagement, including financial and technical support, can aid SMEs in overcoming these hurdles and improving their digital and cybersecurity skills [31]. To summarize, while French SMEs have various problems

when integrating digital transformation and cybersecurity, a holistic, culturally aligned, and well-supported approach can considerably improve their resilience, competitiveness, and operational security in the digital world.

An assessment of the current literature shows that a comprehensive strategy integrating digital transformation and cybersecurity can have a massive impact on small and medium-sized organizations [47]. Studies frequently reveal that SMEs incorporating cybersecurity into their digital transformation strategy perform better in risk management, resilience, and operational reliability. Research emphasizes various beneficial strategies, such as building a comprehensive IT governance framework that corresponds with company goals and continuously adapting cybersecurity measures to stay up with technological developments [18]. This governance framework is critical because it provides a disciplined way to incorporate cybersecurity into all parts of digital operations, ensuring that security considerations are entrenched throughout the technology adoption and deployment process. The literature also emphasizes the importance of incorporating risk management into digital planning, such as completing comprehensive risk assessments and strategic planning to manage and mitigate security threats [48]. Risk management procedures are critical for recognizing potential vulnerabilities and taking proactive steps to remedy them before they are exploited. Furthermore, there is an increasing need for continuous monitoring and adaptable security systems capable of efficiently managing emerging risks in the ever-changing digital ecosystem [34].

The extant literature advocates for a holistically strategic forward-thinking regarding the implementation of adaptable security systems for managing emerging digital risks safeguards the IT infrastructure and fosters a security-conscious culture throughout the organization, boosting the overall success of digital transformation initiatives [27]. Promoting a security-conscious culture entails informing employees about cyber dangers and safe procedures and creating a climate in which everyone accepts responsibility for maintaining security. Regular training and awareness programs can reduce the risk of human error, which frequently contributes to security breaches [4]. Integrating these sanitizing factors guarantees that SMEs are protected from current dangers and ready to face future challenges, promoting an environment where innovation and security coexist. SMEs can gain considerable operational gains and competitive advantages in the digital economy by implementing robust governance, risk management, and a flexible and adaptive approach to cybersecurity. This comprehensive strategy emphasizes the need to embed cybersecurity into the core of digital transformation programs to ensure sustainable growth and long-term success for SMEs in a fast-shifting technology context [23].

To ensure that cybersecurity measures are seamlessly integrated into small and medium-sized enterprises (SMEs), establishing a national cybersecurity institute tailored to each sector could significantly improve their security measures and enhance the nation's economic resilience. Such an institute would function as a centralized entity that provides SMEs with the peculiar resources, training, and assistance they need to strengthen their cybersecurity infrastructure. By offering specialized counseling and facilitating access to cutting-edge technologies, the institute could help SMEs adopt best practices and implement effective security processes, thereby reducing the risks associated with cyber threats. This strategy would ensure that SMEs lacking the skills and resources to develop comprehensive cybersecurity policies independently receive the necessary support to protect their digital assets efficiently.

Furthermore, a national cybersecurity institute tailored to each sector would promote collaboration between the public and private sectors, leading to a more coherent and integrated approach to secure digitalization. By facilitating information sharing and disseminating industry standards, the institute

could help bridge the gap between SMEs and larger enterprises, ensuring that all firms, regardless of size, are prepared to deal with the evolving cyber threat landscape. This collaborative environment would improve the security postures of individual SMEs and contribute to the nation's overall economic resilience. By protecting the digital infrastructure of SMEs, which are looked on as the backbone of many economies, the institute would ensure economic stability and support a secure and robust digital marketplace.

Impact of Organizational Culture on Cybersecurity Implementation

The impact of organizational culture on the deployment and effectiveness of cybersecurity measures in French SMEs is a complex issue that has received substantial attention in the literature [13]. A business culture that opposes technological innovation or ignores the importance of cybersecurity can jeopardize the successful adoption of solid cybersecurity measures. Many small and medium-sized businesses fail to include cybersecurity in their strategic business plans, resulting in insufficient ongoing attention and resources to address cybersecurity risks [24]. To properly handle the ever-changing cyber threat landscape, businesses must be adaptable and aware. However, the presence of rigid or incorrect cultural norms inside an organization might impair the critical capacity for adaptability and consciousness required to cope with the constantly evolving digital security threat. This cultural hesitancy frequently results in sporadic cybersecurity measures that are reactive rather than proactive, leaving firms vulnerable to sophisticated attacks [19].

The disparity in cybersecurity readiness among French SMEs is often connected to cultural views toward technology and security, emphasizing the necessity for a culture shift toward proactive cybersecurity engagement [49]. Research indicates that a proactive, imaginative, and security-conscious culture is required to successfully adopt new technologies and implement appropriate cybersecurity measures [50]. Leadership is critical in creating this cultural shift, ensuring employee participation and education on cybersecurity risks and processes. Companies that value continuous learning, adaptability, and proactive risk management are better prepared to deal with cybersecurity threats. Yet, creating a culture of security, ongoing improvement, and adaptability is vital for French SMEs to improve their cybersecurity readiness and resilience. This cultural shift reduces risks and deeply integrates cybersecurity into the organizational fabric, ensuring long-term protection and competitiveness in the digital realm [28].

