

## Advances in Business & Industrial Marketing Research


<https://advancesinresearch.id/index.php/ABIM>

This Work is Licensed under a Creative Commons Attribution 4.0 International License



# Digital Technology Adaptation Challenges to Enhance Growth and Security of Corporate Online Businesses


Chicilia Nova Yatna  Sylvia Yuanita Banjuradja <sup>2</sup> Sutrisno <sup>3</sup> Noor Ritawaty <sup>4</sup>

 Perbanas Institute Jakarta, Jakarta Selatan, Daerah Khusus Ibukota Jakarta, 12940, Indonesia  
<sup>2,3,4</sup> STIE Pancasetia Banjarmasin, Kalimantan Selatan, 70248, Indonesia

Received: 2025, 01, 02 Accepted: 2025, 01, 30

Available online: 2025, 01, 31

Corresponding author: Chicilia Nova Yatna

 [chicilia.yatna@perbanas.id](mailto:chicilia.yatna@perbanas.id)

KEYWORDS	ABSTRACT
<p><b>Keywords:</b></p> <p>Digital technology adaptation, cybersecurity challenges, organizational innovation, Technology Acceptance Model, corporate online businesses.</p> <p><b>Conflict of Interest Statement:</b></p> <p>The author(s) declares that the research was conducted without any commercial or financial relationships that could be construed as a potential conflict of interest.</p> <p><b>Copyright © 2025 ABIM. All rights reserved.</b></p>	<p><b>Purpose:</b> This study examines the challenges of digital technology adaptation faced by corporate online businesses, focusing on the interplay between growth opportunities and security requirements. The study aims to comprehensively understand technical, security, and organizational barriers while offering actionable strategies to overcome these obstacles.</p> <p><b>Research Design and Methodology:</b> The study employs a qualitative systematic literature review (SLR) methodology to synthesize findings from recent scholarly contributions. The review integrates theoretical frameworks such as the Technology Acceptance Model (TAM) and organizational innovation theories to contextualize digital adaptation's challenges and potential solutions.</p> <p><b>Findings and Discussion:</b> The findings reveal that successful digital adaptation is hindered by technical complexities such as integrating AI and IoT, cybersecurity threats, including ransomware and phishing, and organizational resistance due to limited digital literacy and employee readiness. A holistic approach that combines robust security measures, employee training programs, and cultural transformation is critical for addressing these challenges. The discussion highlights the importance of aligning organizational strategies with advanced technologies to foster operational resilience and market competitiveness.</p> <p><b>Implications:</b> This study provides valuable insights for business leaders and policymakers. Practically, it emphasizes the need for proactive security integration, workforce upskilling, and leveraging AI for enhanced operational efficiency. From a managerial perspective, fostering innovation-supportive cultures and aligning technological strategies with organizational goals is critical. Policymakers are encouraged to create regulatory frameworks that balance technological innovation with robust security measures to promote sustainable business growth.</p>

## Introduction

The rapid advancement of digital technology has profoundly reshaped the global business landscape, redefining how organizations operate, innovate, and compete. Digital transformation is no longer an optional strategy but a critical requirement for businesses seeking to thrive in the modern economy. Technologies such as artificial intelligence (AI), the Internet of Things (IoT), and cloud computing have introduced powerful tools that allow companies to streamline operations, deliver personalized customer experiences, and respond to rapidly changing market demands. For instance,

the explosive growth of e-commerce and the proliferation of digital platforms illustrate how these innovations have fundamentally altered traditional business models, enabling companies to expand their reach and access global markets with unprecedented ease. The adoption of these technologies also drives cost efficiencies, facilitates data-driven decision-making, and enhances collaboration across organizational silos. Despite these significant opportunities, the path toward successful digital adaptation is fraught with practical and theoretical challenges. Companies must navigate complex technological landscapes while addressing significant operational, cultural, and financial barriers. The difficulty lies in adopting and aligning these innovations with organizational capabilities and strategic objectives. Moreover, this process often demands substantial financial investment, long-term commitment, and a willingness to embrace continuous change. Consequently, understanding the implications of digital transformation is essential for appreciating its broader impact on the sustainability and resilience of corporate strategies. Delving deeper, the challenges associated with digital adaptation become increasingly evident, particularly for businesses that operate predominantly online. A primary obstacle lies in the constraints posed by legacy systems that are often outdated and incompatible with modern digital technologies. This technical disconnect results in integration difficulties that can stifle innovation and hinder operational agility. Compounding this issue is a significant skills gap within many organizations, where employees may lack the technical expertise necessary to leverage these advanced technologies effectively. Additionally, resistance to change remains a pervasive issue within corporate cultures, where traditional mindsets and entrenched processes often clash with digital transformation's dynamic and fast-paced demands. Beyond these internal hurdles, external challenges such as the ever-present threat of cybersecurity breaches further complicate the digital adaptation process. Corporate online businesses, which rely heavily on digital platforms, are particularly vulnerable to these threats, facing data breaches, ransomware attacks, and system vulnerabilities. These incidents disrupt operations, erode stakeholder trust, and damage organizational reputations. For example, highly publicized data breaches have demonstrated the severe consequences of inadequate digital security measures, highlighting the critical importance of integrating robust cybersecurity strategies into the broader digital transformation framework. Addressing these interconnected challenges is vital for businesses seeking to navigate the complexities of digital adaptation while achieving sustainable growth and maintaining operational security in a highly volatile digital environment.

