sustainability

MDPI

Article

Organizational Cybersecurity Systems and Sustainable Business Performance of Small and Medium Enterprises (SMEs) in Saudi Arabia: The Mediating and Moderating Role of Cybersecurity Resilience and Organizational Culture

Sabah Abdullah Al-Somali [1,2,*], Raneem Rashad Saqr [1,2], Arwa Mohammed Asiri [1,2] and Najat Abdullah Al-Somali [3]

[1] Faculty of Economics and Administration, Management Information System Department, King Abdulaziz University, Jeddah 21589, Saudi Arabia; rsaqr@kau.edu.sa (R.R.S.); amaasiri@kau.edu.sa (A.M.A.)
[2] The Management of Digital Transformation and Innovation Systems in Organization Research Group, King Abdulaziz University, Jeddah 21589, Saudi Arabia
[3] Warwick Manufacturing Group (WMG), University of Warwick, Coventry CV47AL, UK; najatsomali@gmail.com
* Correspondence: saalsomali@kau.edu.sa

Abstract: Cybersecurity challenges in Saudi Arabia's service and manufacturing sectors are escalating due to increased digital adoption, highlighting the need for robust security measures and awareness in SMEs. Therefore, this research is significant due to the increasing reliance on digital technologies and the unique cybersecurity challenges faced by SMEs in these vital economic sectors. With rapid technological advancements, IT capabilities and cybersecurity have become paramount, particularly in the post-COVID-19 era. The service and manufacturing sectors in Saudi Arabia have seen significant shifts towards digital operations. This study aimed to explore the impact of organizational cybersecurity systems on organizational resilience and sustainable business performance in Saudi Arabia's service and manufacturing sectors, examining the mediating and moderating effects of organizational resilience and culture. A quantitative research method was employed, combining a thorough literature review with empirical data from a sample of 394 respondents in Saudi Arabia, split evenly between the service and manufacturing sectors. Smart PLS 3.3.3 was used to test the proposed hypotheses. The findings suggested a positive effect of the factors of organizational cybersecurity systems on organizational resilience. Organizational cybersecurity systems also significantly influenced sustainable business performance; however, organizational resilience and culture did not play mediating and moderating roles. This study is one of the first to offer a nuanced analysis of IT capabilities and cybersecurity within Saudi Arabia's service and manufacturing sectors, especially in a post-COVID-19 context. The insights gleaned contribute to the academic discourse and have pivotal managerial implications for organizations navigating the digital era in Saudi Arabia.

Keywords: SMEs; the theory of dynamic capabilities; cybersecurity resilience; organizational culture; organizational cybersecurity training and policies; regulatory effectiveness; absorptive capacity; COVID-19 pandemic vulnerabilities consequences; Saudi Arabia

Citation: Al-Somali, S.A.; Saqr, R.R.; Asiri, A.M.; Al-Somali, N.A. Organizational Cybersecurity Systems and Sustainable Business Performance of Small and Medium Enterprises (SMEs) in Saudi Arabia: The Mediating and Moderating Role of Cybersecurity Resilience and Organizational Culture. *Sustainability* **2024**, *16*, 1880. https://doi.org/10.3390/su16051880

Academic Editors: Francesco Caputo, Fenfang Lin, Jaywant Singh and Philip Alford

Received: 20 October 2023
Revised: 21 February 2024
Accepted: 23 February 2024
Published: 25 February 2024

1. Introduction

Cyberattacks are becoming increasingly complex worldwide [1]. According to Fox [1], some sectors have seen a 300% increase in cyberattacks annually. Alotaibi et al. [2] noted that SMEs in Saudi Arabia are at high risk, with incidents rising at a rate of 250% in recent years. Alotaibi et al. [2] emphasized that cybersecurity education gaps make this vulnerability even worse. They reported a 200% increase in cyberthreats targeting Saudi Arabia's critical infrastructure, emphasizing the need for resilient cybersecurity frameworks. Kong et al. [3]

also introduced the advancements, challenges, and prospects of edge computing in the rapidly evolving landscape of the Internet of Things.

Nowadays, most businesses are managed via internet, which makes businesses vulnerable to cybersecurity attacks that have an impact on a firm's core operations [4]. Internet applications are becoming increasingly important for small and medium enterprises (SMEs), in which internet technologies are found to improve corporate reputation and performance [5]. In addition, SMEs significantly contribute to job creation, economic growth, poverty alleviation, and societal well-being [6]. Moreover, it was found that economies with more significant shares of SME activity have higher growth rates compared to economies with a smaller share of SME activity [7]. Therefore, disruptive technologies such as the Internet of Things (IoT), cloud-based solutions, artificial intelligence, and blockchain have substantially increased the performance of the existing business models with innovative business strategies, reducing the cost of products or services and also considerably increasing the vulnerability of organizations to cybersecurity risks [8].

Cybersecurity encompasses a comprehensive set of strategies and measures to safeguard computer systems and networks from deliberate attacks, accidental breaches, and all forms of unauthorized access in the digital realm. This protection is achieved through methods including but not limited to system audits, data confidentiality, ensuring data integrity, user authentication, maintaining system availability, encryption techniques, and the use of digital signatures [9].

Attackers are motivated by various objectives such as monetary gain, corporate espionage, cyberwarfare, and cyberterrorism [10]. Cybercrimes and attacks cause massive damage to the reputation of enterprises, resulting in the loss of data and customers and incurring huge expenses to fix the damage caused [11]. Therefore, it was found that a comprehensive organizational security strategy combined with sophisticated behavioral awareness promotes a proactive cybersecurity culture [12].

SMEs, like large enterprises, are victimized by cybercrime, and researchers have found that SMEs are reluctant to report cyberattacks and threats for several reasons, including a lack of cybersecurity awareness, concern for reputational harm, and the belief that the incident is not serious enough [13,14]. In general, SMEs need more capabilities, experience, and resources to adopt cybersecurity measures in their companies. Moreover, it is believed that SMEs are too static and do not have dynamic capabilities. Therefore, they need more flexibility in solving and dealing with cyberattack issues [15].

Recent studies have increasingly focused on exploring cybersecurity in organizations [14,16,17]. In general, cybersecurity research has broadened its scope to cover professional groups, organizations, and users such as non-IT professionals [17], senior citizens and the elderly [18,19], large organizations [20], and healthcare domains [21]. However, SMEs are a largely under-researched segment, and more research needs to be conducted to measure the importance of cybersecurity as a method of e-protection and in achieving sustainable business performance. In addition, SME research is primarily grounded in developed Western nations [22]. Therefore, this study aims to take the first step in understanding cybersecurity phenomena in SMEs employing data from Saudi Arabia. This country was selected because it is an understudied region in the context of cybersecurity in SMEs [23]. It is noteworthy that most SMEs in Saudi Arabia are specialized in providing goods or services in their local domain. While Mian and Alatawi [24] and Ferdinand [25] examined the importance of cybersecurity in organizations, there is a great need for understanding its direct impact on sustainable business performance, particularly in Saudi Arabian SMEs. Ferdinand [25] and Tagarev et al. [26] showed that cybersecurity resilience is becoming essential to a firm's cyberstrategy. However, prior studies have not explicitly examined the mediation of organizational cybersecurity systems and sustainable business performance. O'Reilly et al. [27], Naranjo-Valencia et al. [28], and Uddin et al. [29] showed how organizational culture affects business processes and outcomes. However, its moderating role in cybersecurity resilience and sustainable business performance has yet to be

discovered. In fact, cybersecurity is a top priority for modern organizations, particularly SMEs that are extremely vulnerable to cyberattacks.

The cybersecurity landscape's complexity warrants in-depth exploration as Saudi Arabian businesses digitize and integrate advanced technologies. Although cybersecurity affects business performance, little is known about how cybersecurity resilience affects sustainable business performance. Understanding how cybersecurity resilience affects business outcomes is crucial given the diversity of Saudi Arabian SMEs' organizational cultures.

This study aims to achieve the following research objectives:

1. To examine the impact of organizational cybersecurity systems on sustainable business performance in Saudi Arabian SMEs;
2. To measure the mediating role of cybersecurity resilience and orientation between organizational cybersecurity systems and sustainable business performance in Saudi Arabian SMEs;
3. To explore the moderating role of organizational culture between cybersecurity resilience and sustainable business performance.

In fact, this study fills a regional and contextual gap in cybersecurity by showing how organizational cybersecurity systems directly affect sustainable business performance in Saudi Arabian SMEs. This research also examines how cybersecurity strategies affect sustainable business performance by examining the mediating role of cybersecurity resilience in organizations. SMEs also gain actionable cyber-resilience insights to improve business outcomes. Furthermore, this study shows how organizational culture significantly impacts cybersecurity resilience and sustainable business performance. Understanding this interaction helps companies align their cybersecurity strategies with their culture, improving performance and resilience to cyberthreats. Finally, this study advances cybersecurity research and provides Saudi Arabian SMEs with practical guidance to grow, sustain, and thrive in a digitalized business environment.

Findings from this research help organizations in general and SMEs in particular to implement overall cyber-resilience strategies, to establish a proactive risk management environment that ensures business survival, and to exploit opportunities. The following section provides an overview of the relevant literature on cybersecurity concepts, preventive measures for cybercrimes, the Saudi Arabian business environment, and theories related to organization and technological capabilities. The third section describes in detail the methodological approach employed to conduct this case study, followed by a section presenting the results of this study. Section 5 discusses the findings and provides insights and managerial implications for SMEs achieving sustainable business performance. Finally, conclusions, limitations, and suggestions for future studies are provided.

2. Literature Review

The effect of organizational culture on cybersecurity resilience and sustainable business performance is highlighted in this study. It emphasizes the importance of understanding how organizational culture moderates cybersecurity resilience, helping businesses integrate their cybersecurity strategies with their cultural frameworks to improve performance.

2.1. The Concept of Cybersecurity

Cybersecurity (CS) refers to a broad range of policies and practices that protect computer networks and systems from both intentional and unintentional threats, fears, and all types of intrusions in cyberspace through procedures such as auditing, confidentiality, integrity, authentication, availability, encryption, and digital signature [9].

Cybersecurity requires various resources and best practices to monitor and secure infrastructure and data against threats or unauthorized access [30]. According to Sutton [28], cybersecurity overlaps with several other aspects of security: information security, application security, network security, internet security, and critical information infrastructure protection. Information security is about safeguarding confidentiality, integrity, and availability in all domains of information and not just that which exists in cyberspace. On the

other hand, application security is related to the introduction of controls and measurements to a firm's applications. Moreover, network security protects an organization's internal networks, operating systems (OS), and associated management systems. Internet security is related to protecting the accessibility and reliability of a firm's internet-based services and protecting end users at work and in their home environment. Finally, critical information infrastructure protection covers the cybersecurity aspects of a country's critical information infrastructure elements [31]. Figure 1 shows these relationships.

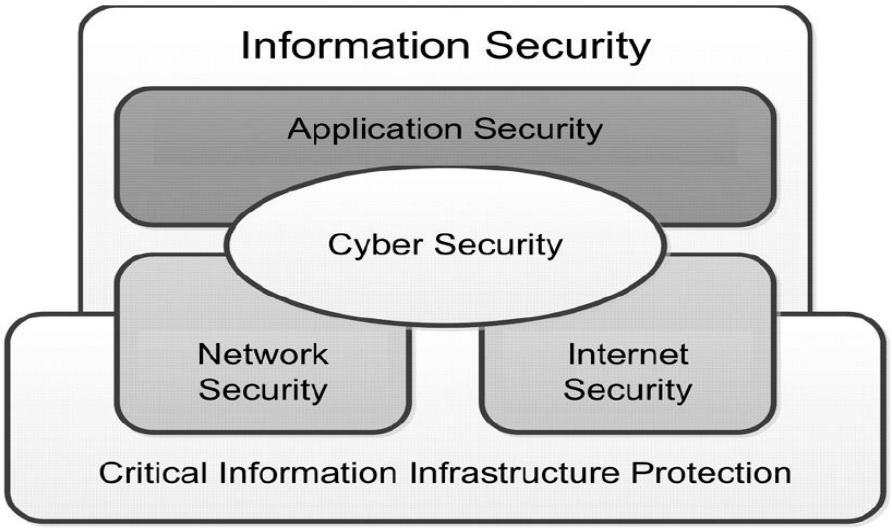

Figure 1. Relationship between security domains [31].