The present literature emphasizes the necessity of creating a positive organizational culture that values cybersecurity, as this considerably improves a company's ability to manage cyber risks and remain resilient to threats [51]. According to research, small and medium-sized firms (SMEs) prioritizing continuous learning, proactive risk management, and adopting new technologies are more likely to implement robust and effective cybersecurity measures. In these companies, cybersecurity is smoothly integrated into day-to-day operations, becoming a critical component of the business workflow rather than merely a technological problem. Leadership is crucial in facilitating this cultural shift, as pro-cybersecurity leaders consistently demonstrate compliance behaviors and encourage open discussions about cyber dangers are essential to creating a culture that is aware of and prepared to address cybersecurity challenges [35].

Current research highlights the importance of prioritizing thorough and frequently updated training programs for SMEs undergoing digitalization to stay current with the ever-changing cyber threat landscape [36]. Training programs play a crucial role in enhancing cybersecurity awareness, knowledge,

and skills among employees, which is essential for protecting SMEs from cyber threats. Also, effective communication and the implementation of practical policies across the organization are likely to emphasize the importance of collaboration in cybersecurity and its impact on the well-being and success of SMEs [34]. Companies can better protect themselves from potential attacks by fostering an environment where cybersecurity is a shared responsibility and an integral part of their business strategy. This holistic approach to cybersecurity promotes an intense environment, significantly improving the overall security of small and medium-sized businesses in France's dynamic and increasingly digital world [8]. This strategy ensures that SMEs are equipped to deal with current and future cyber threats, promoting long-term growth and stability.

This ILR underscores the need to build a proactive organizational culture that prioritizes cybersecurity within French SMEs through staff training and continuous risk assessment. Training has to be delivered through virtual cybersecurity labs to ensure that all employees, from entry-level to senior, possess the knowledge and skills to identify and mitigate potential risks. These virtual labs provide a hands-on, immersive learning experience that replicates real-world scenarios, enabling the effective practice and application of cybersecurity concepts and techniques. Risk assessment has to be performed through the use of advanced cybersecurity learning devices to evaluate threats on a regular basis. These devices can simulate various attack vectors and vulnerabilities, providing valuable insights and data that help businesses stay ahead of potential threats and enhance their overall security posture. This proactive strategy helps prevent security breaches, often caused by human error or a lack of awareness.

Indeed, developing a culture that prioritizes cybersecurity awareness is critical for mitigating risks and strengthening the resilience of French SMEs. This proactive strategy includes providing the necessary skills to employees through modern training approaches and seamlessly integrating cybersecurity into the organization's daily activities and decision-making processes. Organizations can create a culture where security entails a collaborative responsibility by incorporating cybersecurity issues into all firm levels, including strategic planning and operational execution. Constantly changed training programs and regular risk assessments using cutting-edge learning gadgets ensure that personnel remain vigilant and prepared in the face of ever-changing cyber threats. Furthermore, through the meticulous examination of data and the discernment of insights derived from these sophisticated training and assessment tools, organizations can discern patterns and proactively anticipate upcoming vulnerabilities, allowing for the implementation of more effective and timely interventions. The execution of this comprehensive strategy for creating a cybersecurity-centric organizational culture protects digital assets while also improving general integrity and competitiveness.

Influence of Regulatory Environment and Government Policies

The legal environment considerably impacts SMEs' digital transformation projects as far as cybersecurity is concerned, since government regulations play a crucial role in balancing the promotion of innovation with enforcing strict security measures. While they can stimulate the use of standardized security practices, they can also impose onerous compliance requirements, creating a complex landscape in which SMEs must tread carefully [37]. Yet, Excessive regulatory frameworks risk stifling entrepreneurial spirit by introducing burdensome bureaucracy that can impede swift and innovative responses to digital opportunities [52]. This delicate balance between supporting innovation and enforcing compliance necessitates significant resources from SMEs to understand and apply these policies, which can be incredibly challenging for smaller enterprises with limited capabilities.

Furthermore, the significant discrepancy in the provision of government support to SMEs exacerbates the problem of their limited ability to effectively implement digital transformation and cybersecurity measures. Some SMEs benefit significantly from government initiatives that provide direction, financial assistance, and technological support, while others need to be included. That could be due to a lack of understanding about available opportunities or a failure to meet eligibility criteria for assistance [2]. The uneven allocation of resources aggravates the existing digital divide, leaving resource-constrained SMEs at a significant disadvantage. These SMEs struggle to keep up with their better-supported peers, widening the gap between technologically proficient and less digitally prepared businesses [7]. This situation highlights the significance of creating legislative frameworks that protect and empower all SMEs, resulting in a more inclusive digital environment. Adequate regulatory and support frameworks should create a fair environment, ensuring that all SMEs, regardless of size or resources, can benefit from digital transformation and robust cybersecurity measures, enhancing their resilience and competitiveness in the digital landscape [53].