Recent studies emphasize the multifaceted nature of digital transformation, illustrating the interplay of challenges and opportunities that businesses encounter in this complex process. Syamsuddin et al. (2024) highlight several critical obstacles, including organizational resistance to change, a significant shortage of digital skills within the workforce, reliance on outdated legacy systems, and the persistent threat of cybersecurity breaches. To mitigate these challenges, organizations are increasingly channeling investments toward digital infrastructure, upskilling employees to enhance technological proficiency, and fostering a culture of innovation that supports adaptability. These efforts aim to create a resilient organizational framework capable of navigating the rapidly evolving technological landscape. Similarly, Vera Maria et al. (2024) discuss the transition toward Industry 5.0, which is characterized by the integration of advanced technologies such as artificial intelligence (AI), the Internet of Things (IoT), and Big Data. This evolution represents a pivotal step for organizations striving to improve operational efficiency and enhance decision-making processes. However, they caution that such advancements demand substantial financial commitments and must be accompanied by ethical considerations to ensure responsible implementation. Benga and Elhamma (2024) further assert that successful digital transformation requires well-defined strategic frameworks, meaningful stakeholder engagement, and a willingness to adapt continuously to emerging technological trends. Ambo Upe (2023) underscores the vital role of digital technology adaptation in maintaining organizational competitiveness in an increasingly digitalized market. Meanwhile, Ionescu et al. (2022) emphasize the importance of institutional frameworks, including the Rule of Law and Government Effectiveness, in facilitating the adoption of digital technologies. Nonetheless, Bartczak (2021) warns of the detrimental impact of unresolved cybersecurity threats on managerial confidence in digital platforms, underscoring the necessity of addressing security concerns to encourage widespread adoption.

While the existing body of literature provides a robust understanding of the broader dynamics of digital transformation, notable gaps persist between theoretical models and practical realities. Many studies emphasize the strategic advantages and technical frameworks required for digital adoption. Yet, they often fail to delve deeply into the dual challenges of achieving growth and ensuring security within corporate online businesses. For example, research by Syamsuddin et al. (2024) and Benga and Elhamma (2024) focuses extensively on organizational readiness and stakeholder engagement yet provides a limited analysis of how these factors interact with security threats such as data breaches or cyberattacks in the context of digital transformation. This omission is critical, as the security dimension plays a pivotal role in determining the success and sustainability of digital adaptation efforts. Further gaps are evident in digital technology adaptation's ethical and institutional dimensions. Vera Maria et al. (2024) highlight the ethical considerations associated with Industry 5.0 advancements. Yet, practical applications of these considerations remain underexplored, especially in regions where governance and regulatory frameworks are insufficiently developed to support such transitions. Similarly, Ionescu et al. (2022) emphasize the importance of institutional support, but empirical analyses of how these frameworks influence real-world digital adaptation efforts are sparse. Bartczak's (2021) findings on cybersecurity threats underscore the growing importance of risk mitigation strategies; however, there remains a limited examination of how businesses can balance the imperatives of growth and security in volatile digital environments. This study addresses these gaps by comprehensively analyzing the interplay between growth opportunities and security challenges in corporate online businesses, providing valuable insights to bridge the disconnect between theoretical discourse and empirical practice.

This study offers a unique contribution by employing a systematic literature review (SLR) methodology to investigate digital technology adaptation's interconnected growth and security challenges. Unlike prior research focusing on the technical aspects of digital transformation or its strategic benefits, this study explores the nuanced interplay between technological innovation, organizational dynamics, and risk management within corporate online businesses. The novelty of this research lies in its ability to bridge theoretical gaps and empirical inconsistencies identified in prior studies. Specifically, while many researchers have highlighted the benefits of digital adoption, few have addressed how businesses can balance their growth imperatives with the increasing need for robust cybersecurity measures in a highly volatile and competitive digital landscape. By synthesizing insights from recent academic contributions, this study focuses on two critical research questions: (1) What are the primary challenges of digital technology adaptation faced by corporate online businesses? (2) How do these challenges influence the ability of businesses to balance growth opportunities with security requirements? Through these inquiries, the study seeks to provide a comprehensive understanding of the barriers and enablers of successful digital adaptation. The findings are intended to offer actionable recommendations for business leaders and policymakers, aiming to establish practical frameworks for navigating the complexities of digital transformation while maintaining operational resilience. This research underscores the urgent need for a more integrated approach to understanding and addressing the dual challenges that define the digital transformation journey in corporate online businesses.

## Literature Review

### *Technology Acceptance Model (TAM)*

The Technology Acceptance Model (TAM) is a robust theoretical framework for understanding how individuals and organizations adopt and use new technologies. Introduced by Davis (1989), TAM emphasizes two core constructs: perceived usefulness (PU) and perceived ease of use (PEOU). Recent studies, such as Al-Qaysi et al. (2020), have demonstrated how TAM continues to evolve, particularly in its application to emerging technologies like social media and advanced communication platforms. Their findings illustrate that PU remains a critical determinant of user acceptance, as individuals often prioritize technology's benefits in enhancing productivity and efficiency. The adaptability of TAM to diverse contexts has been explored extensively. Florenthal (2019) applied the model within the domain of social media branding, revealing that PEOU significantly influences user engagement with technology when platforms are intuitive and user-friendly. Similarly, Weerasinghe & Hindagolla (2018)

highlighted the importance of extending TAM by integrating motivational factors specific to social network sites, where ease of use amplifies perceived value. The relevance of TAM has also been reaffirmed in its application to evolving technologies. Ishengoma (2024) revisited the model to address advanced technological ecosystems, suggesting that future applications of TAM must consider adaptive behaviors and the dynamic interaction between users and sophisticated systems. These perspectives underscore the enduring value of TAM in addressing challenges related to technology adoption and adaptation in various contexts.