The cybersecurity marketplace is expanding rapidly all over the world. The COVID-19 pandemic caused a widespread disruption in organizational operations, in which organizations adopted a wide range of digital and innovative technologies such as the Internet of Things (IoT) with next-generation telecommunication networks (e.g., 5G), digital contact-tracing technology, blockchain technology, artificial intelligence (AI) with machine learning/deep learning, and big data analytics [32,33]. These technologies extensively disrupt established business processes and increase enterprises' exposure to cyber-risks and crimes [33]. Notably, cybersecurity expertise has become the most in-demand skill set, especially in cloud and data security. It is projected that by 2026, 70% of boards will include one member with cybersecurity expertise [34]. On the other hand, it is estimated that cyberattacks and crimes will cost around USD 10.5 trillion annually by 2025 [35]. The global cybersecurity market is predicted to reach USD 266.2 billion by 2027 [36].

2.2. Digital Dependency and the Era of Cybercrime

The COVID-19 pandemic suddenly and quickly forced businesses to engage in digital transformation to maintain operations and secure business continuity [32,33,37]. Digital transformation has become essential for most organizations in our world of emergent and continuous changes. However, organizations undergoing digital transformation continue to face the risk of cybercrimes and attacks on their business operations and assets [38]. Therefore, protection is needed in all communication, authentication, and authorization of things or humans [8]. The costs and impacts of such attacks and crimes on organizations and governments are substantial. The cost of cyberattacks was more than USD 45 billion worldwide in 2018 and is expected to reach more than USD 5 trillion in 2024 [38]. Cybercrimes and threats can have a variety of causes and online hazards such as malicious software (malware), ransomware, social engineering attacks, web-based attacks, phishing emails, and inadequate security monitoring [39]. SMEs are vulnerable to cyberattacks due to insufficient budgets, non-devoted IT staff, lack of IS security knowledge, and limited awareness of cyberattack effects. Moreover, according to Raghavan et al. [40], small businesses often do not take the time to develop a response plan to cyberattacks. The reasons

behind this behavior can be a lack of financial resources and an inability to recover from an incident due to a lack of appropriate training, awareness, and education.

It is believed that adopting adequate cybersecurity controls and measures can deliver genuine benefits for SMEs and help them innovate, maintain high-level confidentiality, and generate revenue [41]. Harvey [42] noted that cybersecurity controls and measures are essential in strengthening organizational cyber-resilience and decreasing cyberattacks. Indeed, organizations need to adopt and implement different preventive tools and measures to defend against cybercrimes and attacks, protect their networks from data breaches, and stay aware of security advancements to help them face any new challenges against security. Figure 2 illustrates different approaches and measures that are used to curb cybercrimes and attacks.

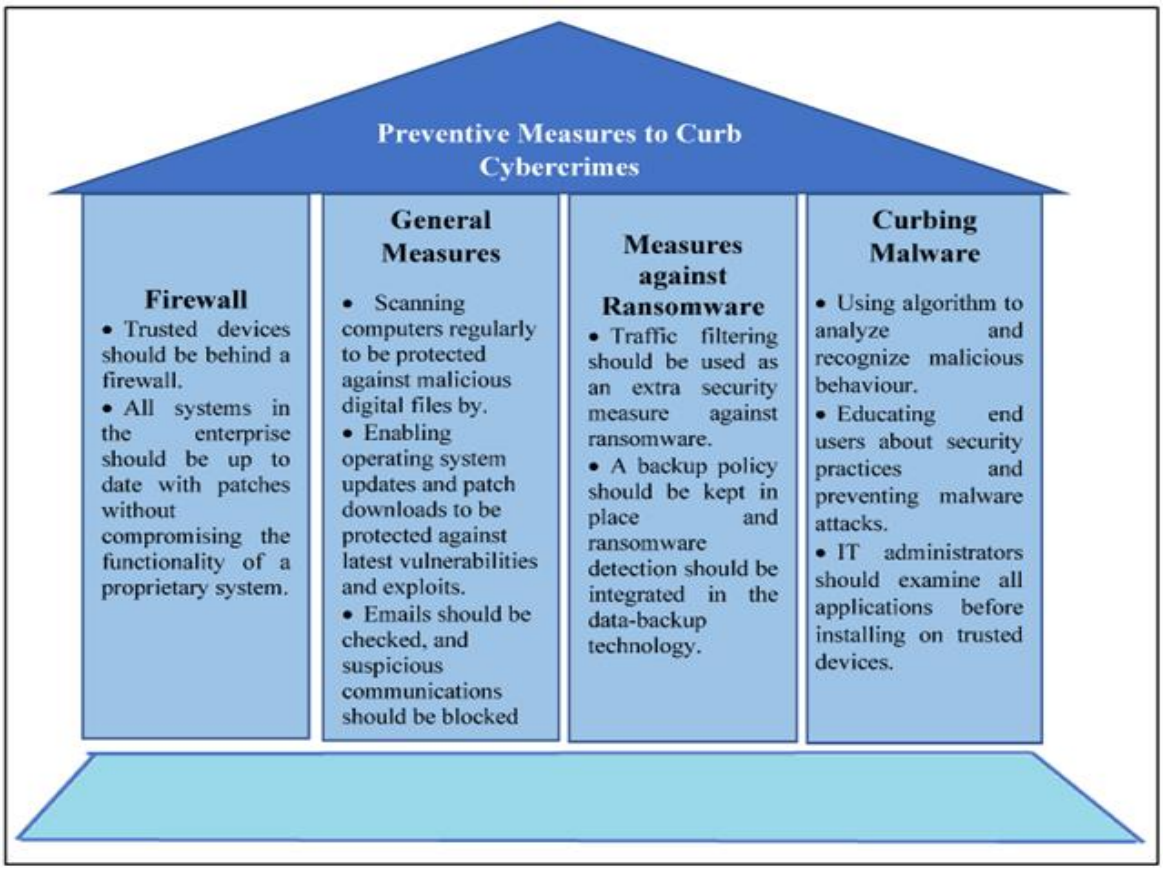

Figure 2. Preventive measures for cybercrimes [43].

2.3. Saudi Arabian Business Environment and SMEs

Saudi Arabia is a developing country, and the World Bank has classified Saudi Arabia as a high-income economy. The gross domestic product (GDP) in Saudi Arabia was worth USD 1108.15 billion in 2022 [44]. The Saudi government is fostering private sector expansion in an effort to diversify the country's economy and increase employment opportunities for Saudis. Moreover, the Saudi Vision 2030 aims to raise the contribution of SMEs to GDP from 20% to 35% [45]. It is worth mentioning that Saudi Arabia announced the establishment of the General Authority for Small and Medium Enterprises, "Monshaat", in order to achieve the following goals: (1) boost the economic impact of SMEs and (2) generate additional employment opportunities. It is worth noting that Saudi Arabia's Vision 2030 focuses on digital transformation to enhance organizational operations, which has increased the demand for cybersecurity systems to manage cybersecurity risks and challenges.

2.4. Theoretical Background

This research used dynamic capabilities as its primary theoretical approach. Dynamic capability is the ability of an organization to consciously integrate, build, and reconfigure internal and external competences to respond quickly to changing environments [46].

2.4.1. Dynamic Capability Theory

The dynamic capability theory emphasizes the importance of organizations continuously adapting to the external environment in which they operate. Given the prevalence of digital technology today, one of the most essential ways organizations can achieve this adaptation is by improving their cybersecurity. According to Teece [47] and Danneels [48], the commitment of a company to the training of its workforce and the establishment of stringent cybersecurity policies equips it to deal with cyberthreats, which in turn strengthens the company's resilience. This viewpoint becomes even more apparent when one considers the regulatory measures. According to Teece [49], a significant factor that contributes to the formation of a company's dynamic capabilities is the broader environment, which includes governmental regulations. Consequently, in areas that have stringent cybersecurity mandates, SMEs are likely to demonstrate improved resilience strategies and orientations. In the context of absorptive capacity, the ability of a company to assimilate, comprehend, and put to use information obtained from outside sources is of the utmost importance. Taking into consideration the findings of Wang and Kim [50], businesses that are able to successfully harness external data such as those obtained from social media platforms demonstrate superior capabilities in adopting cybersecurity best practices. This level of expertise has the potential to lead to improved cybersecurity posture. Furthermore, as demonstrated by the strategic shifts at Smith Corona mentioned by Danneels [48], being aware of one's vulnerabilities and the complexities of those vulnerabilities can be a determining factor in the efficacy of the cybersecurity resilience strategies that are employed by SMEs.

When looking at spheres of activity other than cybersecurity, the intricate relationship that exists between dynamic capabilities and sustainable business performance becomes immediately apparent. For example, Chowdhury and Quaddus [51] drew parallels between supply chain resilience and dynamic capability theory in their research. In a similar vein, a strong organizational cybersecurity system that operates with a pivotal dynamic capability is required in order to maintain consistent business performance in a world that is becoming increasingly dependent on digital tools and platforms. Taking into consideration the research from Dangelico et al. [52], one can deduce that resilience strategies in cybersecurity can function as essential drivers or even mediators in the process of achieving and ensuring sustainable business outcomes.

Therefore, the foundations of organizational culture should be addressed when discussing the impact of cybersecurity resilience on business performance. Numerous studies, such as those conducted by Linnenluecke and Griffiths [53] and O'Reilly et al. [27], highlight the significant impact that organizational culture has on a variety of operational results. When it comes to the field of cybersecurity, having a cultural fabric that is permeated with adaptability and resilience has the potential to strengthen cybersecurity strategies, which in turn can boost overall performance. Appendix A summarizes previous theoretical frameworks and models in the context of SMEs.