The current literature extensively demonstrates the government's crucial role in facilitating digital transformation and improving cybersecurity among SMEs. Studies regularly show that targeted government efforts that provide technical and financial assistance can help SMEs overcome various barriers to digital adoption [54]. Grants, tax breaks, and access to expert consultations are typical initiatives that significantly reduce entry barriers to modern digital technologies and comprehensive cybersecurity solutions. Furthermore, the literature emphasizes the importance of providing clear and accessible information about regulatory requirements and relevant support mechanisms to ensure that SMEs can comply with regulations and fully benefit from government initiatives [21]. These regulations are critical for increasing digital adoption, ensuring robust security, and creating a competitive and innovative business climate.

By substantially eliminating technological and financial barriers, government support enables even the smallest businesses to participate actively in digital solutions and cybersecurity measures. This strategy contributes to a vibrant, competitive business environment where innovation thrives, and security concerns are proactively managed [11]. Effective government intervention is critical for ensuring that SMEs can navigate the digital age safely and securely, making the benefits of digital transformation accessible across the business community. This support not only mitigates the challenges SMEs face but also strengthens their resilience and competitive advantage in the rapidly evolving digital economy [55].

Establishing a sectorial cybersecurity regulatory framework may be crucial to increasing regulatory support for small and medium-sized businesses (SMEs) as they embrace digital transformation and improve cybersecurity. Such a framework would serve as a specialized hub, providing SMEs with tailored resources, professional assistance, and practical solutions to help them navigate the problems of digitalization and cybersecurity within the regulatory framework. By focusing on sector-specific requirements and difficulties, the framework might provide customized help to SMEs in their unique legal, technological, and economic environments, successfully closing the gap between national policy and local implementation.

The sectorial cybersecurity regulatory framework may be crucial in interpreting and distributing government policies and legislation on digital transformation and cybersecurity. By providing comprehensive training programs, workshops, and consulting sessions, the framework may assist SMEs in understanding and complying with regulatory standards, lowering a compliance burden. Furthermore, the framework might act as a liaison between SMEs and government organizations, ensuring that

enterprises are aware of and have access to numerous grants, tax breaks, and other forms of financial assistance designed to promote digital adoption and cybersecurity. This coordinated strategy would improve SMEs' digital capabilities and security postures while ensuring that government policies are successfully executed, resulting in a more inclusive and resilient digital economy at the sectoral level.

Critique of the Extant Literature to Identify the Future of Practice and Policy

The strategic integration of digital transformation and cybersecurity is critical for French SMEs to drive growth and gain a competitive advantage while addressing rising cyber risks. However, many SMEs prioritize technological advancements and operational efficiency over cybersecurity, resulting in vulnerabilities and potential disruptions [30]. The rapid pace of technological change frequently outpaces the development of suitable security measures, emphasizing the importance of a comprehensive approach that incorporates cybersecurity as an integral component of digital strategy to ensure organizational success and stability.

Corporate culture significantly impacts the effective management of cybersecurity and digital transformation. A proactive, imaginative, and security-conscious culture is required to successfully deploy new technology and robust cybersecurity safeguards. Leadership is crucial in developing such a culture by engaging and training employees about cybersecurity risks and processes. Government regulations also provide valuable assistance and guidance while enforcing compliance requirements that SMEs may need more work to meet. Effective government intervention, including financial and technical aid, can help SMEs overcome any obstacles and improve their digital and cybersecurity capabilities [22].

A thorough digital transformation and cybersecurity strategy can significantly impact SMEs. Studies indicate that organizations with solid cybersecurity procedures outperform those without risk management, resilience, and operational reliability [28]. Essential strategy include creating a comprehensive IT governance framework aligned with business goals and constantly updating cybersecurity measures to keep pace with technological changes. Risk management should be integrated into digital planning through risk assessments and strategic planning to control and mitigate security threats [27]. Continuous monitoring and flexible security solutions are necessary to confront new threats in the digital world.

Proactive corporate cultures that prioritize cybersecurity are essential for French SMEs. Employee training ensures that all employees understand the value of cybersecurity and are prepared to handle attacks. Regular training sessions keep personnel current on the latest cyber threats and best practices, promoting vigilance and accountability. Continuous risk assessment enables SMEs to quickly identify and resolve threats, allowing them to tailor their strategies to the evolving cyber environment. Strong leadership commitment is essential to integrate cybersecurity into strategic objectives, provide resources, and set clear policies that foster a security-first culture [24].

The legal environment considerably impacts SMEs' digital transformation efforts, particularly regarding cybersecurity. Government regulations balance fostering innovation with enforcing security measures, but they also impose complex compliance requirements that present challenges for SMEs, significantly smaller enterprises with limited capacities [19]. Also, the unequal distribution of resources exacerbates the digital divide and harms resource-constrained SMEs. There is a significant imbalance in government aid for SMEs, with some benefiting from initiatives while others are excluded due to a lack of awareness

or eligibility [54]. Therefore, creating regulatory frameworks that protect and empower all SMEs is vital to cultivating an inclusive digital economy.