The Technology Acceptance Model (TAM) remains a pivotal framework for analyzing how businesses and consumers adopt new technologies. TAM continues to evolve, adapting to the complexities of digital innovation. Recent studies have expanded its application in diverse areas, particularly online business and e-commerce. For instance, Ritz et al. (2019) explored TAM in the context of small business digital marketing adoption, emphasizing the significance of perceived usefulness (PU) and perceived ease of use (PEOU) in driving successful adoption strategies. Their findings underline that businesses are more likely to adopt digital tools when the perceived benefits align with operational goals. The integration of TAM with other models has become increasingly common. Lai et al. (2025) combined TAM with the Value-Based Adoption Model (VAM) to assess consumer perceptions of augmented reality (AR) in online shopping. This integration highlights how emotional and rational factors shape consumer adoption behavior alongside PU and PEOU. Similarly, Al-Emran & Shaalan (2021) provided a bibliometric analysis of TAM's applications from 2010 to 2020, demonstrating its relevance in education and social media. Expanding TAM's theoretical scope, Saravanos et al. (2022) incorporated the concept of "warm-glow" into TAM, examining how affective motivations influence technology acceptance. These studies illustrate TAM's adaptability and enduring relevance in analyzing digital technology adoption, offering valuable insights for academic and practical applications.

#### *Digital Technology Adaptation*

Digital technology adaptation is a transformative process integrating new technologies into a company's operational and strategic frameworks, fostering efficiency, innovation, and customer engagement. Artificial intelligence (AI), cloud computing, and the Internet of Things (IoT) have emerged as foundational technologies in this transition. Ardito et al. (2024) highlight how the synergy between AI, IoT, and big data analytics can drive significant revenue growth in European SMEs, illustrating the importance of these technologies in business transformation. As Xue et al. (2021) emphasize, cloud computing offers decentralized data management that enhances operational flexibility and efficiency, particularly in banking and e-commerce sectors where data security and scalability are paramount. The role of IoT is equally significant, enabling interconnected devices to support real-time, data-driven decision-making. Botta et al. (2016) describe the integration of cloud computing and IoT as a critical step for businesses seeking to optimize supply chains and improve customer experiences. Furthermore, Wirtz (2021) explores how these technologies collectively contribute to digital business strategies, enabling companies to respond dynamically to market demands. Applications of these technologies are evident in e-commerce platforms, where AI-powered tools personalize product recommendations and IoT optimizes supply chains. These advancements create new value for businesses and help them maintain competitiveness in rapidly evolving markets. The convergence of AI, cloud computing, and IoT underscores their pivotal role in shaping the future of digital business adaptation.

Organizations must adopt a structured and strategic approach to ensure the successful adaptation of digital technology. The process begins with assessing the readiness of their technological infrastructure and determining the compatibility of new technologies with customer needs and regulatory standards. Berman et al. (2024) emphasize that such evaluations help organizations identify barriers and formulate mitigation strategies to address them effectively. Alongside infrastructure readiness, organizational learning and employee training are critical components. Schiuma et al. (2022) highlight that leadership competencies in driving digital transformation must focus on empowering employees to maximize the potential of new technologies. Flexibility and continuous updates in organizational processes are crucial for keeping pace with technological advancements.

Kowalski et al. (2024) argue that dynamic capabilities at the micro-level allow businesses to adapt quickly and seize emerging market opportunities. This agility is vital in the competitive online business landscape, where rapid adaptation often determines a company's survival. Integrating digital technologies, such as AI and IoT, significantly enhances operational efficiency, reduces costs, and accelerates production processes. Cosa (2024) further notes that personalized customer experiences enabled by these technologies play a pivotal role in fostering customer loyalty and competitive advantage. By embedding these strategies into their core operations, businesses support growth objectives and solidify their market presence in a rapidly evolving global economy.

#### *Growth Through Digital Technology*

Growth through digital technology is a strategic approach that enables businesses to enhance productivity, efficiency, and innovation in competitive markets (Syahnur, 2024). Digital transformation is increasingly vital as companies integrate artificial intelligence (AI), machine learning, and data analytics to optimize processes and create sustainable advantages. Zhao et al. (2024) emphasize that digital transformation enhances firm performance by aligning technological advancements with organizational objectives, allowing businesses to accelerate workflows and reduce operational costs. This alignment is critical for fostering growth in an era characterized by dynamic market changes. E-commerce platforms exemplify how digital technology facilitates global market access and cross-border sales. These platforms also enable data-driven decision-making, as highlighted by Yang (2023), who examines how AI improves service quality and enhances customer co-creation experiences. Such personalization, powered by AI and machine learning, allows companies to predict trends, refine pricing strategies, and deliver tailored customer experiences. Singh et al. (2024) further explore the role of AI in customer retention, identifying its capacity to transform customer relationship management through predictive insights and engagement strategies. Willcocks (2024) discusses how automation and digitalization redefine the future of work, emphasizing that adapting to these technologies ensures sustainability and competitive resilience. These insights illustrate that leveraging digital technology is an operational upgrade and a transformative strategy essential for sustained growth and innovation.

Growth through digital technology involves leveraging modern tools to enhance productivity, efficiency, and innovation, enabling businesses to remain competitive in dynamic markets. Akter et al. (2016) emphasize that digital transformation significantly improves firm performance by aligning technological advancements with strategic objectives. This alignment enables organizations to accelerate workflows, optimize resources, and reduce operational costs. Furthermore, Chandra & Rahman (2024) highlight that artificial intelligence (AI) enhances customer co-creation experiences by aligning AI functionalities with user capabilities, which fosters more personalized and effective engagement strategies. E-commerce platforms exemplify how digital technologies expand market reach and create new revenue streams. According to Rane et al. (2024), AI plays a critical role in customer retention by offering predictive insights that help businesses refine their approaches to meet consumer demands. The integration of data analytics allows companies to optimize market segmentation and implement targeted marketing strategies. Willcocks (2023) discusses how automation and digitalization reshape the workforce, stressing the importance of adaptability for sustaining growth in a technologically driven economy. Machine learning further enhances personalization efforts by predicting market trends and optimizing pricing strategies. By embedding these tools into operational frameworks, businesses respond to rapid changes in consumer behavior and create sustainable competitive advantages. Together, these advancements highlight the transformative potential of digital technologies in driving long-term growth and innovation.