2.4.2. Organizational Cybersecurity Training and Policies and Cybersecurity Resilience Strategy and Orientation

The study of Wided [54], who highlighted the mediating and moderating roles of big data analytics capabilities, which are seen as an advanced form of cybersecurity management, emphasized the critical importance of IT capabilities and strategic flexibility in bolstering organizational resilience post COVID-19. The importance of factors that increase the intention to adopt cybersecurity was further highlighted by Mian and Alatawi's [24] research on the Saudi banking industry, suggesting the potential efficacy of structured training and policies in enhancing such intentions. A systematic review by Nifakos et al. [55]

stressed the importance of human factors in cybersecurity, especially in healthcare organizations, and the need for comprehensive training and strong policy frameworks. This supports the hypothesis that organizational cybersecurity training and policies shape Saudi Arabian SMEs' cybersecurity resilience strategy and orientation. Rajamäki et al. [56] and Tagarev and Polimirova [26] showed that well-structured training, effective information security policies, and organizational cybersecurity postures are strongly linked. Rajamäki et al. [56] emphasized the importance of cybersecurity education in hospitals, which can be applied to Saudi Arabian SME contexts. Together, these studies offer strong justifications for the beneficial effects of organizational cybersecurity policies and training on resilience strategies, especially in contexts such as that of Saudi Arabian SMEs. Finally, the present study offers the following research hypothesis:

H1. *Organizational cybersecurity training and policies significantly influence cybersecurity resilience strategy and orientation in Saudi Arabian SMEs.*

2.4.3. Regulatory Effectiveness and Government Policies and Cybersecurity Resilience Strategy and Orientation

Recent literature has clarified the complex interplay between regulatory effectiveness, governmental policies, and cybersecurity resilience in organizations, particularly SMEs. Wided [54] suggested that data protection regulations and strategic IT use affect SMEs' resilience in the post-COVID-19 era. This supports the hypothesis that regulatory effectiveness and government policies shape Saudi Arabian SMEs' cybersecurity resilience strategy and orientation. Mian and Alatawi [24] emphasized the need for the Saudi banking industry to adopt cybersecurity measures, implying that effective regulation drives this. Ferdinand's [25] knowledge-based view of cybersecurity management and Hossain et al.'s [57] sustainable performance research provided insights into organizational resilience, emphasizing the importance of regulatory frameworks in improving cybersecurity resilience strategies in Saudi Arabian SMEs. The nuances of organizational information security policies and cybersecurity education were further explored by Tagarev and Polimirova [26] and Rajamäki et al. [56], emphasizing the value of structured guidance, which frequently results from effective regulatory frameworks. In the meantime, research on the cybersecurity environment in the European Union, such as that by Wessel [58] and Fuster and Jasmontaite [59], has offered comparative insights and emphasized the significance of regulation in fostering cybersecurity resilience. Regulational efficiency and governmental policies play a crucial role in forming the cybersecurity resilience strategy of SMEs in Saudi Arabia, with its distinct socioeconomic dynamics. Finally, the present study offers the following research hypothesis:

H2. *Regulatory effectiveness and government policies significantly influence cybersecurity resilience strategy and orientation in Saudi Arabian SMEs.*

2.4.4. Absorptive Capacity and Cybersecurity Resilience Strategy and Orientation

The literature lends credence to the idea that, particularly in the context of SMEs, absorptive capacity significantly affects cybersecurity resilience strategy and orientation. Cohen and Levinthal [60] proposed the concept of "absorptive capacity", which scholars developed to describe a company's capacity to recognize, assimilate, and use new external knowledge for competitive advantage. Wided [54] emphasized the role of big data's analytic capabilities, which inherently depend on firms' absorptive capacity, and stressed the importance of IT capabilities and strategic flexibility in bolstering organizational resilience in the post-COVID-19 era. Chowdhury and Quaddus [51] argued that resilience, including that in cybersecurity, can be understood through dynamic capability theory, which emphasizes absorptive capacity. Zahra and George [61] proposed a framework for understanding absorptive capacity and highlighted its visibility as a crucial factor in enhancing firm performance and innovation. Their research adds significant value to the understanding and

application of absorptive capacity in the field of innovation management. Teece's [47,49] insights on how dynamic capabilities like absorptive capacity affect firm strategies and performance support this hypothesis. Mian and Alatawi [24] also highlighted the importance of understanding factors that increase cybersecurity adoption intentions in Saudi Arabian SMEs, arguing that these businesses must be able to absorb and adapt to evolving cyberthreats, supporting the hypothesis that it significantly impacts cybersecurity resilience. Given these arguments and supporting evidence, it is clear that absorptive capacity has a significant impact on cybersecurity resilience strategy and orientation in Saudi Arabian SMEs. Therefore, the present study offers the following research hypothesis:

H3. *Absorptive capacity significantly influences cybersecurity resilience strategy and orientation in Saudi Arabian SMEs.*

2.4.5. Complexities of Vulnerabilities and Cybersecurity Resilience Strategy and Orientation

Today's business environment is becoming more interconnected and digital, ushering in a time when cybersecurity is crucial for all businesses, regardless of size. The studies by AlHamdani [62] and Alahmari and Duncan [63], with the former concentrating on architectural considerations and the latter on the complexities of risk management, highlighted the urgent need for resilient cybersecurity architectures and risk management, especially within the SME sector. A further step was taken by Ferdinand [25], who outlined the key components of building organizational cyber-resilience, including risk awareness, incident response planning, and continuous monitoring and evaluation. Additionally, Cheng et al. [64] discussed organizational dynamics' crucial role in violating IS security policies, arguing that complexity, including organizational culture and human factors, may expose vulnerabilities. As Tam et al. [65] and Rahman and Lackey [66] both emphasized the significance of e-commerce systems security and the broad spectrum of cybersecurity implications, the worries of Saudi Arabian SMEs may align with the global insights provided by these authors. Together, these studies provide strong evidence for the claim that the complexity of vulnerabilities significantly affects Saudi Arabian SMEs' cybersecurity resilience strategies and orientation, whether those vulnerabilities are technical, organizational, or human. Considering the above, the present study draws upon the following research hypothesis:

H4. *COVID-19 pandemic vulnerability consequences significantly influence cybersecurity resilience strategy and orientation in Saudi Arabian SMEs.*

2.4.6. Organizational Cybersecurity System and Cybersecurity Resilience Strategy and Orientation

The literature provides evidence supporting hypothesis H5, which states that organizational cybersecurity systems significantly affect long-term business performance in Saudi Arabian SMEs. In an increasingly cyber-centric business environment, AlHamdani's [62] exposition on resilient cybersecurity architectures emphasized the significance of digital solid defenses and hinted at their function in preserving and boosting business continuity and competitiveness. In their systematic review of cybersecurity risk management's crucial role in SMEs, Alahmari and Duncan [63] explained how it affects overall business performance. The work of Haseeb et al. [67], which emphasized the role of technological challenges in achieving sustainable business performance, further strengthens this argument. They suggested that addressing cybersecurity flaws is viewed as a solution to these technological problems. Additionally, Rahman and Lackey's [66] attention to the security of e-commerce systems for small businesses speaks to the necessity of protecting online business operations, a mainstay of contemporary commerce, to guarantee consistent and sustained business performance. Finally, Watad, Washah, and Perez's [68] insights into managers' perceptions of IT security threats and challenges for small firms highlighted

the effects of cybersecurity on business operations, reputation, customer trust, and long-term sustainability. These combined insights provide a strong case for how cybersecurity systems are essential to the long-term success of SMEs, including those in Saudi Arabia. Therefore, the present study designed the following research hypothesis:

H5. *Organizational cybersecurity systems significantly influence sustainable business performance in Saudi Arabian SMEs.*

2.4.7. Cybersecurity Resilience Strategy and Orientation and Sustainable Business Performance

Research has shown a direct link between cybersecurity measures and sustainable business performance, particularly for SMEs, which supports H6. According to AlHamdani [62], resilient cybersecurity architecture is essential for preventing digital threats and business continuity. Alahmari and Duncan [63] emphasized the growing risks for SMEs and the need for effective cybersecurity strategies to protect assets and ensure operational continuity. This directly supports the hypothesis that a well-defined cybersecurity resilience strategy and orientation can significantly impact Saudi Arabian SMEs' sustainable business performance. Tagarev and Polimirova [26] discussed the importance of strategic planning and policy development in addressing cyberthreats and promoting resilience. Ambrosini and Bowman's [46] discussion on dynamic capabilities, including cybersecurity resilience, in strategic management and sustainable performance supports this hypothesis, indicating that Saudi Arabian SMEs need a strong cybersecurity resilience orientation to succeed in the long term. Rahman and Lackey [66] supported the need for more robust cyber-resilience strategies by highlighting the weakness of e-commerce systems in SMEs. Finally, Watad, Washah, and Perez [68] offered a managerial perspective, highlighting both how decision making is directly impacted by perceptions of IT security threats as well as the importance of a proactive cybersecurity resilience orientation for long-term business success. This idea supports the hypothesis by showing how cybersecurity resilience improves business performance. Therefore, the present study proposes the following research hypothesis:

H6. *Cybersecurity resilience strategy and orientation significantly influence sustainable business performance in Saudi Arabian SMEs.*

2.4.8. The Mediations between Organizational Cybersecurity Systems and Sustainable Business Performance

Numerous studies have shown the significance of organizational cybersecurity policies and training in determining business performance. Wided [54] highlighted the significance of organizational resilience while emphasizing the role of IT capabilities and strategic flexibility in SMEs post COVID-19. Ferdinand [25] emphasized the importance of enhancing organizational cyber-resilience through a strategic, knowledge-based approach to cybersecurity management, which further underlines this concept. Additionally, Huang and Pearlson [69] argued that developing an organizational cybersecurity culture is necessary because technology by itself cannot address all vulnerabilities. This suggests that efficient cybersecurity policies and training could result in a solid resilience strategy, improving long-term business performance, particularly in environments such as Saudi Arabian SMEs.

Governmental policies and regulatory frameworks are crucial in determining how resilient an organization is online. In his overview of cybersecurity resilience in the European Union for 2019, Wessel [58] emphasized the importance of regulation in promoting resilience. In their article from 2019, Clark-Ginsberg and Slayton discussed how controlling risks in intricate systems such as critical infrastructure results in tighter cybersecurity regulations. AlDaajeh et al. [70] also showed how national cybersecurity strategies positively enhance cybersecurity education. Stronger cybersecurity resilience strategies could thus be

made possible in the Saudi Arabian context by efficient regulation and government policies, increasing the likelihood of achieving sustainable business performance in SMEs.

The dynamic capabilities theory's concept of absorptive capacity is essential for organizations to absorb and apply external knowledge successfully. Chowdhury and Quaddus [51] conceptualized and created a scale for supply chain resilience using dynamic capability theory. Teece presented similar work [47,49] that emphasized the value of dynamic capabilities, including absorptive capacity, in boosting entrepreneurial management and organizational performance. Further highlighting the importance of absorptive capacity in supply chain resilience, Gölgeci and Kuivalainen [71] hypothesized that it may enhance overall business performance. As a result, a firm's capacity for absorption significantly affects its cybersecurity resilience strategy, mediating its path to long-term success.

A robust resilience strategy is required to ensure sustainability due to the complexity of organizational vulnerabilities. Turner [72] discussed the similarities between vulnerability and resilience, highlighting how they are intertwined in sustainability science. In his further exploration of the terms adversity, risk, and vulnerability in the context of systemic protection, Daniel [73] emphasized the importance of resilience in dealing with these difficulties. A strong resilience strategy is necessary for cybersecurity to comprehend and navigate these complexities [26]. Similar to other organizational settings, Saudi Arabian SMEs can benefit greatly from addressing the COVID-19 pandemic vulnerability consequences with a cybersecurity resilience orientation. Based on the evidence from the literature, the present study proposes the following research hypotheses:

H7. *Cybersecurity resilience strategy and orientation significantly mediate the relationship between organizational cybersecurity training and policies and sustainable business performance in Saudi Arabian SMEs.*

H8. *Cybersecurity resilience strategy and orientation significantly mediate the relationship between regulatory effectiveness and government policies and sustainable business performance in Saudi Arabian SMEs.*

H9. *Cybersecurity resilience strategy and orientation significantly mediate the relationship between absorptive capacity and sustainable business performance in Saudi Arabian SMEs.*

H10. *Cybersecurity resilience strategy and orientation significantly mediate the relationship between COVID-19 pandemic vulnerability consequences and sustainable business performance in Saudi Arabian SMEs.*

2.4.9. The Moderation of Organizational Culture

The literature supports cybersecurity resilience strategy and orientation in modern business environments. Wided [54] emphasized the importance of IT capabilities and strategic flexibility in enhancing organizational resilience in SMEs in the post-COVID-19 era, emphasizing the importance of adapting to new technological trends and challenges. In support of this claim, Ferdinand [25] and Tagarev et al. [26] emphasized the importance of developing organizational cyber-resilience, presenting it as a strategic, knowledge-based perspective that ensures continuous and sustainable operations. These studies emphasized cybersecurity's protective and strategic role, particularly in settings characterized by high digitalization and technological dependence, such as SMEs. Furthermore, organizational culture has been identified as a determinant of various business performance metrics. For example, Linnenluecke and Griffiths [53] linked corporate sustainability to organizational culture, implying that cultural factors play an important role in firms' long-term operations. Studies such as those of Naranjo-Valencia et al. [28] and O'Reilly et al. [27], which empirically demonstrated the links between organizational culture and innovation, operational performance, and CEO's personality, support this viewpoint.