To ensure that cybersecurity measures are seamlessly integrated into SMEs, establishing a national cybersecurity institute tailored to each sector dedicated to this purpose could significantly improve security measures and boost the country's economic resilience. Such an institute would serve as a centralized entity, providing SMEs with resources, training, and assistance to improve their cybersecurity infrastructure. Offering specialist advice and facilitating access to cutting-edge technologies could help SMEs adopt best practices and implement effective security processes, thereby reducing the risks associated with cyber threats [48]. This policy would ensure that SMEs, which often need more knowledge and resources to develop comprehensive cybersecurity policies independently, receive the support they need to protect their digital assets effectively.

Furthermore, a national cybersecurity institute tailored to each sector would foster collaboration between the public and private sectors, resulting in a more cohesive and integrated approach to national cybersecurity. By encouraging information sharing and disseminating industry standards, the institute could help bridge the gap between SMEs and more giant corporations, ensuring that all businesses, regardless of size, are equipped to deal with the changing cyber threat landscape. A collaborative ecosystem would strengthen the security postures of individual SMEs while also contributing to the nation's overall economic resilience [14]. The institute would also promote financial stability and a secure and robust digital marketplace by safeguarding SMEs' digital infrastructure, frequently the backbone of many economies.

Discussion and Implications of the Integrative Literature Review

This integrative literature review (ILR) examines French SMEs' evolving digital transformation landscape and cybersecurity. The findings are consistent with previous studies, underlining the need to strategically combine digital technology and cybersecurity to foster growth and competitive advantage while reducing cyber risks. The results align with digital transformation and cybersecurity theories, emphasizing the importance of comprehensive and proactive solutions that incorporate both technological and cultural components. This agreement underscores SMEs' need to develop an integrated digital and cybersecurity strategies approach. Such integration is critical to achieving long-term organizational success and stability.

However, literature reveals several inconsistencies, particularly in the varying levels of cybersecurity readiness among SMEs [8]. This variation stems from differences in company culture, resource availability, and regulatory environments. While some SMEs have fully embraced digital transformation, others need more resources or knowledge to catch up. These findings suggest that future research should identify the barriers preventing SMEs from effectively implementing cybersecurity into their digital strategies. Addressing these gaps is crucial for building a more resilient SME sector.

Several factors influenced the interpretation of the findings, ranging from the diverse nature of the SME sector to the dynamic landscape of digital technology and cyber threats [53]. The diverse nature of the SME sector, encompassing various industries and sizes, makes a one-size-fits-all strategy impractical. Furthermore, the ever-changing landscape of digital technology and cyber threats complicates the creation of standardized frameworks that remain relevant over time. This ILR addresses these issues by highlighting the importance of adaptable and scalable cybersecurity measures tailored to the specific

needs of different SMEs. This personalized approach ensures that cybersecurity initiatives are both practical and relevant.

The findings of this ILR not only address the study's problem and objective but also provide a unique and comprehensive examination of the relationship between digital transformation and cybersecurity in French SMEs. This study introduces new knowledge to the existing literature by emphasizing the importance of organizational culture and the need for adaptable regulatory frameworks. It underscores the significance of specialized plans that combine digital transformation efforts with cybersecurity measures to ensure long-term growth and resilience. These insights lay the groundwork for more effective digital and cybersecurity initiatives, offering a fresh perspective to the field.

The findings have significant implications for business leaders and policymakers. The study stresses the importance of implementing comprehensive digital transformation strategies incorporating robust cybersecurity safeguards for SMEs. Managers should prioritize creating a security-conscious culture within their organizations, ensuring all employees understand and adhere to cybersecurity best practices. Continuous training and professional development are essential for maintaining a competent and resilient workforce capable of navigating the challenges of digital transformation [11]. For SMEs, emphasizing education and fostering a strong cybersecurity culture is critical for achieving long-term success.

For policymakers, the study emphasizes the necessity of targeted government assistance in supporting digital transformation and enhancing cybersecurity in SMEs. That includes providing financial incentives, technical assistance, and clear regulatory requirements that SMEs can comprehend and implement. Creating sector-specific cybersecurity legislative frameworks and a national cybersecurity institution could be crucial for providing targeted resources and support, bridging the gap between national policy and local implementation. Such an initiative will play an essential role in enhancing SME capacity. Effective government intervention is vital for a secure and competitive SME sector.

This ILR study generates new knowledge that advances practice and provides SMEs with practical and actionable insights and approaches for merging digital transformation and cybersecurity. Virtual cybersecurity laboratories provide training that guarantees personnel at all levels, from entry-level to senior, can detect and mitigate potential hazards through hands-on, immersive learning. Establishing a national cybersecurity institute tailored to each industry would provide SMEs with the resources, training, and assistance needed to construct their cybersecurity architecture, ultimately improving their security and resilience. Additionally, sectorial cybersecurity regulatory frameworks can provide SMEs with targeted resources, professional assistance, and practical solutions to help them navigate the challenges of digitalization and cybersecurity within the framework. This comprehensive approach guarantees that SMEs are well-prepared to deal with the changing cyber threat landscape while reaping the full benefits of digital transformation.