#### *Security in Digital Adaptation*

Security has become a critical concern in digital technology adaptation due to the growing reliance of businesses on digital platforms for operations and customer interactions. Cyber threats like hacking, ransomware, and phishing pose significant risks to corporate systems and data integrity. Kuzlu et al. (2021) highlight the role of artificial intelligence (AI) in enhancing cybersecurity within the Internet of Things (IoT), emphasizing its ability to detect and mitigate threats in real-time. These advancements



are essential as cybercriminals continuously exploit vulnerabilities in digital systems, often targeting inadequately secured networks. Another challenge lies in the lack of employee awareness and training, which makes them vulnerable to social engineering attacks like phishing. Radanliev et al. (2020) discuss how cyber risk analytics and AI are increasingly being applied in industrial IoT and supply chains to address such vulnerabilities proactively. Furthermore, Wang et al. (2024) argue that a managerial focus on cybersecurity is crucial for mitigating risks in digital banking, a sector heavily reliant on customer trust and operational integrity. Emerging technologies, while transformative, often introduce new security challenges. Prajapati & Singh (2022) emphasize that IoT devices, without robust security measures, can serve as entry points for cyberattacks. These findings underscore the importance of integrating advanced security protocols and comprehensive employee training into digital adaptation strategies to protect organizational assets and maintain customer trust.

Addressing security challenges in adapting digital technology requires a holistic and proactive approach. Companies must implement fundamental measures such as data encryption, multi-factor authentication, and continuous monitoring. These tools are essential for safeguarding corporate assets against cyber threats. Zhang et al. (2022) emphasize that artificial intelligence (AI) can enhance these efforts by identifying and mitigating potential real-time vulnerabilities, particularly in evolving cyber threats. However, Catal et al. (2023) argue that technological solutions alone are insufficient without adequately addressing knowledge gaps in cybersecurity. They highlight the importance of employee education as a critical component of organizational resilience. Integrating security strategies into the early stages of technology adaptation is another vital aspect. Creese et al. (2021) stress that embedding security into an organization's cultural and operational fabric builds long-term capacity to handle cyber risks effectively. Furthermore, Kozanoglu & Abedin (2021) identify digital literacy as an organizational affordance that strengthens employee capabilities, enabling them to recognize and counteract potential threats like phishing attacks. A robust security framework protects assets, and fosters trust among customers. Organizations demonstrating a commitment to data protection enhance customer loyalty and business resilience. This integration of proactive security strategies positions businesses to maintain operations and leverage competitive advantages in an increasingly complex digital economy. Security is thus both a defensive and strategic imperative.

## Research Design and Methodology

### *Study Design*

This research adopts a qualitative systematic literature review (SLR) methodology to analyze the challenges and strategies associated with digital technology adaptation and its implications for business growth and security. The SLR method provides a structured framework to synthesize existing academic literature, ensuring comprehensive coverage of relevant studies while minimizing bias. By following established guidelines for SLR, this study identifies, evaluates, and synthesizes scholarly works that contribute to a deeper understanding of the topic.

### *Sample Population or Subject of Research*

This research comprises peer-reviewed journal articles, conference papers, and academic book chapters published after 2015. Its focus is on studies on digital technology adaptation, cybersecurity challenges, and strategies in business contexts. Articles are sourced from prominent databases such as Elsevier, Springer, Wiley, and Emerald, ensuring the inclusion of high-quality and credible literature. Selection criteria emphasize relevance to the research objectives, originality, and methodological rigor.

### *Data Collection Techniques and Instrument Development*

Data collection involves a systematic search of academic databases using specific keywords such as "digital technology adaptation," "cybersecurity," "automation," and "IoT." Boolean operators and filters (e.g., publication year, peer-reviewed status) are applied to refine search results. A protocol is developed to screen titles, abstracts, and full texts for eligibility. The PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) framework ensures a transparent and replicable selection process.

### *Data Analysis Techniques*

Data analysis is conducted through thematic synthesis, where findings from selected studies are categorized into key themes, such as implementation strategies, security challenges, and organizational impact. NVivo software is employed to manage and code qualitative data, facilitating the identification of patterns and relationships. This systematic approach enables the development of a comprehensive narrative that integrates theoretical insights with practical implications, ensuring the study's relevance and academic contribution.

## **Findings and Discussion**

### ***Findings***

Digital technology adaptation presents significant challenges that businesses must address to maintain competitive advantage and operational efficiency. One major challenge lies in the technical domain, where integrating legacy systems with advanced technologies like AI and IoT often demands substantial resources and time. Ardito et al. (2024) emphasize that while these technologies offer synergies that enhance efficiency, they require scalable and flexible infrastructure, which many organizations lack. Additionally, scalability constraints can prevent businesses from fully utilizing technological advancements, limiting their ability to innovate and expand. Cybersecurity is another critical issue; ransomware, phishing, and hacking are becoming increasingly sophisticated, targeting vulnerabilities within organizational systems (Zhang et al., 2022). These threats compromise data integrity, disrupt operations, and undermine customer trust, making cybersecurity a top priority for digital adaptation. Organizational challenges also play a significant role. Resistance to change and low levels of digital literacy among employees often hinder the adoption of new technologies. Kozanoglu & Abedin (2021) highlight that without adequate training and support, employees may struggle to utilize digital tools effectively, leading to inefficiencies and increased operational risks. A lack of innovation-friendly organizational culture exacerbates these issues, as employees may be reluctant to adopt new processes. To navigate these challenges, businesses must invest in technological infrastructure and prioritize employee readiness and cultural transformation. These interconnected technical, security, and organizational hurdles form a complex framework that companies must address to ensure successful digital adaptation.