Furthermore, Teece's [47,49] dynamic capabilities framework provides a compelling perspective on how firms can integrate and reconfigure internal and external competencies to address rapidly changing environments. Danneels [48] and Wang and Kim [50] presented examples of how dynamic capabilities, such as adapting to new technological paradigms, can lead to long-term competitive advantage and improved performance.

In the context of Saudi Arabia, the country's economic diversification efforts have fueled growth in the SME sector, making it a focal point for understanding the intersection of cybersecurity, organizational culture, and business performance. Mian and Alatawi's [24] research on increasing intentions to adopt cybersecurity in the Saudi banking sector emphasized the importance of this domain in the region. Synthesizing these findings reveals that organizational culture plays an important moderating role. At the same time, cybersecurity resilience strategies are critical for long-term business performance, particularly in technologically driven contexts such as Saudi Arabian SMEs. The combined cultural attitude towards innovation, adaptability, and cybersecurity significantly affects the effectiveness of cybersecurity strategies in driving long-term business outcomes. As a result, the academic literature strongly supports the hypothesis that organizational culture significantly moderates the relationship between cybersecurity resilience strategy and long-term business performance in Saudi Arabian SMEs.

H11. *Organizational culture significantly moderates the relationship between cybersecurity resilience strategy and orientation and sustainable business performance in Saudi Arabian SMEs.*

Finally, we present the study's developed theoretical framework (see Figure 3).

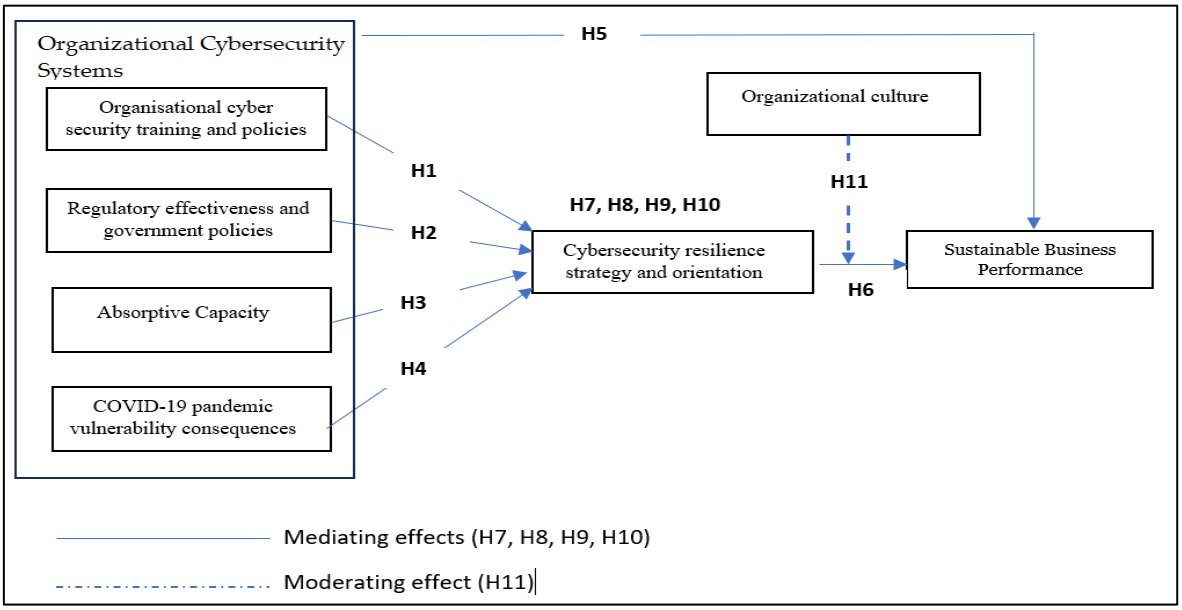

Figure 3. The research's conceptual framework.

3. Research Methods and Materials

3.1. Sampling and Data Collection Procedure

Based on the research goal, the present study utilized quantitative research and used survey questionnaires to understand cybersecurity phenomena in Saudi Arabian SMEs. In general, the survey method is used in scientific research to collect data from individuals to capture their beliefs, actions, and experiences.

Small- and medium-sized enterprises (SMEs) in Saudi Arabia were the focus of this research project's population analysis. The researchers paid particular attention to SMEs operating in the service industry and manufacturing companies. The decision to focus on these industries was motivated by the sizeable contributions they make to the country's economy

as well as the growing need to measure the link between the cybersecurity systems of these companies and their ability to maintain sustainable business performance. The method of sampling that was utilized was known as purposive sampling. The study targeted those SMEs that hold online systems for deliveries, supplies, and products sharing. In this way, stakeholders (suppliers, employees, shareholders, and CEOs) were targeted to ensure the correct responses about how they deal with cybersecurity issues. One stakeholder was selected from each SMEs to guarantee the generalizability of the research findings. By taking advantage of this strategy, the researchers selected those small- and medium-sized enterprises (SMEs) that most accurately reflected the conditions and challenges currently prevalent in the manufacturing and service industries. This sampling strategy was deemed the most appropriate given the specific objectives of the research. This ensured that the data collected were relevant and generalized to a broader context within the Saudi Arabian SME landscape.

The process of collecting data took place over several months in 2023. A questionnaire in the form of an online survey was designed to accomplish the research goals. This approach was selected because it could effectively communicate with many respondents in various geographic locations across Saudi Arabia. The link to the survey was sent out via email to some different SMEs. Reminders were sent out irregularly to guarantee a higher overall response rate. The initial data collection phase started on 15 March 2023 and continued until 15 April 2023 before ending. A second round was started on 10 June 2023 and concluded on 10 July 2023. This method was chosen because the data that were obtained were rich, and there was a need for more representation. In the end, the study obtained 394 survey questionnaires that were completed and fully filled out.

Immediately after they were received, all the data were meticulously cleaned and then stored in encrypted files to protect the respondents' privacy and confidentiality. The raw data were only available to the members of the research team. Pseudonyms were used in place of real names and other identifying information to prevent any possibility of individual businesses being directly linked to the responses they provided. During all stages of the research process, the participants' trust was protected by the stringent measures put into place to uphold the study's ethical considerations and ensure that their trust was not betrayed.

The demographic information from Table 1 indicates a predominantly male sample, with males comprising 67% and females 33%. A majority of the participants are directors (83.2%), followed by managers (9.9%) and owners (6.9%). Regarding the sectors, 60.4% are from the manufacturing sector, and the rest, 39.6%, are from wholesale and retail. A vast majority of participants have a bachelor's degree (83%), with a smaller percentage holding a higher degree (11.7%) or an associate's degree (5.3%). Regarding enterprise ownership, sole proprietorships are the most common at 41.1%, closely followed by partnerships at 38.6%, with private companies constituting 20.3%.

3.2. Survey Instruments

In the current study, the measurement scales for each construct were adapted from various previous research to maintain robustness and suit this study's context. The construct of "organizational culture" was measured using three items primarily sourced from the work of Dobni [74], Zhang et al. [75], and Azanza et al. [76]. Organizational cybersecurity training and policies were gauged with six items drawn from Zwilling et al. [16], Wang et al. [50], and Shillair et al. [77]. For assessing "regulatory effectiveness and government policies", three items were employed based on the studies by Srinivas et al. [78], and Wang et al. [50]. "Absorptive capacity" was examined with four items adapted from Levinson [79] and Andrawina and Govindaraju [80]. The construct of "sustainable business performance" involved five items inspired by Haseeb et al. [67] and Zulkiffli et al. [81]. The "cybersecurity resilience strategy and orientation" was captured with four items referencing Harrop and Matteson [82]. Lastly, the impact of "COVID-19 pandemic vulnerabilities" was evaluated using five items, with some being original to the current study and others adapted from Ku-

mar et al. [83] and Pranggono and Arabo [84]. The details of the measurement instruments with their sources are provided in Appendix B. All instruments were measured on 5-point Likert scales ranging from 1 = strongly disagree to 5 = strongly agree. In this study, the independent variables are "organizational cybersecurity training and policies", "regulatory effectiveness and government policies", "absorptive capacity", and "COVID-19 pandemic vulnerabilities consequences". The dependent variable is "sustainable business performance". The mediator in the model is "cybersecurity resilience strategy and orientation." The moderator in the model is "organizational culture".

Table 1. Demographic information.

Demographics	Frequency	Frequency	% Ages
Gender	Male	264	67.0
	Female	130	33.0
	Total	394	100%
Position	Owner	27	6.9
	Manager	39	9.9
	Director	328	83.2
	Total	394	100%
Sector	Manufacturing	238	60.4
	Wholesale and retail	156	39.6
	Total	394	100%
Education	Associate's degree	21	5.3
	Bachelor's degree	327	83.0
	Higher degree	46	11.7
	Total	394	100%
Enterprise Ownership	Sole proprietor	162	41.1
	Partnership	152	38.6
	Private company	80	20.3
	Total	394	100%

3.3. Data Analysis

In the present investigation, the data analysis procedure was carried out using the structural equation modeling (SEM) method, specifically using the application of Smart PLS 3.3.3. According to Hair et al. [85], one reason Smart PLS is gaining popularity is its capability to manage complex models, mainly when working with smaller sample sizes and when the data distribution is abnormal. At first, the measurement model was analyzed to determine whether the constructs' validity and reliability had been established. Validity was determined using convergent and discriminant validity, and the reliability of the constructs was determined using Cronbach's alpha and composite reliability (CR) metrics [86]. Validity was determined using convergent and discriminant validity. After that, the structural model was analyzed to establish the hypothesized relationships between the latent variables as in the research hypotheses. To determine whether the path coefficients were statistically significant, the bootstrapping method, built into Smart PLS, was applied [87].

4. Results

4.1. Assessing Validity and Reliability

The study used the algorithm technique with 5000 sub-samples in Smart PLS. Based on the guidelines set forth by Hair et al. [85] and Henseler et al. [86], convergent validity is typically assessed using factor loadings and the average variance extracted (AVE). Factor loadings should be 0.6 or higher [88], indicating that the respective items share significant variance with their assigned latent construct. From Table 2, all the items have factor loadings well above this threshold, signifying satisfactory convergent validity for each construct. The AVE, which measures the variance captured by a construct concerning the variance attributable to measurement error, should be greater than 0.5 [85,88]. All

constructs shown in Table 2 had AVE values greater than this benchmark, reinforcing the adequacy of convergent validity.

Table 2. Convergent validity and reliability.