Furthermore, this research promotes positive social change and directly contributes to achieving the United Nations' Sustainable Development Goals (SDGs), particularly Goals 8 (Decent Work and Economic Growth) and 9 (Industry, Innovation, and Infrastructure). By fostering a secure and innovative digital environment, SMEs can drive economic growth and create job opportunities, thereby contributing to a more equitable and resilient economy [30]. The study's recommendations align with these global goals, promoting sustainable development. This connection emphasizes the broader implications of integrating digital and cybersecurity efforts, making it a crucial resource for policymakers.

Future Recommendations for Practice and Policy

Future studies should identify the obstacles preventing SMEs from effectively implementing cybersecurity into their digital strategies. The findings of this ILR reveal that while some SMEs have successfully embraced digital transformation, others lag due to a lack of resources, knowledge, and diverse corporate cultures. Studies should aim to delve deeper into Addressing SME cybersecurity barriers and suggesting tailored solutions that consider the various challenges SMEs face across industries and geographies [34]. That is likely to allow academics to build focused strategies that address specific constraints and facilitate the integration of cybersecurity into digital transformation activities. Such research projects will contribute to a more secure and resilient SME sector.

To expand on the strengths of this ILR, future research should look at the development and implementation of adaptive and scalable cybersecurity frameworks tailored to the specific needs of distinct SMEs. The ever-changing nature of digital technology and cyber dangers necessitates flexible and easily updated frameworks [35]. Such frameworks would equip SMEs with the tools they need to stay ahead of emerging threats. Future studies might evaluate their efficiency in real-world circumstances, providing valuable insights into their practical relevance and effects on SMEs' resilience and competitiveness. That will help ensure cybersecurity safeguards stay relevant and practical as the technological landscape evolves.

Another key topic for future research is the impact of government action in improving cybersecurity in SMEs. This study underlines the importance of targeted government support, such as financial incentives, technical assistance, and explicit regulatory requirements. Researchers should assess current government initiatives' performance and identify improvement areas. Comparative research across regions may uncover best practices and effective government assistance models that can be implemented elsewhere. Understanding the impact of government policies can help design more effective and supportive frameworks for SMEs [10].

Given the discovered disparities in cybersecurity readiness among SMEs, future research should look into how organizational culture affects the adoption of cybersecurity measures. The study found that a proactive, inventive, and security-conscious culture is required for successful digital transformation and cybersecurity integration. Researchers should investigate how organizational culture can be established and the role of leadership in facilitating this development. Longitudinal research may indicate how cultural shifts influence cybersecurity procedures over time. These insights can help SMEs build a security-first attitude [50].

This paper strongly encourages the establishment of national cybersecurity institutes customized to each industry that would provide SMEs with localized assistance and resources. Future research should explore the viability and usefulness of such institutions in providing targeted resources, professional guidance, and practical solutions to SMEs. Developing pilot initiatives to establish such institutions in specific places can effectively test the concept and acquire insights for future, more comprehensive implementation [19]. Academics can run pilot projects to evaluate the findings and offer best practices based on the results. This cyclical process allows for refining the institute's structure, curriculum, and operational processes before expanding the concept to additional countries.

Future researchers should plan their investigations with the limitations of this study in mind. This ILR was hampered by a lack of current data and a narrow focus on French SMEs. Expanding the scope to include SMEs from diverse countries and regions may provide a more complete picture of the global challenges and opportunities in digital transformation and cybersecurity [15]. Furthermore, combining

qualitative and quantitative approaches may improve the findings and provide a more thorough insight into SMEs' experiences and needs. Addressing these restrictions will yield more comprehensive and relevant insights.

The next logical step in this research is to develop and test particular interventions based on this study's findings. That could involve creating and implementing training programs for SME employees, designing comprehensive digital transformation strategies that include cybersecurity from the outset, and forming public-private partnerships to support SMEs. This collaborative approach will facilitate the translation of research findings into actionable solutions [7]. Testing such collaborative work in real-world contexts will provide vital feedback and allow for further development. Researchers should work with industry stakeholders to make sure that such initiatives are viable, scalable, and tailored to the needs of SMEs.

All in all, the findings of this ILR emphasize the critical necessity for a holistic, culturally aligned, and well-supported approach to combining digital transformation and cybersecurity in French SMEs. Establishing specialized institutions, cultivating security-conscious company culture, and ensuring strong government support are critical steps for a safe digitalization [14]. Future research can considerably improve SMEs' resilience, competitiveness, and operational security in the digital age by addressing these issues. The future of practice and policy in this subject will depend on continued collaboration and innovation to meet the changing problems and opportunities in the digital landscape [13]. Continued efforts will ensure that SMEs are prepared to prosper in the digital age.