The challenges associated with digital technology adaptation have profound implications for the growth of online businesses. Technical and security barriers can significantly limit the ability of companies to achieve key objectives, such as automation, personalization, and process optimization, which are critical to maintaining a competitive edge. Wang et al. (2024) emphasize that cybersecurity vulnerabilities, particularly in sensitive sectors like banking, not only disrupt operations but also erode customer trust, which is essential for sustaining long-term growth. When businesses fail to address technical inefficiencies, they risk operational bottlenecks that stifle innovation and reduce their ability to offer differentiated products or services. Customer loyalty is another critical area affected by these challenges. Breaches in data security or delays in technological responses can lead to dissatisfaction and loss of trust among consumers. Berman et al. (2024) argue that businesses operating in digital ecosystems must align technological capabilities with robust security measures to reassure customers and maintain engagement. Adaptability plays a central role in overcoming these challenges. Wirtz (2021) highlights that organizations capable of responding swiftly to technological changes and market demands are better positioned to seize opportunities and maintain market relevance. Conversely, businesses that lack agility may struggle to keep pace, resulting in stagnation and loss of competitive advantage. Therefore, addressing these challenges requires strategic investments in technology and a commitment to fostering agility and resilience across all organizational levels.

To effectively balance growth and security, businesses must adopt comprehensive strategies that address the multifaceted challenges of digital technology adaptation. One key strategy involves embedding security measures into digital transformation initiatives. Zhang et al. (2022) emphasize the importance of implementing advanced protocols, such as real-time threat monitoring, encryption, and multi-factor authentication, to mitigate risks while maintaining operational efficiency. These measures ensure that businesses can safeguard sensitive data while innovating and expanding. Another critical element is workforce development. Kozanoglu & Abedin (2021) argue that employee digital

literacy and cybersecurity awareness are fundamental to reducing vulnerabilities stemming from human error. Comprehensive training programs enable employees to identify and respond to potential threats, such as phishing attacks, among the most common cyber intrusions. Beyond employee development, businesses must also prioritize proactive innovation in security-focused technologies. Wirtz (2021) highlights the role of AI in predicting and mitigating cybersecurity risks, allowing organizations to stay ahead of evolving threats and integrate security seamlessly with their growth strategies. These strategies collectively create a framework that addresses immediate security concerns and positions businesses for sustainable growth. By ensuring that security measures are integral to digital adaptation, organizations can enhance their resilience, build customer trust, and maintain a competitive edge in rapidly evolving digital markets. The balance between growth and security is not a trade-off but a mutually reinforcing process critical for long-term success.

While digital technology adaptation poses challenges, it also unlocks substantial opportunities for businesses to enhance growth and innovation. Technologies such as AI-driven analytics and IoT provide organizations with tools to optimize market segmentation, personalize customer experiences, and streamline operations. Yang (2023) emphasizes that AI-powered systems enable companies to analyze consumer preferences in real time, creating opportunities for tailored marketing strategies that enhance customer loyalty. Additionally, e-commerce platforms and cloud computing allow businesses to expand their market reach, facilitating cross-border trade and creating new revenue streams (Xue et al., 2021). These technologies reduce operational costs and enable scalability, making it easier for businesses to adapt to changing market conditions. Digital adaptation accelerates decision-making processes, giving businesses a competitive advantage in dynamic markets. Zhao et al. (2024) highlight how companies that effectively integrate technologies like IoT and AI often outperform competitors by leveraging real-time data to optimize supply chains and predict market trends—the ability to respond quickly to consumer demands and technological advancements positions these businesses as industry leaders. Furthermore, digital adaptation fosters innovation by enabling organizations to develop new products and services that cater to evolving consumer needs. These opportunities underscore the transformative potential of digital technologies, reinforcing their role as essential drivers of business growth and market differentiation in the digital era.

### **Discussion**

The findings of this study reveal that digital technology adaptation in online business contexts faces a range of challenges that are both complex and multifaceted, encompassing technical, security, and organizational dimensions. From a technical perspective, integrating advanced technologies such as artificial intelligence (AI) and the Internet of Things (IoT) into existing legacy systems requires substantial investments, both financially and in terms of time. These technical challenges are particularly pronounced in smaller businesses, which often lack the robust infrastructure and financial resources needed for seamless adoption. This creates a widening technological gap between large corporations and small to medium-sized enterprises (SMEs), further exacerbating inequalities in the competitive landscape. Moreover, advanced technologies like AI and IoT demand infrastructure capable of handling real-time data on a massive scale, a requirement many companies struggle to meet. Ardito et al. (2024) highlight the importance of future-ready infrastructure in realizing the full potential of digital innovations. Companies that fail to address these requirements risk operational inefficiencies and the inability to respond effectively to market demands. In addition, the scalability of digital solutions remains a persistent challenge, as businesses must balance the immediate need for innovation with long-term operational stability. These technical barriers underline the critical need for strategic investments in scalable and adaptive systems supporting continuous growth and evolution in a rapidly digitalizing market. Without such investments, companies may find themselves at a significant disadvantage in an increasingly competitive global economy.