Scales	Items	Factor Loadings	Cronbach's Alpha	Composite Reliability	AVE
Absorptive Capacity (ABS)	ABS1	0.887	0.861	0.889	0.906
	ABS2	0.884			
	ABS3	0.881			
	ABS4	0.698			
COVID-19 Pandemic Vulnerabilities Consequences (VUL)	VUL1	0.895	0.906	0.908	0.935
	VUL2	0.925			
	VUL3	0.897			
	VUL4	0.816			
Cybersecurity Resilience Strategy and Orientation (RES)	RES1	0.819	0.904	0.907	0.933
	RES2	0.917			
	RES3	0.893			
	RES4	0.895			
Organizational Culture (ORG)	ORG1	0.863	0.913	0.914	0.933
	ORG2	0.896			
	ORG3	0.846			
Organizational Cybersecurity Training and Policies (PU)	PU1	0.799	0.849	0.850	0.852
	PU2	0.849			
	PU3	0.851			
	PU4	0.844			
	PU5	0.841			
	PU6	0.829			
Regulatory Effectiveness and Government Policies (REG)	REG1	0.835	0.835	0.842	0.901
	REG2	0.842			
	REG3	0.825			
Sustainable Business Performance (SBP)	SBP1	0.862	0.912	0.914	0.934
	SBP2	0.814			
	SBP3	0.897			
	SBP4	0.892			
	SBP5	0.834			

The reliability of the constructs was evaluated using Cronbach's alpha and composite reliability (CR) [85,87,88]. According to previous studies, both Cronbach's alpha and CR should exceed the value of 0.7 for a construct to be considered reliable. All constructs shown in Table 2 had both Cronbach's alpha and CR values comfortably above this threshold. It is worth noting that CR values often exceed Cronbach's alpha, which is expected, as CR is a more robust and lenient measure of reliability. Therefore, all scales in Table 2 demonstrated strong convergent validity and reliability, indicating that the measures are both valid and consistent in capturing their respective constructs.

According to Hair et al. [85] and Henseler et al. [86], an item's cross-loadings should be higher on its construct than on any other construct to establish discriminant validity. Table 3 shows that most items had higher construct cross-loadings, indicating good discriminant validity. However, some items appeared to have close cross-loadings with other constructs, raising discriminant validity concerns that may require further investigation. Awang et al. [88] recommended model evaluation to address potential issues for robust and reliable model results.

Table 3. Discriminant validity (cross-loadings).

	Absorptive Capacity	COVID-19 Pandemic Vulnerabilities Consequences	Cybersecurity Resilience Strategy and Orientation	Organizational Cybersecurity Training and Policies	Organizational Culture	Regulatory Effectiveness and Government Policies	Sustainable Business Performance
ABS1	0.887	0.695	0.606	0.570	0.483	0.609	0.586
ABS2	0.884	0.661	0.682	0.656	0.560	0.640	0.680
ABS3	0.881	0.632	0.586	0.583	0.492	0.635	0.589
ABS4	0.698	0.454	0.374	0.364	0.316	0.406	0.348
ORG1	0.523	0.470	0.530	0.578	0.863	0.538	0.599
ORG2	0.476	0.454	0.551	0.600	0.896	0.556	0.653
ORG3	0.469	0.367	0.435	0.656	0.846	0.504	0.635
PU1	0.561	0.488	0.543	0.799	0.663	0.584	0.660
PU2	0.533	0.466	0.491	0.849	0.546	0.528	0.641
PU3	0.572	0.547	0.498	0.851	0.573	0.561	0.611
PU4	0.536	0.509	0.472	0.844	0.556	0.512	0.614
PU5	0.559	0.441	0.524	0.841	0.590	0.569	0.695
PU6	0.548	0.484	0.530	0.829	0.597	0.555	0.750
REG1	0.628	0.533	0.560	0.635	0.575	0.882	0.609
REG2	0.591	0.546	0.590	0.603	0.593	0.891	0.637
REG3	0.583	0.461	0.509	0.469	0.413	0.825	0.498
RES1	0.509	0.540	0.819	0.531	0.486	0.477	0.639
RES2	0.645	0.648	0.917	0.583	0.551	0.609	0.659
RES3	0.654	0.622	0.893	0.506	0.466	0.577	0.567
RES4	0.600	0.595	0.895	0.531	0.543	0.587	0.642
SBP1	0.532	0.475	0.649	0.687	0.559	0.556	0.862
SBP2	0.493	0.492	0.629	0.624	0.563	0.568	0.814
SBP3	0.597	0.550	0.594	0.706	0.695	0.600	0.897
SBP4	0.629	0.537	0.613	0.684	0.650	0.587	0.892
SBP5	0.631	0.579	0.580	0.709	0.643	0.591	0.834
VUL1	0.673	0.895	0.600	0.495	0.433	0.531	0.547
VUL2	0.702	0.925	0.632	0.545	0.483	0.570	0.568
VUL3	0.615	0.897	0.573	0.468	0.388	0.467	0.468
VUL4	0.605	0.816	0.606	0.556	0.440	0.526	0.578

For discriminant validity using the Fornell–Larcker criterion, the square root of any given construct is AVE (diagonal values) and should be higher than its highest correlation with any other construct (off-diagonal values). According to Hair et al. [85] and Henseler et al. [86], Table 4 suggests that most constructs in the model met this criterion, indicating satisfactory discriminant validity. However, some values were close, implying the need for careful interpretation and potential model refinement, as Awang et al. [88] recommended. Finally, the study confirmed the discriminant validity.

Table 4. Fornell–Larcker criteria.

Fornell–Larcker Criteria	1	2	3	4	5	6	7
Absorptive Capacity	0.841						
COVID-19 Pandemic Vulnerabilities Consequences	0.736	0.884					
Cybersecurity Resilience Strategy and Orientation	0.684	0.683	0.882				
Organizational Cybersecurity Training and Policies	0.661	0.585	0.611	0.836			
Organizational Culture	0.562	0.495	0.581	0.704	0.869		
Regulatory Effectiveness and Government Policies	0.692	0.594	0.640	0.661	0.613	0.867	
Sustainable Business Performance	0.672	0.613	0.711	0.793	0.725	0.675	0.861

4.2. Assessing Path Model

The study used SEM analysis to test the research hypotheses (Table 5). The study used a 5% significance level with a 95% confidence interval. Therefore, the value of p should be lower than 0.05, and the t-value should be higher than +1.96. The direct effects elucidate the straightforward impact of one variable on another, uninfluenced by other intervening variables (Figure 4). H1 demonstrates a significant positive relationship between organizational cybersecurity training and policies and cybersecurity resilience strategy and orientation, with values indicative of this effect (β = 0.151, t = 2.638, p = 0.008). Similarly, H2 reveals that regulatory effectiveness and government policies significantly influence cybersecurity resilience strategy and orientation (β = 0.208, t = 3.537, p = 0.000). H3 and H4 also present significant direct effects, where absorptive capacity affects cybersecurity resilience strategy and orientation (β = 0.204, t = 3.215, p = 0.001), and the implications of the COVID-19 pandemic vulnerability consequences on the same outcome were notable (β = 0.321, t = 5.407, p = 0.000). In terms of organizational performance, H5 establishes a potent direct influence of the organizational cybersecurity system on sustainable business performance (β = 0.784, t = 17.647, p = 0.000), and the effect of organizational culture on sustainable business performance was also significant (β = 0.116, t = 3.432, p = 0.001).

Table 5. Direct, mediating, and moderating effects.

Effects	Direct Effects	Mediating Effects	Moderating Effect		
	Beta Value	Beta Value	Beta Value	t-Value	*p*-Value
H1. Organizational Cybersecurity Training and Policies → Cybersecurity Resilience Strategy and Orientation	0.151			2.638	0.008
H2. Regulatory Effectiveness and Government Policies → Cybersecurity Resilience Strategy and Orientation	0.208			3.537	0.000
H3. Absorptive Capacity → Cybersecurity Resilience Strategy and Orientation	0.204			3.215	0.001
H4. COVID-19 Pandemic Vulnerabilities Consequences → Cybersecurity Resilience Strategy and Orientation	0.321			5.407	0.000
H5. Organizational Cybersecurity System → Sustainable Business Performance	0.784			17.647	0.000
H6. Cybersecurity Resilience Strategy and Orientation → Sustainable Business Performance	0.023			0.627	0.531
H7. Organizational Cybersecurity Training and Policies → Cybersecurity Resilience Strategy and Orientation → Sustainable Business Performance		0.004		0.589	0.556
H8. Regulatory Effectiveness and Government Policies → Cybersecurity Resilience Strategy and Orientation → Sustainable Business Performance		0.005		0.575	0.566
H9. Absorptive Capacity → Cybersecurity Resilience Strategy and Orientation→ Sustainable Business Performance		0.005		0.605	0.546
H10. COVID-19 Pandemic Vulnerabilities Consequences → Cybersecurity Resilience Strategy and Orientation → Sustainable Business Performance		0.008		0.616	0.538
H11. Cybersecurity Resilience Strategy and Orientation × Culture-Sustainable → Sustainable Business Performance			0.036	1.901	0.057

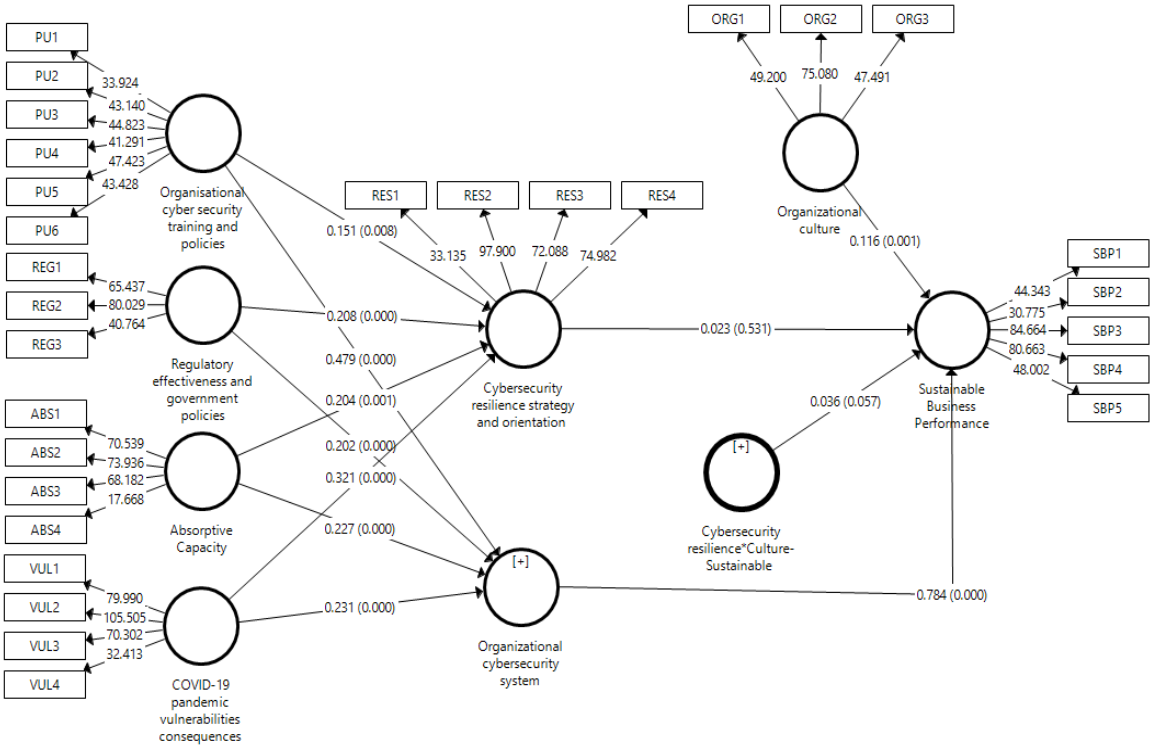

Figure 4. SEM model.