Conclusions

In recent years, digital transformation has been critical for strengthening French SMEs' operational and strategic capacities, increasing efficiency, broadening market reach, and raising competitiveness. Studies have shown that embracing digital technologies has enabled SMEs to streamline processes, reduce costs, and access new markets, driving business growth and innovation [14]. However, this transformation has brought significant concerns, particularly regarding cybersecurity and equal access to technology. This integrated literature review (ILR) emphasizes the need to tackle these concerns so that SMEs may fully benefit from digital transformation while maintaining strong cybersecurity measures.

The problem raised in this ILR is the difficulties SMEs experience in implementing cybersecurity safeguards while undergoing digital transformation. Establishing a national cybersecurity institute customized to each industry may improve security measures while strengthening the nation's economic resiliency. Such an institute would serve as a centralized entity, providing SMEs with the resources, training, and assistance required to build their cybersecurity architecture. Specialist advice and easy access to cutting-edge technologies enable SMEs to adopt best practices and implement effective security processes, lowering the risks associated with cyber-attacks [31].

This study aims to look into how French SMEs can successfully undertake digital transformation while also implementing cybersecurity measures to boost organizational resilience and competitiveness. Creating sectorial cybersecurity regulatory frameworks can give SMEs targeted resources, professional advice, and practical solutions to help them negotiate the problems of digitalization and cybersecurity within the framework. By focusing on sector-specific requirements and challenges, these frameworks can help SMEs navigate their unique legal, technological, and economic environments, successfully bridging the gap between national policy and local implementation.

The significance of this study lies in its urgent call for French SMEs to incorporate cybersecurity measures into their operational strategy. This integration enables them to harness digital transformation while remaining competitive and secure in the global market [16]. It is crucial to foster a proactive organizational culture through employee training and ongoing risk assessment. Training provided by virtual cybersecurity laboratories ensures that all employees, from entry-level to senior, have the knowledge and skills to detect and manage potential hazards. This proactive approach helps to prevent security breaches, which are often caused by human error or a lack of awareness.

This ILR underscores the importance of seamlessly integrating cybersecurity measures into SMEs' digital transformation initiatives. The establishment of sector-specific cybersecurity legislative frameworks and a national cybersecurity institution can provide SMEs with the resources, training, and assistance they need to build their cybersecurity infrastructure. This integrated approach ensures that government initiatives are effectively implemented, leading to a more inclusive and resilient digital economy. By addressing these issues, the ILR lays the groundwork for future research and policy development, ensuring that digital transformation serves as a catalyst for innovation and growth rather than a barrier.

References

1. Peillon S, Dubruc N, Barriers to digital servitization in French manufacturing SMEs, Procedia CIRP, 2019, 83, 146-150, doi:10.1016/j.procir.2019.04.008
2. Telukdarie A, Dube T, Matjuta P, Philbin S, The opportunities and challenges of digitalization for SME's, Procedia Comput Sci, 2023, 217, 689-698, doi:10.1016/j.procs.2022.12.265
3. Azevedo AL, Almeida A, Grasp the challenge of digital transition in SMEs—a training course geared towards decision-makers, Educ Sci, 2021, https://api.semanticscholar.org/CorpusID:233645798
4. Saeed S, Altamimi SA, Alkayyal NA, Alshehri E, Alabbad DA, Digital transformation and cybersecurity challenges for businesses resilience: issues and recommendations, MDPI, 2023 Jul, 23(15), doi:10.3390/s23156666
5. SlideShare [Internet], Digitalization of SMEs in Germany and France, Digital Journeys and In-Depth Analysis, 2021, https://www.slideshare.net/slideshow/digitalization-of-smes-in-germany-and-france-digital-journeys-and-indepth-analysis/247621312
6. Verhoef PC, Broekhuizen T, Bart Y, Bhattacharya A, Dong QJ, Fabian N, et al, Digital transformation: a multidisciplinary reflection and research agenda, J Bus Res, 2021,122:889-901, doi:10.1016/j.jbusres.2019.09.022
7. Kallmuenzer A, Mikhaylov A, Chelaru M, et al, Adoption and performance outcome of digitalization in small and medium-sized enterprises, Rev Manag Sci, 2024, doi:10.1007/s11846-024-00744-2
8. Damiano JP, La cybersécurité : contexte, enjeux, constats et perspectives cybersecurity: context, issues, findings and outlook, 2023 Feb 7.
9. Brodin M, A framework for GDPR compliance for small- and medium-sized enterprises, Eur J Secur Res, 2019, 4, 243-264, doi:10.1007/s41125-019-00042-z
10. Gevorgyan A, de Rocca Serra O, La transformation digitale dans les entreprises : attentes et retombées, 2020 Nov 26.