Cybersecurity challenges are another critical barrier to successful digital technology adaptation in online businesses. The constantly evolving nature of cyber threats, including ransomware, phishing attacks, and hacking, places companies at significant risk of operational disruption and data breaches. This study emphasizes that businesses unable to implement robust cybersecurity measures are vulnerable to immediate financial losses and long-term reputational harm. Zhang et al. (2022) argue



that a company's ability to protect sensitive data heavily influences customer trust, a cornerstone of business sustainability. The fallout from a security breach often extends beyond monetary damages, leading to diminished customer confidence, loss of market share, and even regulatory penalties. In some cases, Organizational shortcomings compound these risks. Many companies face internal resistance to change, which can slow down or obstruct the adoption of necessary security measures. A lack of digital literacy among employees presents a significant challenge. Without adequate training and awareness programs, employees may inadvertently expose the organization to risks, such as phishing schemes or mismanaging sensitive data. This underscores the necessity of comprehensive cybersecurity training that empowers employees to identify, mitigate, and respond to potential threats effectively. Moreover, fostering a culture of security awareness within the organization ensures that cybersecurity becomes a shared responsibility rather than a siloed function. By addressing these cybersecurity challenges proactively, businesses can build a more resilient digital infrastructure, safeguarding their operations and earning customer trust in an increasingly volatile digital environment.

The relationship between the study's findings and foundational theories in digital adaptation highlights that the success of implementing new technologies relies on the availability of advanced tools and the organization's readiness and capacity to leverage them effectively. A proactive approach is essential, focusing on equipping employees with the skills and knowledge necessary to optimize new technologies. Comprehensive training programs bridge the gap in digital literacy, ensuring that employees can confidently and competently navigate emerging tools while minimizing risks associated with human error. Furthermore, establishing an innovation-supportive culture within the organization fosters an environment where change is embraced rather than resisted. This cultural shift is crucial, as it encourages collaboration, flexibility, and adaptability—indispensable qualities in the fast-evolving technological landscape. The study also demonstrates that organizations with higher levels of flexibility are better equipped to respond to technological advancements and capitalize on emerging market opportunities. This finding aligns with broader theoretical frameworks, such as the Technology Acceptance Model (TAM), which underscores the importance of perceived usefulness and ease of use in driving the adoption of new technologies. The interplay between technical, security, and organizational challenges reinforces the need for a holistic strategy that aligns technological innovation with operational and cultural readiness. By adopting such an integrated approach, businesses can turn potential barriers into growth enablers, ensuring long-term resilience and competitiveness in the ever-changing digital economy.

The findings of this study align closely with theories emphasizing the importance of technological integration and organizational adaptation. A particularly relevant framework is the Technology Acceptance Model (TAM), introduced by Davis (1989), which posits that the acceptance of technology by individuals or organizations is significantly influenced by two key factors: perceived usefulness (PU) and perceived ease of use (PEOU). In the context of this research, perceived usefulness can be observed in how technologies like artificial intelligence (AI) and the Internet of Things (IoT) enhance operational efficiency and enable the personalization of customer services. These technologies allow organizations to optimize processes, streamline workflows, and respond to customer needs more effectively. However, the challenges identified in this study, particularly technical complexities and cybersecurity concerns, can negatively impact perceived ease of use. For instance, integrating advanced technologies often demands significant financial and temporal resources, which may create a perception of complexity and hinder adoption. Similarly, the ever-evolving nature of cyber threats introduces additional layers of difficulty, undermining the seamless integration of these technologies into business operations. In addition to TAM, organizational innovation theories are pertinent, emphasizing that the success of technological innovation relies heavily on an organization's ability to manage change and develop its human capital. Organizations that invest in employee training and foster a culture of adaptability are better positioned to overcome these barriers and capitalize on the potential of digital technologies (Al-Emran & Shaalan, 2021). These theoretical connections underscore the intertwined relationship between technological advancements and organizational readiness.

Compared with previous studies, the findings of this research demonstrate strong consistency with much of the existing literature highlighting the challenges associated with digital technology

adaptation. For instance, Ardito et al. (2024) emphasize that adopting digital technologies in Europe often faces significant barriers due to inadequate infrastructure and the high investment requirements needed for successful implementation. This study reinforces those findings by providing additional context, particularly regarding the disparity in technological capabilities between large corporations and small-to-medium enterprises (SMEs). Such a gap creates an uneven playing field, where smaller businesses struggle to keep pace with larger competitors due to resource constraints, ultimately exacerbating the technological divide within the digital economy. The results align with Zhang et al. (2022), who identified cybersecurity threats as a primary factor undermining organizational customer trust. This study reflects these findings, highlighting the critical role of robust cybersecurity measures in maintaining operational integrity and protecting sensitive customer data. However, a key distinction emerges in addressing these security challenges. While prior research has predominantly focused on the technological aspects of security, such as encryption and authentication mechanisms, this study underscores the equally vital importance of employee training and the development of an organizational culture that prioritizes security. By emphasizing the human and cultural dimensions, the findings expand upon existing research and advocate for a more holistic approach to overcoming the challenges of digital technology adaptation. This broader perspective offers valuable insights for organizations striving to balance technological advancement with operational resilience in an increasingly digitalized business landscape.

From a practical perspective, the findings of this study provide several actionable recommendations for companies seeking to address the challenges associated with digital technology adaptation. First, organizations must integrate robust security measures into their digital transformation strategies. This includes implementing multi-factor authentication, advanced data encryption techniques, and real-time threat monitoring systems. These proactive steps safeguard critical business assets and foster customer trust, protecting sensitive data and maintaining operational continuity. Second, businesses must develop comprehensive training programs to enhance employees' digital literacy and increase their awareness of cybersecurity risks. Such programs play a dual role: they mitigate the likelihood of human error, often exploited in cyberattacks, and empower employees to engage more proactively with new technologies. In addition to strengthening internal capabilities, companies should adopt innovative approaches to leverage technologies like artificial intelligence (AI) for detecting and countering cyber threats. AI-driven solutions can analyze vast amounts of data in real time, identifying patterns that may indicate potential security breaches while optimizing operational efficiency. Finally, governments and policymakers are critical in creating regulatory frameworks that encourage technological innovation without compromising security. By establishing clear guidelines and offering incentives for secure digital transformation, these frameworks can create a supportive environment that enables companies to thrive in the digital economy. By implementing these practical recommendations, businesses can effectively overcome the barriers to digital technology adaptation while capitalizing on the opportunities for growth and sustainability. This holistic approach ensures that companies remain resilient in a rapidly evolving technological landscape and are well-positioned to maintain their competitive edge in the global market.