Mediating effects expound on how a specific variable can influence another by introducing an intervening variable. In our study, the hypotheses from H7 to H10 attempt to outline these effects. H7 to H9, which explore the influence of organizational cybersecurity training and policies, regulatory effectiveness and government policies, and absorptive capacity on sustainable business performance through cybersecurity resilience strategy and orientation, do not seem statistically significant. Their corresponding values, such as the β-values (0.004 to 0.005) and *p*-values (ranging from 0.546 to 0.566), validate this lack of significance. Similarly, H10, which observes the mediating role of cybersecurity resilience strategy and orientation in the relationship between the COVID-19 pandemic vulnerability consequences and sustainable business performance, also appeared insignificant, as supported by its corresponding values (β = 0.008, *t* = 0.616, *p* = 0.538).

Moderating effects shed light on how the relationship dynamics between two variables might evolve based on the level of a third variable. In this context, H11 is crucial. The interaction between cybersecurity resilience strategy and orientation and organizational culture has implications for sustainable business performance. Although this effect was marginally significant (β = 0.036, *t* = 1.901, *p* = 0.057), it hints that organizational culture might slightly moderate the relationship between cybersecurity resilience strategy and sustainable business performance.

Finally, the findings showed that H1, H2, H3, H4, H5, and the direct effect of organizational culture on sustainable business performance were significant and are therefore accepted. In contrast, hypotheses H6, H7, H8, H9, and H10 were not statistically significant and thus are rejected. The outcome for H11 teeters on the edge of significance, suggesting a potential area for future investigation or more expansive data collection to derive a conclusive stance. It is worth noting that the direct effect of organizational culture on sustainable business performance was tested, and this effect was significant (β = 0.116, *t* = 3.432, *p* = 0.001).

5. Discussion

The study was conducted in Saudi Arabia by targeting SMEs in the service and manufacturing sectors. The study used a quantitative research design by administering a

survey questionnaire. As from the plethora of research studies presented over the years, cybersecurity and organizational resilience have garnered significant attention recently. The recognition of the interplay between technological advancements and the strategic capabilities of organizations and the subsequent impacts on resilience is a theme that resonates throughout many of these studies. This is especially true during challenges such as the COVID-19 pandemic. For example, Wided's [54] study on IT capabilities and organizational resilience in SMEs post COVID-19 aligns with the consensus that integrating advanced IT capabilities such as big data analytics strengthens strategic flexibility and resilience in an organization. This echoes the findings of Huang and Pearlson's [69] work, which highlighted the importance of cultivating a cybersecurity culture within an organization and suggested that technology, while essential, is not the only solution; cultural and strategic alignment is equally as important.

Drawing parallels with previous studies, the emphasis on absorptive capacity as a cornerstone for cyber-resilience is consistently highlighted. Cybersecurity resilience is dependent on absorptive capacity. The research conducted by Levinson [79] investigated the importance of absorptive capacities in promoting proactive and inclusive approaches to cybersecurity governance. This is consistent with Chowdhury and Quaddus's [51] research, in which they discussed resiliency utilizing the dynamic capability theory and asserted that absorptive capacity is essential to the long-term viability of supply chains. This finding is consistent with their findings. This points to a trend in the research that indicates that for organizations to be adaptable and resilient, they need to recognize, assimilate, and exploit new information effectively. In addition, the cybersecurity landscape is not limited to technical defenses and strategies; rather, it encompasses a broader spectrum including human factors, governance, and regulatory frameworks. This is because technical defenses and strategies are only part of the equation. For instance, the systematic review conducted by Nifakos et al. [55] emphasized human factors' role in cybersecurity within healthcare organizations. This supports the findings of other research, such as that conducted by Rajamäki et al. [56], highlighting the necessity of providing cybersecurity education in hospitals. Concerning governance, the research conducted by Clark-Ginsberg and Slayton [89] highlighted the significance of regulating risks within complex systems. This perspective is congruent with the research conducted by Wessel [58] on the role that regulation plays in enhancing the cybersecurity resilience of the European Union.

Therefore, it is abundantly clear that the role that dynamic capabilities and strategic alignment plays in cultivating resilience is widely acknowledged across the studies. Garcia-Perez et al. [90] and Golgeci and Kuivalainen [71] found a relationship between digital transformation and resilience. Moreover, these findings echo the broader sentiment captured by Teece's [47,49] work on dynamic capabilities, which emphasized the need for organizations to continuously adapt, integrate, and reconfigure their internal and external competencies to address rapidly changing environments. This accumulated knowledge points toward an all-encompassing, multi-pronged approach to resiliency that incorporates technological prowess, human factors, governance, and the flexibility of strategic planning.

5.1. Managerial Implications

The service industry in Saudi Arabia is currently at a pivotal crossroads due to the country's rapidly developing digital landscape. According to Wided [54], managers in the service sector should prioritize investments in information technology capabilities and big data analytics to ensure strategic flexibility and organizational resilience. This is because there is an increasing dependence on these two areas. In light of the findings of Mian and Alatawi's [24] study, it is clear that there is a pressing need to improve cybersecurity, particularly in industries such as banking. Because of the inherently data-intensive nature of the service sector, the protection of customer and transactional data should be of the utmost importance. In addition, as digital service touchpoints become more prevalent (such as online banking, e-commerce, and e-health), service providers should cultivate a robust cybersecurity culture. This requirement is based on the findings

of Huang and Pearlson [69]. In order to accomplish this goal, continuous training, regular risk assessments, and the cultivation of a culture in which everyone shares responsibility for cybersecurity are required.

In the years after COVID-19, the Saudi Arabian manufacturing sector, particularly the country's small- and medium-sized enterprises (SMEs), has been confronted with significant difficulties. According to Wided [54], for managers to succeed in such uncertain times, they need to integrate information technology capabilities into their operations to enhance their resilience and flexibility. In addition, research conducted by Andrawina and Govindaraju [80] highlighted the significance of absorptive capacity and knowledge sharing capability in enhancing innovation performance. In light of Saudi Arabia's role as a hub in the global supply chain, manufacturing companies in the country should prioritize supply chain visibility and improve their capacity for rapid adaptation to and adoption of innovative technologies and business procedures. According to Golgeci and Kuivalainen [71], the role of social capital in supply chain resilience is another important area of focus that should be examined. As a result, the leaders of the manufacturing sector in Saudi Arabia ought to prioritize cultivating vigorous, trusting relationships with their suppliers, partners, and other stakeholders. This will allow for more effective communication and collaboration and greater collective resilience in the face of disruptions.

Several hypotheses had insignificant effects for various reasons. For H6, cybersecurity resilience strategy and orientation have not displayed a significant effect on sustainable business performance, suggesting that while these strategies are important for immediate cybersecurity response [51,54], they might not have a significant impact on long-term business performance due to other cultural factors. The mediating effects in H7, H8, H9, and H10 have not shown significant mediating effects, suggesting that cybersecurity resilience strategy and orientation do not directly affect sustainable business performance. This might be because market dynamics, technological advances, or internal organizational factors drive sustainable business performance more [8,14,30]. The moderating effect of culture in H11, despite being close to significance, suggests that organizational culture improves sustainable business performance but has a weaker effect on cybersecurity resilience strategy.

5.2. Limitations and Future Directions

The current investigation is restricted by its heavy reliance on a select number of studies, which may not comprehensively capture the entire scope of information technology capabilities and cybersecurity in Saudi Arabia. In addition, by concentrating only on the service and manufacturing sectors, one risks missing nuanced insights from other important industries. Conducting empirical studies directly within Saudi organizations to gauge the real-time challenges and implementations of IT capabilities would be extremely helpful for future research and would be an excellent idea. Comparisons across industries rather than between the service and manufacturing sectors may produce more insightful results. Furthermore, because Saudi Arabia's Vision 2030 emphasizes technological advancement and digital transformation, longitudinal studies that track the evolution of IT capabilities and cybersecurity measures over a decade can provide crucial insights into the nation's journey toward becoming a transformed state.

To overcome these limitations, future studies should broaden their scope by including a diverse range of industries beyond just service and manufacturing, thereby capturing a more comprehensive picture of IT capabilities and cybersecurity in Saudi Arabia. Longitudinal research in Saudi organizations can reveal real-time cybersecurity challenges and applications. Longitudinal studies aligned with Saudi Arabia's Vision 2030 would provide valuable insights into IT and cybersecurity evolution during digital transformation.

Author Contributions: Conceptualization, S.A.A.-S., R.R.S. and N.A.A.-S.; Methodology, S.A.A.-S., A.M.A. and N.A.A.-S.; Validation, R.R.S.; Formal analysis, S.A.A.-S.; Investigation, S.A.A.-S. and A.M.A.; Resources, A.M.A.; Data curation, Raneem R.R.S. and N.A.A.-S.; Writing—original draft, S.A.A.-S., A.M.A. and N.A.A.-S.; Writing—review & editing, S.A.A.-S. and R.R.S.; funding acquisition, S.A.A.-S. All authors have read and agreed to the published version of the manuscript.

Funding: This research work was funded by Institutional Fund Project under grant no. (IFPIP 1399-245-1443). The authors gratefully acknowledge technical and financial support provided by the ministry of education and King Abdulaziz University, DSR, Jeddah, Saudi Arabia.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: The datasets generated and analyzed during the current study are not publicly available due to privacy and confidentiality agreements as well as other restrictions. The datasets, however, are available upon reasonable request. Inquiries related to these may be submitted to the corresponding author.

Acknowledgments: We are grateful to all respondents who participated in this study.

Conflicts of Interest: The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

Appendix A. Theoretical Frameworks and Models Applied in SMEs' Context

Study	Underpinning Theories	Research Participants
Rawindaran et al. [15]	Stakeholder theory, resource-based view, and institutional theory	Wales SMEs
Wided [54]	Dynamic capability theory	Saudi Arabian SMEs
Hossain et al. [57]	Dynamic capability theory	Malaysian SMEs
Haseeb et al. [67]	Resource-based view theory	Malaysian SMEs
Zulkiffli et al.[81]	Resource-based view theory	Malaysian SMEs
Valdez-Juárez et al. [91]	Dynamic capability theory	Mexican SMEs
Skafi et al. [92]	The technology–organization–environment (TOE) framework	Lebanese SMEs
Donbesuur et al. [93]	The dynamic capability and the institutional theory	Ghana's SMEs

Appendix B. Measurement of Research Variables and Their Sources

Construct	Items	Reference
Organizational culture	ORG1: Innovation is a core value in this organization.	Dobni [74]; Zhang et al. [75]; Azanza et al. [76].
	ORG2: Our organization searches for new markets for existing products.	
	ORG3: In our organization, technological innovation is easily accepted.	
Organizational cybersecurity training and policies	PU1: Our organization conducts training sessions to raise cybersecurity awareness and to fill any gaps.	Zwilling et al. [16]; Wang et al. [50]; Shillair et al. [77].
	PU2: I am familiar with the term cybersecurity.	
	PU3: In our organization, there is average length of standard password.	
	PU4: We have adequate management support.	
	PU5: I have skills and knowledge in using computer applications.	
	PU6: I know how to behave in case of cyberattack.	