11. Ibrahimi G, Benchekroun B, The contribution of agility to an organization's digital transformation, TEM J. 2023, https://api.semanticscholar.org/CorpusID:265537823
12. France - national plan for digital inclusion | digital skills and jobs platform [Internet], [cited 2024 May 6], https://digital-skills-jobs.europa.eu/en/actions/national-initiatives/national-strategies/france-national-plan-digital-inclusion
13. Jacob S, Defacqz S, Agossou N, Promesses et défis de la transformation numérique du secteur public, 2022 Dec 2.
14. Goh ZJ, Singh J, Digitalization and its Impact on Small and Medium-sized Enterprises (SMEs): An Exploratory Study of Challenges and Proposed Solutions, Int J Bus Technol Manag, 2023 Dec, 5(4), 238-255, ISSN 2682-7646, https://myjms.mohe.gov.my/index.php/ijbtm/article/view/24997
15. Hervé A, Schmitt C, Baldegger R, Internationalization and digitalization: applying digital technologies to the internationalization process of small and medium-sized enterprises, Technol Innov Manag Rev, 2020, 10, 29-41
16. European commission, Directorate general for economic and financial affairs, 2023 country report: France [Internet], LU: Publications Office, 2023 [cited 2024 May 3], doi:10.2765/9757
17. Enhancing sustainable business by SMEs' digitalization, J Strateg Innov Sustain, 2022, 17(1), doi:10.33423/jsis.v17i1
18. Burinskienė A, Nalivaikė J, Digital and sustainable (Twin) transformations: a case of SMEs in the european union, Sustainability, 2024, 16(4), 1533, doi:10.3390/su16041533
19. Verma R, Cybersecurity challenges in the era of digital transformation, In: 2024, p. 187, doi:10.25215/9392917848.20
20. Spencer P, Understanding the evolving cybersecurity threat landscape in France [Internet], Kiteworks | Your Private Content Network, 2023 [cited 2024 May 6], https://www.kiteworks.com/cybersecurity-risk-management/threat-landscape-in-france/
21. Philbin S, Viswanathan R, Telukdarie A, Understanding how digital transformation can enable SMEs to achieve sustainable development: a systematic literature review, Small Bus Int Rev, 2022, 6(1), e473, doi:10.26784/sbir.v6i1.473
22. Melo IC, Queiroz GA, Alves Junior PN, Sousa TB, Yushimito WF, Pereira J, Sustainable digital transformation in small and medium enterprises (SMEs): A review on performance, Heliyon, 2023 Feb 21, 9, e13908, doi:10.1016/j.heliyon.2023.e13908
23. Leso BH, Cortimiglia MN, Ghezzi A, The contribution of organizational culture, structure, and leadership factors in the digital transformation of SMEs: a mixed-methods approach, Cogn Tech Work, 2023, 25, 151-79, doi: 10.1007/s10111-022-00714-2 24
24. Wallang M, Shariffuddin M, Mokhtar M, Cyber security in small and medium enterprises (SMEs), J Gov Dev, 2022, 18(1), 75-87, doi: 10.32890/jgd2022.18.1.5
25. Elsbach KD, van Knippenberg D, Creating high-impact literature reviews: An argument for "integrative reviews", J Manag Stud, 2020, 57, 1277-89.
26. lahmari A, Duncan B, Cybersecurity risk management in small and medium-sized enterprises: a systematic review of recent evidence, 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), 2020 Jun 15-19, Dublin, Ireland, Piscataway (NJ): IEEE, 2020, p. 1-5, doi: 10.1109/CyberSA49311.2020.9139638
27. Omotunde H, Ahmed M, A comprehensive review of security measures in database systems: Assessing authentication, access control, and beyond, Mesopotamian J CyberSecurity, 2023, 2023,