## Conclusion

This study has explored the complex challenges of digital technology adaptation in the context of corporate online businesses, focusing on the balance between growth and security imperatives. The findings have addressed critical research questions, identifying technical, security, and organizational barriers as significant obstacles to successful digital adaptation. The research has comprehensively understood how companies navigate these challenges by integrating theoretical frameworks such as the Technology Acceptance Model (TAM) and organizational innovation theories. The study highlights that the success of digital adaptation depends not solely on the availability of advanced technologies but also on the organization's readiness to leverage them effectively through strategic planning and workforce empowerment.

The study offers substantial contributions to both theory and practice. Scientifically, it broadens the understanding of digital technology adaptation by emphasizing the interplay between

organizational readiness and technological challenges. Practically, the study provides actionable recommendations for companies to integrate security measures into their digital strategies, develop employee training programs, and leverage technologies like AI for enhanced operational efficiency and security. The originality of this research lies in its holistic perspective, which identifies barriers and provides strategic pathways to overcome them. These findings hold managerial implications, underscoring the importance of fostering a culture of innovation and adaptability while ensuring robust security practices are in place. Additionally, policymakers are encouraged to create supportive regulatory frameworks that balance innovation with security.

Despite its contributions, this study is not without limitations. The primary constraint lies in its reliance on a systematic literature review, which, while comprehensive, limits direct empirical validation. Future research should focus on empirical studies that examine the implementation of proposed strategies in diverse business contexts, including small-to-medium enterprises and industries with varying levels of technological maturity. Moreover, longitudinal studies could provide insights into the long-term impact of digital adaptation strategies on organizational growth and security. Researchers are encouraged to explore the intersection of advanced technologies like blockchain and their implications for secure digital transformation. Future studies can build upon this work by addressing these limitations to deepen the understanding of digital technology adaptation in an ever-evolving technological landscape.

## References

- Akter, S., Wamba, S. F., Gunasekaran, A., Dubey, R., & Childe, S. J. (2016). How to improve firm performance using big data analytics capability and business strategy alignment? *International Journal of Production Economics*, 182, 113-131. <https://doi.org/10.1016/j.ijpe.2016.08.018>
- Al-Emran, M., & Shaalan, K. (2021). *Recent advances in technology acceptance models and theories*. Springer. <https://doi.org/10.1007/978-3-030-64987-6>
- Al-Qaysi, N., Mohamad-Nordin, N., & Al-Emran, M. (2020). Employing the technology acceptance model in social media: A systematic review. *Education and Information Technologies*, 25(6), 4961-5002. <https://doi.org/10.1007/s10639-020-10197-1>
- Ardito, L., Filieri, R., Raguseo, E., & Vitari, C. (2024). Artificial intelligence adoption and revenue growth in European SMEs: synergies with IoT and big data analytics. *Internet Research, ahead-of-print*(ahead-of-print). <https://doi.org/10.1108/INTR-02-2024-0195>
- Berman, T., Schallmo, D., & Kraus, S. (2024). Strategies for digital entrepreneurship success: the role of digital implementation and dynamic capabilities. *European Journal of Innovation Management*, 27(9), 198-222. <https://doi.org/10.1108/EJIM-01-2024-0081>
- Botta, A., de Donato, W., Persico, V., & Pescapé, A. (2016). Integration of Cloud computing and Internet of Things: A survey. *Future Generation Computer Systems*, 56, 684-700. <https://doi.org/10.1016/j.future.2015.09.021>
- Catal, C., Ozcan, A., Donmez, E., & Kasif, A. (2023). Analysis of cyber security knowledge gaps based on cyber security body of knowledge. *Education and Information Technologies*, 28(2), 1809-1831. <https://doi.org/10.1007/s10639-022-11261-8>
- Cetindamar Kozanoglu, D., & Abedin, B. (2021). Understanding the role of employees in digital transformation: conceptualization of digital literacy of employees as a multi-dimensional organizational affordance. *Journal of Enterprise Information Management*, 34(6), 1649-1672. <https://doi.org/10.1108/JEIM-01-2020-0010>
- Chandra, B., & Rahman, Z. (2024). Artificial intelligence and value co-creation: a review, conceptual framework and directions for future research. *Journal of Service Theory and Practice*, 34(1), 7-32. <https://doi.org/10.1108/JSTP-03-2023-0097>
- Cosa, M. (2024). Business digital transformation: strategy adaptation, communication and future agenda. *Journal of Strategy and Management*, 17(2), 244-259. <https://doi.org/10.1108/JSMA->

[09-2023-0233](#)