Construct	Items	Reference
Regulatory effectiveness and government policies	REG1: We have quicker responses to cybersecurity breaches to reduce the impact of reputational damage.	Srinivas et al. [78] ; Wang et al. [50].
	REG2: We have a cybersecurity regulation protect our systems and information from cyberattacks.	
	REG3: There are various government policies in protecting critical infrastructures against cyberattacks.	
Absorptive capacity	ABS1: Our company collaborates with external partners to foster innovation and drive creative advancements.	Zahra and George [61]; Levinson [79]; Andrawina and Govindaraju [80].
	ABS2: We collaborate with external partners to offer comprehensive programs designed to retrain and enhance the skills of our employees.	
	ABS3: We have established protocols with our partners for assessing, improving, and training our employees.	
	ABS4: In our company, we have available employees with the necessary skills to deal with cyberattacks.	
Sustainable business performance	SBP1: Net profit margin of our organization increased.	Haseeb et al. [67]; Zulkiffli et al. [81].
	SBP2: Return on investment of our organization increased.	
	SBP3: Profitability growth has been outstanding.	
	SBP4: Profitability has exceeded our competitors.	
	SBP5: Overall financial performance has exceeded competitors.	
Cybersecurity resilience strategy and orientation	RES1: We have data recovery capability in our organization.	Harrop and Matteson [82].
	RES2: We keep track of authorized and unauthorized devices and software.	
	RES3: There are secure configurations for hardware and software.	
	RES4: We have a strategy for monitoring and analyzing security audit logs.	
Vulnerabilities consequences ofCOVID-19 pandemic	VUL1: Cyberattacks during the COVID-19 pandemic increased.	Current study; Kumar et al. [83]; Pranggono and Arabo [84].
	VUL2: COVID-19 is having a crucial impact on our business.	
	VUL3: We implemented new innovations and systems to handle the COVID-19 pandemic situation.	
	VUL4: During COVID-19, the adoption of new business models and online applications has increased.	

References

1. Fox, J. Top Cybersecurity Statistics for 2024. Retrieved from Cobalt Website. Available online: https://www.cobalt.io/blog/cybersecurity-statistics-2024 (accessed on 8 January 2024).
2. Alotaibi, F.; Furnell, S.; Stengel, I.; Papadaki, M. A survey of cyber-security awareness in Saudi Arabia. In Proceedings of the 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST), Barcelona, Spain, 5–7 December 2016; pp. 154–158.
3. Kong, X.; Wu, Y.; Wang, H.; Xia, F. Edge Computing for Internet of Everything: A Survey. *IEEE Internet Things J.* **2022**, *9*, 23472–23485. [CrossRef]
4. Corallo, A.; Lazoi, M.; Lezzi, M. Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts. *Comput. Ind.* **2020**, *114*, 103165. [CrossRef]
5. Chege, S.M.; Wang, D. Information technology innovation and its impact on job creation by SMEs in developing countries: An analysis of the literature review. *Technol. Anal. Strateg. Manag.* **2020**, *32*, 256–271. [CrossRef]
6. Agyapong, D. Micro, small and medium enterprises' activities, income level and poverty reduction in ghana—A synthesis of related literature. *Int. J. Bus. Manag.* **2010**, *5*, 196. [CrossRef]
7. Carree, M.; Thurik, A.R. Small firms and economic growth in Europe. *Atl. Econ. J.* **1998**, *26*, 137–146. [CrossRef]

8. Kempegowda, S.M.; Chaczko, Z. Industry 4.0 Complemented with EA Approach: A Proposal for Digital Transformation Success. In Proceedings of the 26th International Conference on Systems Engineering (ICSEng), Sydney, Australia, 18–20 December 2018; pp. 1–6. [CrossRef]
9. Craigen, D.; Diakun-Thibault, N.; Purse, R. Defining cybersecurity. *Technol. Innov. Manag. Rev.* **2014**, *4*, 13–21. [CrossRef]
10. Kala, N.; Balakrishnan, M. Cyber Preparedness in Maritime Industry. *Int. J. Sci. Technol. Adv.* **2019**, *5*, 19–28.
11. Ismail, N. 7 Nightmare Cyber Security Threats to SMEs and How to Secure against Them. 2017. Available online: https://www.information-age.com/7-nightmare-cyber-security-threats-smes-secure-123466495/ (accessed on 12 July 2023).
12. Khan, N.F.; Ikram, N.; Saleem, S.; Zafar, S. Cyber-security and risky behaviors in a developing country context: A Pakistani perspective. *Secur. J.* **2022**, *36*, 373–405. [CrossRef]
13. Choo, K.-K.R. The Cyber Threat Landscape: Challenges and Future Research Directions. *Comput. Secur.* **2011**, *30*, 719–731. [CrossRef]
14. Jansen, J.; Veenstra, S.; Zuurveen, R.; Stol, W. Guarding against online threats: Why entrepreneurs take protective measures. *Behav. Inf. Technol.* **2016**, *1*, 368–379. [CrossRef]
15. Rawindaran, N.; Jayal, A.; Prakash, E.; Hewage, C. Perspective of small and medium enterprise (SME's) and their relationship with government in overcoming cybersecurity challenges and barriers in Wales. *Int. J. Inf. Manag. Data Insights* **2023**, *3*, 100191. [CrossRef]
16. Zwilling, M.; Klien, G.; Lesjak, D.; Wiechetek, Ł.; Cetin, F.; Basim, H.N. Cyber security awareness, knowledge and behavior: A comparative study. *J. Comput. Inf. Syst.* **2022**, *62*, 82–97. [CrossRef]
17. Carlton, M.; Levy, Y. Expert assessment of the top platform independent cybersecurity skills for non-IT professionals. In Proceedings of the 2015 IEEE SoutheastCon, Ft. Lauderdale, FL, USA, 9–12 April 2015; pp. 1–6. Available online: https://ieeexplore.ieee.org/abstract/document/7132932 (accessed on 20 June 2023).
18. Zulkipli, N.H.N. Synthesizing cybersecurity issues and challenges for the elderly. *Turk. J. Comput. Math. Educ. (TURCOMAT)* **2021**, *12*, 1775–1781.
19. Morgan, J.A. Exploring Senior Citizen Perceptions of Their Cyber Data Privacy and Security. Doctoral Dissertation, Capella University, Minneapolis, MN, USA, 2015.
20. Kuypers, M.A.; Maillart, T.; Paté-Cornell, E. *An Empirical Analysis of Cyber Security Incidents at a Large Organization*; Working Paper; Stanford University, School of Information: Palo Alto, CA, USA, 2016. Available online: https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/kuypersweis_v7.pdf (accessed on 12 June 2023).
21. Javaid, M.; Haleem, A.; Singh, R.P.; Suman, R. Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends. *Cyber Secur. Appl.* **2023**, *1*, 100016. [CrossRef]
22. Li, C.; Murad, M.; Shahzad, F.; Khan, M.A.S.; Ashraf, S.F.; Dogbe, C.S.K. Entrepreneurial Passion to Entrepreneurial Behavior: Role of Entrepreneurial Alertness, Entrepreneurial Self-Efficacy and Proactive Personality. *Front. Psychol.* **2020**, *11*, 1611. [CrossRef] [PubMed]
23. Alelyani, S.; Kumar, H. Overview of cyberattack on Saudi organizations. *J. Inf. Secur. Cybercrimes Res.* **2018**, *1*, 42–50. [CrossRef]
24. Mian, T.S.; Alatawi, E.M. Exploring Factors to Improve Intentions to Adopt Cybersecurity: A Study of Saudi Banking Sector. *Humanit. Nat. Sci. J.* **2023**, *4*, 101–115.
25. Ferdinand, J. Building organisational cyber resilience: A strategic knowledge-based view of cybersecurity management. *J. Bus. Contin. Emerg. Plan.* **2015**, *9*, 185–195.
26. Tagarev, T.; Sharkov, G.; Stoianov, N. Cybersecurity and resilience of modern societies: A research management architecture. *Inf. Secur.* **2017**, *38*, 93–108.
27. O'Reilly, C.A., III; Caldwell, D.F.; Chatman, J.A.; Doerr, B. The promise and problems of organizational culture: CEO personality, culture, and firm performance. *Group Organ. Manag.* **2014**, *39*, 595–625. [CrossRef]
28. Naranjo-Valencia, J.C.; Jiménez-Jiménez, D.; Sanz-Valle, R. Studying the links between organizational culture, innovation, and performance in Spanish companies. *Rev. Latinoam. Psicol.* **2016**, *48*, 30–41. [CrossRef]
29. Uddin, M.J.; Luva, R.H.; Hossian, S.M.M. Impact of organizational culture on employee performance and productivity: A case study of telecommunication sector in Bangladesh. *Int. J. Bus. Manag.* **2013**, *8*, 63. [CrossRef]
30. Singh, S.; Kumar, S. The Times of Cyber Attacks. *Acta Tech. Corvininesis—Bull. Eng.* **2020**, *13*, 133–137.
31. Sutton, D. *Cyber Security: A Practitioner's Guide*; BCS, The Chartered Institute for IT: Swindon, UK, 2017.
32. He, H.; Qi, W.; Liu, Z.; Wang, M. Adaptive attack-resilient control for Markov jump system with additive attacks. *Nonlinear Dyn.* **2021**, *103*, 1585–1598. [CrossRef]
33. Papadopoulos, T.; Baltas, K.N.; Balta, M.E. The use of digital technologies by small and medium enterprises during COVID-19: Implications for theory and practice. *Int. J. Inf. Manag.* **2020**, *55*, 102192. [CrossRef] [PubMed]
34. Gartner. Gartner Unveils Top Eight Cybersecurity Predictions for 2023–2024. 2023. Available online: https://www.gartner.com/en/newsroom/press-releases/2023-03-28-gartner-unveils-top-8-cybersecurity-predictions-for-2023-2024 (accessed on 2 September 2023).
35. Morgan, S. Cybercrime to Cost: The World $10.5 Trillion Annually by 2025. 2020. Available online: https://cybersecurityventures.com/cyberwarfare-report-intrusion/ (accessed on 13 September 2023).
36. Fortune Business Insights. Saudi Arabia Facility Management Market. Available online: https://www.fortunebusinessinsights.com/saudi-arabia-facility-management-market-106258 (accessed on 8 April 2023).