115-33, doi: 10.58496/MJCSC/2023/016
28. Chaudhary S, Gkioulos V, Katsikas S, A quest for research and knowledge gaps in cybersecurity awareness for small and medium-sized enterprises, Comput Sci Rev, 2023, 50, 100592, doi: 10.1016/j.cosrev.2023.100592
29. Ingrid T, Silva TI, Braz P, Cavalcante R, Alves M, Diffusion of innovations theory and its applicability in research studies on nursing and health, Texto Contexto Enferm, 2022, 31,1-12, doi: 10.1590/1980-265X-TCE-2021-0322
30. Bozkus K, Organizational culture change and technology: navigating the digital transformation [Internet], Business, Management and Economics, IntechOpen, 2024, doi: 10.5772/intechopen.112903
31. Ameen N, Choudrie J, Jones P, Ramayah T, Morris S, Innovative technologies and small-medium sized enterprises in times of crisis, Inf Syst Front, 2022, 24, 1055-60, doi: 10.1007/s10796-022-10353-7
32. Mesa Manzano R, Esparcia Pérez J, Theoretical framework and methods for the analysis of the adoption-diffusion of innovations in agriculture: a bibliometric review, Bol Asoc Geogr Esp, 2023, (96), doi: 10.21138/bage.3336
33. Polojärvi D, Palmer E, Dunford C, A systematic literature review of sociotechnical systems in systems engineering, Syst Eng, 2023, 26, doi: 10.1002/sys.21664
34. Admass WS, Munaye YY, Diro AA, Cyber security: state of the art, challenges and future directions, Cyber Secur Appl, 2024, 2, 100031, doi: 10.1016/j.csa.2023.100031
35. Manulis M, Bridges CP, Harrison R, et al, Cyber security in new space, Int J Inf Secur, 2021, 20, 287-311, doi: 10.1007/s10207-020-00503-w
36. Hasani T, O'Reilly N, Dehghantanha A, Parizi RM, Hammoudeh M, Evaluating the adoption of cybersecurity and its influence on organizational performance, SN Bus Econ, 2023, 3:97, doi: 10.1007/s43546-023-00477-6
37. Moursellas A, De D, Wurzer T, et al, Sustainability practices and performance in european small-and-medium enterprises: insights from multiple case studies, Circ Econ Sust, 2023, 3, 835-60, doi: 10.1007/s43615-022-00224-3
38. Ramdani B, Raja S, Kayumova M, Digital innovation in SMEs: a systematic review, synthesis and research agenda, Inf Technol Dev, 2022, 28(1), 56-80, doi: 10.1080/02681102.2021.1893148
39. Ketonen-Oksi S, Vigren M, Methods to imagine transformative futures: an integrative literature review, Futures, 2024, 157, 103341, doi: 10.1016/j.futures.2024.103341
40. Omrani N, Rejeb N, Maalaoui A, Dabić M, Kraus S, Drivers of digital transformation in SMEs, IEEE Trans Eng Manag, 2024, 71, 5030-43, doi: 10.1109/TEM.2022.3215727
41. Taherdoost H, What are different research approaches? comprehensive review of qualitative, quantitative, and mixed method research, their applications, types, and limitations, J Manag Sci Eng Res, 2022, 5(1), 53-63, doi: 10.30564/jmser.v5i1.4538
42. Mwita K, Factors to consider when choosing data collection methods, Int J Res Bus Soc Sci, 2022, 11(5), 532-8, doi: 10.20525/ijrbs.v11i5.1842
43. Fernandez KV, Critically reviewing literature: a tutorial for new researchers, Australas Mark J, 2019, 27(3), 187-96, doi: 10.1016/j.ausmj.2019.05.001
44. Condon P, Simpson J, Emanuel M, Research data integrity: a cornerstone of rigorous and reproducible research, IASSIST Q, 2022, 46, doi: 10.29173/iq1033

45. Hirt J, Nordhausen T, Appenzeller-Herzog C, Ewald H, Citation tracking for systematic literature searching: A scoping review, Res Synth Methods, 2023, 14, doi: 10.1002/jrsm.1635
46. Martín-Martín A, Thelwall M, Orduna-Malea E, Delgado López-Cózar E, Google scholar, microsoft academic, scopus, dimensions, web of science, and open citations' COCI: a multidisciplinary comparison of coverage via citations, Scientometrics, 2021, 126, 871-906, doi: 10.1007/s11192-020-03690-4
47. Costa J, Castro R, SMEs must go online—e-commerce as an escape hatch for resilience and survivability, J Theor Appl Electron Commer Res, 2021, 16(7), 3043-62, doi: 10.3390/jtaer16070166
48. de Mattos CS, Pellegrini G, Hagelaar G, Trienekens J, Systematic literature review on technological transformation in SMEs: a transformation encompassing technology assimilation and business model innovation, Manag Rev Q, 2024, 74, 1057-95, doi: 10.1007/s11301-023-00327-7
49. Bowers J, Cybersecurity flaws make French industry vulnerable [Internet], Polytechnique Insights, 2023 [cited 2024 May 17], Available from: https://www.polytechnique-insights.com/en/columns/digital/cybersecurity-the-gaps-that-make-the-french-industry-vulnerable/
50. Jeong JJ, Oliver G, Kang E, Stewart G, The current state of research on people, culture and cybersecurity, Pers Ubiquit Comput, 2021, 25, 809-12, doi: 10.1007/s00779-021-01591-8
51. Aksoy C, Building a cyber security culture for resilient organizations against cyber attacks, İşletme Ekonomi ve Yönetim Araştırmaları Dergisi, 2024, 7, 96-110, doi: 10.33416/baybem.1374001
52. Motjolopane I, Chanza M, Digital transformation dimensions for evaluating SMEs' readiness for big data analytics and artificial intelligence: A review, Int J Res Bus Soc Sci, 2023, 12, 583-95, doi: 10.20525/ijrbs.v12i7.2837
53. Mishra B, Kumar A. How does regulatory framework impact sectoral performance? A systematic literature review, Int J Prod Perform Manag, 2023, 72(5), 1419-44, doi: 10.1108/IJPPM-07-2021-0398
54. Kumar S, Singh P, An analysis of government support programs for small business development and growth, Scholedge Int J Bus Policy Gov, 2023,10, 8, doi: 10.19085/sijbpg100201
55. Wang Z, Digital transformation and risk management for SMEs: a systematic review on available evidence, Adv Econ Manag Polit Sci, 2023, 65, 209-18, doi: 10.54254/2754-1169/65/20231639