- Creese, S., Dutton, W. H., & Esteve-González, P. (2021). The social and cultural shaping of cybersecurity capacity building: a comparative study of nations and regions. *Personal and Ubiquitous Computing*, 25(5), 941-955. <https://doi.org/10.1007/s00779-021-01569-6>
- Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 319-340. <https://doi.org/10.2307/249008>
- Florenthal, B. (2019). Young consumers' motivational drivers of brand engagement behavior on social media sites. *Journal of Research in Interactive Marketing*, 13(3), 351-391. <https://doi.org/10.1108/JRIM-05-2018-0064>
- Ishengoma, F. (2024). Revisiting the TAM: adapting the model to advanced technologies and evolving user behaviours. *The Electronic Library*, 42(6), 1055-1073. <https://doi.org/10.1108/EL-06-2024-0166>
- Kowalski, M., Bernardes, R. C., Gomes, L., & Borini, F. M. (2024). Microfoundations of dynamic capabilities for digital transformation. *European Journal of Innovation Management*, ahead-of-print(ahead-of-print). <https://doi.org/10.1108/EJIM-12-2023-1074>
- Kuzlu, M., Fair, C., & Guler, O. (2021). Role of Artificial Intelligence in the Internet of Things (IoT) cybersecurity. *Discover Internet of Things*, 1(1), 7. <https://doi.org/10.1007/s43926-020-00001-4>
- Lai, Z. J., Leong, M. K., Khoo, K. L., & Sidhu, S. K. (2025). Integrating technology acceptance model and value-based adoption model to determine consumers' perception of value and intention to adopt AR in online shopping. *Asia Pacific Journal of Marketing and Logistics*, 37(1), 1-19. <https://doi.org/10.1108/APJML-03-2024-0386>
- Prajapati, S., & Singh, A. (2022). *Cyber-Attacks on Internet of Things (IoT) Devices, Attack Vectors, and Remedies: A Position Paper BT - IoT and Cloud Computing for Societal Good* (J. K. Verma, D. Saxena, & V. González-Prida (eds.); pp. 277-295). Springer International Publishing. [https://doi.org/10.1007/978-3-030-73885-3\\_17](https://doi.org/10.1007/978-3-030-73885-3_17)
- Radanliev, P., De Roure, D., Page, K., Nurse, J. R. C., Mantilla Montalvo, R., Santos, O., Maddox, L., & Burnap, P. (2020). Cyber risk at the edge: current and future trends on cyber risk analytics and artificial intelligence in the industrial internet of things and industry 4.0 supply chains. *Cybersecurity*, 3(1), 13. <https://doi.org/10.1186/s42400-020-00052-8>
- Rane, N. L., Paramesha, M., Choudhary, S. P., & Rane, J. (2024). Artificial intelligence, machine learning, and deep learning for advanced business strategies: a review. *Partners Universal International Innovation Journal*, 2(3), 147-171. <https://doi.org/10.5281/zenodo.12208298>
- Ritz, W., Wolf, M., & McQuitty, S. (2019). Digital marketing adoption and success for small businesses. *Journal of Research in Interactive Marketing*, 13(2), 179-203. <https://doi.org/10.1108/JRIM-04-2018-0062>
- Saravanos, A., Zervoudakis, S., & Zheng, D. (2022). Extending the technology acceptance model 3 to incorporate the phenomenon of warm-glow. *Information*, 13(9), 429. <https://doi.org/10.3390/info13090429>
- Schiuma, G., Schettini, E., Santarsiero, F., & Carlucci, D. (2022). The transformative leadership compass: six competencies for digital transformation entrepreneurship. *International Journal of Entrepreneurial Behavior & Research*, 28(5), 1273-1291. <https://doi.org/10.1108/IJEBR-01-2021-0087>
- Singh, C., Dash, M. K., Sahu, R., & Kumar, A. (2024). Artificial intelligence in customer retention: a bibliometric analysis and future research framework. *Kybernetes*, 53(11), 4863-4888. <https://doi.org/10.1108/K-02-2023-0245>

- Syahnur, H. (2024). Leveraging Technology and Innovation for Effective E-Business Management. *Advances in Business & Industrial Marketing Research*, 2(2 SE-Articles), 83-95. <https://doi.org/10.60079/abim.v2i2.285>
- Wang, S., Asif, M., Shahzad, M. F., & Ashfaq, M. (2024). Data privacy and cybersecurity challenges in the digital transformation of the banking sector. *Computers & Security*, 147, 104051. <https://doi.org/https://doi.org/10.1016/j.cose.2024.104051>
- Weerasinghe, S., & Hindagolla, M. C. B. (2018). Technology acceptance model and social network sites (SNS): a selected review of literature. *Global Knowledge, Memory and Communication*, 67(3), 142-153. <https://doi.org/10.1108/GKMC-09-2017-0079>
- Willcocks, L. P. (2024). Automation, digitalization and the future of work: A critical review. *Journal of Electronic Business & Digital Economics*, 3(2), 184-199. <https://doi.org/10.1108/JEBDE-09-2023-0018>
- Wirtz, B. W. (2021). *Artificial Intelligence, Big Data, and Cloud Computing BT - Digital Business and Electronic Commerce: Strategy, Business Models and Technology* (B. W. Wirtz (ed.); pp. 217-258). Springer International Publishing. [https://doi.org/10.1007/978-3-030-63482-7\\_7](https://doi.org/10.1007/978-3-030-63482-7_7)
- Xue, M., Xiu, G., Saravanan, V., & Montenegro-Marin, C. E. (2021). Cloud computing with AI for banking and e-commerce applications. *The Electronic Library*, 39(4), 539-552. <https://doi.org/10.1108/EL-07-2020-0207>
- Yang, X. (2023). The effects of AI service quality and AI function-customer ability fit on customer's overall co-creation experience. *Industrial Management & Data Systems*, 123(6), 1717-1735. <https://doi.org/10.1108/IMDS-08-2022-0500>
- Zhang, Z., Ning, H., Shi, F., Farha, F., Xu, Y., Xu, J., Zhang, F., & Choo, K.-K. R. (2022). Artificial intelligence in cyber security: research advances, challenges, and opportunities. *Artificial Intelligence Review*, 55(2), 1029-1053. <https://doi.org/10.1007/s10462-021-09976-0>
- Zhao, X., Li, X., Li, Y., & Wang, Z. (2024). The impact of digital transformation on firm performance. *Industrial Management & Data Systems*, 124(8), 2567-2587. <https://doi.org/10.1108/IMDS-09-2023-0661>