37. Dwivedi, Y.K.; Hughes, D.L.; Coombs, C.; Constantiou, I.; Duan, Y.; Edwards, J.S.; Upadhyay, N. Impact of COVID-19 pandemic on information management research and practice: Transforming education, work and life. *Int. J. Inf. Manag.* **2020**, *55*, 102211. [CrossRef]
38. Hasan, S.; Ali, M.; Kurnia, S.; Thurasamy, R. Evaluating the cyber security readiness of organizations and its influence on performance. *J. Inf. Secur. Appl.* **2021**, *58*, 102726. [CrossRef]
39. Shah, M.H.; Muhammad, R.; Ameen, N. Cybersecurity Readiness of E-tail Organisations: A Technical Perspective. In Proceedings of the Conference on e-Business, e-Services and e-Society, Skukuza, South Africa, 6–8 April 2020; Springer: Cham, Switzerland, 2020; pp. 153–160.
40. Raghavan, K.; Desai, M.S.; Rajkumar, P.V. Managing cybersecurity and ecommerce risks in small businesses. *J. Manag. Sci. Bus. Intell.* **2017**, *2*, 9–15.
41. Lloyd, G. The business benefits of cyber security for SMEs. *Comput. Fraud Secur.* **2020**, *2020*, 14–17. [CrossRef]
42. Harvey, J.T. An Economics Primer for Cyber Security Analysts. *Mil. Cyber Aff.* **2018**, *3*, 4. [CrossRef]
43. Kamat, A.; Tomar, C.; Tainwala, A.; Akram, S. Performance analysis and survey on security of password managers and various schemes of p2p models. In Proceedings of the 2018 3rd IEEE International Conference on Recent Trends in Electronics, Information and Communication Technology (RTEICT), Bangalore, India, 18–19 May 2018; pp. 23–26.
44. World Bank. Saudi Arabia. 2022. Available online: https://data.worldbank.org/country/saudi-arabia?view=chart (accessed on 7 July 2023).
45. Vision 2030. Saudi Vision 2030. 2016. Available online: https://vision2030.gov.sa/en (accessed on 20 June 2021).
46. Ambrosini, V.; Bowman, C. What are dynamic capabilities and are they a useful construct in strategic management? *Int. J. Manag. Rev.* **2009**, *11*, 29–49. [CrossRef]
47. Teece, D.J. A dynamic capabilities-based entrepreneurial theory of the multinational enterprise. *J. Int. Bus. Stud.* **2014**, *45*, 8–37. [CrossRef]
48. Danneels, E. Trying to become a different type of company: Dynamic capability at Smith Corona. *Strateg. Manag. J.* **2011**, *32*, 1–31. [CrossRef]
49. Teece, D.J. Dynamic capabilities and entrepreneurial management in large organizations: Toward a theory of the (entrepreneurial) firm. *Eur. Econ. Rev.* **2016**, *86*, 202–216. [CrossRef]
50. Wang, Z.; Kim, H.G. Can social media marketing improve customer relationship capabilities and firm performance? Dynamic capability perspective. *J. Interact. Mark.* **2017**, *39*, 15–26. [CrossRef]
51. Chowdhury, M.M.H.; Quaddus, M. Supply chain resilience: Conceptualization and scale development using dynamic capability theory. *Int. J. Prod. Econ.* **2017**, *188*, 185–204. [CrossRef]
52. Dangelico, R.M.; Pujari, D.; Pontrandolfo, P. Green product innovation in manufacturing firms: A sustainability-oriented dynamic capability perspective. *Bus. Strategy Environ.* **2017**, *26*, 490–506. [CrossRef]
53. Linnenluecke, M.K.; Griffiths, A. Corporate sustainability and organizational culture. *J. World Bus.* **2010**, *45*, 357–366. [CrossRef]
54. Wided, R. IT Capabilities, Strategic Flexibility and Organizational Resilience in SMEs Post-COVID-19: A Mediating and Moderating Role of Big Data Analytics Capabilities. *Glob. J. Flex. Syst. Manag.* **2023**, *24*, 123–142. [CrossRef]
55. Nifakos, S.; Chandramouli, K.; Nikolaou, C.K.; Papachristou, P.; Koch, S.; Panaousis, E.; Bonacina, S. Influence of human factors on cybersecurity within healthcare organisations: A systematic review. *Sensors* **2021**, *21*, 5119. [CrossRef]
56. Rajamäki, J.; Nevmerzhitskaya, J.; Virág, C. Cybersecurity education and training in hospitals: Proactive resilience educational framework (Prosilience EF). In Proceedings of the 2018 IEEE Global Engineering Education Conference (EDUCON), Santa Cruz de Tenerife, Spain, 17–20 April 2018; pp. 2042–2046.
57. Hossain, M.I.; Teh, B.H.; Tabash, M.I.; Alam, M.N.; San Ong, T. Paradoxes on sustainable performance in Dhaka's enterprising community: A moderated-mediation evidence from textile manufacturing SMEs. *J. Enterprising Communities People Places Glob. Econ.* 2022; *ahead-of-print*.
58. Wessel, R.A. Cybersecurity in the European Union: Resilience through regulation. In *Routledge Handbook of EU Security Law and Policy*; Conde, E., Yaneva, Z., Scopelliti, M., Eds.; Routledge: Abingdon, Oxfordshire, 2019; pp. 283–300.
59. Fuster, G.G.; Jasmontaite, L. Cybersecurity regulation in the European union: The digital, the critical and fundamental rights. *Ethics Cybersecur.* **2020**, *21*, 97–115.
60. Cohen, W.M.; Levinthal, D.A. Absorptive Capacity: A New Perspective on Learning and Innovation. *Adm. Sci. Q.* **1990**, *35*, 128–152. [CrossRef]
61. Zahra, S.A.; George, G. Absorptive capacity: A review, reconceptualization, and extension. *Acad. Manag. Rev.* **2002**, *27*, 185–203. [CrossRef]
62. AlHamdani, W.A. Resilient cybersecurity architecture. In Proceedings of the 15th International Conference on Cyber Warfare and Security, Norfolk, VA, USA, 12–13 March 2020; Academic Conferences and Publishing Limited: Cambridge, MA, USA, 2020; pp. 23–33.
63. Alahmari, A.; Duncan, B. Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence. In Proceedings of the 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), Dublin, Ireland, 15–17 June 2020; pp. 1–5.

64. Cheng, L.; Li, Y.; Li, W.; Holm, E.; Zhai, Q. Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *Comput. Secur.* **2013**, *39*, 447–459. [CrossRef]
65. Tam, T.; Rao, A.; Hall, J. The good, the bad and the missing: A Narrative review of cyber-security implications for australian small businesses. *Comput. Secur.* **2021**, *109*, 102385. [CrossRef]
66. Rahman, S.; Lackey, R. E-Commerce systems security for small businesses. *Int. J. Netw. Secur. Its Appl.* **2013**, *5*, 193–210. [CrossRef]
67. Haseeb, M.; Hussain, H.I.; Kot, S.; Androniceanu, A.; Jermsittiparsert, K. Role of social and technological challenges in achieving a sustainable competitive advantage and sustainable business performance. *Sustainability* **2019**, *11*, 3811. [CrossRef]
68. Watad, M.; Washah, S.; Perez, C. IT security threats and challenges for small firms: Managers' perceptions. *Int. J. Acad. Bus. World* **2018**, *12*, 23–30.
69. Huang, K.; Pearlson, K. For What Technology Can't Fix: Building a Model of Organizational Cybersecurity Culture. In Proceedings of the 52nd Hawaii International Conference on System Sciences, Maui, HI, USA, 8–13 January 2019; pp. 6398–6407.
70. AlDaajeh, S.; Saleous, H.; Alrabaee, S.; Barka, E.; Breitinger, F.; Choo, K.K.R. The role of national cybersecurity strategies on the improvement of cybersecurity education. *Comput. Secur.* **2022**, *119*, 102754. [CrossRef]
71. Gölgeci, I.; Kuivalainen, O. Does social capital matter for supply chain resilience? The role of absorptive capacity and marketing-supply chain management alignment. *Ind. Mark. Manag.* **2020**, *84*, 63–74. [CrossRef]
72. Turner Ii, B.L. Vulnerability and resilience: Coalescing or paralleling approaches for sustainability science? *Glob. Environ. Chang.* **2010**, *20*, 570–576. [CrossRef]
73. Daniel, B. Concepts of adversity, risk, vulnerability and resilience: A discussion in the context of the 'child protection system'. *Soc. Policy Soc.* **2010**, *9*, 231–241. [CrossRef]
74. Dobni, C.B. Measuring innovation culture in organizations: The development of a generalized innovation culture construct using exploratory factor analysis. *Eur. J. Innov. Manag.* **2008**, *11*, 539–559. [CrossRef]
75. Zhang, W.; Zeng, X.; Liang, H.; Xue, Y.; Cao, X. Understanding How Organizational Culture Affects Innovation Performance: A Management Context Perspective. *Sustainability* **2023**, *15*, 6644. [CrossRef]
76. Azanza, G.; Moriano, J.A.; Molero, F. Authentic leadership and organizational culture as drivers of employees' job satisfaction. *J. Work Organ. Psychol.* **2013**, *29*, 45–50. [CrossRef]
77. Shillair, R.; Esteve-González, P.; Dutton, W.H.; Creese, S.; Nagyfejeo, E.; von Solms, B. Cybersecurity education, awareness raising, and training initiatives: National level evidence-based results, challenges, and promise. *Comput. Secur.* **2022**, *119*, 102756. [CrossRef]
78. Srinivas, J.; Das, A.K.; Kumar, N. Government regulations in cyber security: Framework, standards and recommendations. *Future Gener. Comput. Syst.* **2019**, *92*, 178–188. [CrossRef]
79. Levinson, N. Inclusive Anticipatory Governance: Cyber Technologies, Absorptive Capacities & The Case of the United Nations Open-Ended Working Group re: ICTS. In Proceedings of the 2022 APSA Annual Meeting: Rethink, Restructure, and Reconnect, Montreal, QC, Canada, 15–18 September 2022.
80. Andrawina, L.; Govindaraju, R. Knowledge sharing capability, absorptive capacity, and innovation: An empirical study of Indonesia's information and communication technology industries. In Proceedings of the 2008 Knowledge Management International Conference 2008, langkawi, Malaysia, 10–12 June 2008.
81. Zulkiffli, S.N.A.; Zaidi, N.F.Z.; Padlee, S.F.; Sukri, N.K.A. Eco-Innovation Capabilities and Sustainable Business Performance during the COVID-19 Pandemic. *Sustainability* **2022**, *14*, 7525. [CrossRef]
82. Harrop, W.; Matteson, A. Cyber resilience: A review of critical national infrastructure and cyber security protection measures applied in the UK and USA. *J. Bus. Contin. Emerg. Plan.* **2014**, *7*, 149–162.
83. Kumar, M.; Patel, A.K.; Shah, A.V.; Raval, J.; Rajpara, N.; Joshi, M.; Joshi, C.G. First proof of the capability of wastewater surveillance for COVID-19 in India through detection of genetic material of SARS-CoV-2. *Sci. Total Environ.* **2020**, *746*, 141326. [CrossRef]
84. Pranggono, B.; Arabo, A. COVID-19 pandemic cybersecurity issues. *Internet Technol. Lett.* **2021**, *4*, e247. [CrossRef]
85. Hair, J.F.; Hult, G.T.M.; Ringle, C.; Sarstedt, M. *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*; Sage Publications: Thousand Oaks, CA, USA, 2017.
86. Henseler, J.; Ringle, C.M.; Sarstedt, M. A new criterion for assessing discriminant validity in variance-based structural equation modeling. *J. Acad. Mark. Sci.* **2015**, *43*, 115–135. [CrossRef]
87. Ringle, C.M.; Wende, S.; Becker, J.M. SmartPLS 3. Boenningstedt: SmartPLS GmbH. *J. Serv. Sci. Manag.* **2015**, *10*, 32–49.
88. Awang, Z.; Afthanorhan, A.; Mohamad, M.; Asri, M.A.M. An evaluation of measurement model for medical tourism research: The confirmatory factor analysis approach. *Int. J. Tour. Policy* **2015**, *6*, 29–45. [CrossRef]
89. Clark-Ginsberg, A.; Slayton, R. Regulating risks within complex sociotechnical systems: Evidence from critical infrastructure cybersecurity standards. *Sci. Public Policy* **2019**, *46*, 339–346. [CrossRef]
90. Garcia-Perez, A.; Cegarra-Navarro, J.G.; Sallos, M.P.; Martinez-Caro, E.; Chinnaswamy, A. Resilience in healthcare systems: Cybersecurity and digital transformation. *Technovation* **2023**, *121*, 102583. [CrossRef]
91. Valdez-Juárez, L.E.; Castillo-Vergara, M. Technological capabilities, open innovation, and eco-innovation: Dynamic capabilities to increase corporate performance of SMEs. *J. OpenInnov. Technol. Mark. Complex.* **2021**, *7*, 8. [CrossRef]

92. Skafi, M.; Yunis, M.M.; Zekri, A. Factors influencing SMEs' adoption of cloud computing services in Lebanon: An empirical analysis using TOE and contextual theory. *IEEE Access* **2020**, *8*, 79169–79181. [CrossRef]
93. Donbesuur, F.; Ampong, G.O.A.; Owusu-Yirenkyi, D.; Chu, I. Technological innovation, organizational innovation and international performance of SMEs: The moderating role of domestic institutional environment. *Technol. Forecast. Soc. Chang.* **2020**, *161*, 120252. [CrossRef]