International Journal of Scientific Research and Management (IJSRM)
||Volume||13||Issue||12||Pages||10162-10175||2025||
Website: https://ijsrm.net ISSN (e): 2321-3418
DOI: 10.18535/ijsrm/v13i12.em13

SMEs' Resilience Toward Cyberattacks in Saudi Arabia: A Review Paper

Saleh Alarifi

Taif University Saudi Arabia

Abstract
This paper is a literature review of articles published in various journals and conference proceedings, examining the resilience of small and medium-sized enterprises (SMEs) in Saudi Arabia against cyberattacks, drawing on 19 peer-reviewed studies published between 2020 and 2025, the synthesis integrates empirical surveys, case studies, policy analyses, and comparative research. It intends to help scholars interested in the topic by presenting the issues that have been stated in the review. This review paper also highlights open topics that can be undertaken in future research, The findings reveal that SME resilience is multidimensional, shaped by four interdependent pillars: technological tools, organizational strategies, policy support, and employee training and awareness. Despite notable progress under Saudi's Vision 2030, gaps persist in awareness, enforcement, and sectoral readiness. This review concludes with recommendations for policymakers, practitioners, and SME leaders, while highlighting limitations and future research opportunities in longitudinal assessments, sector-specific analyses, and evaluations of emerging technologies.

Keywords: Cyberattack, resilience, SMEs, Saudi Arabia

1. Introduction

Small and medium-sized enterprises (SMEs) in Saudi Arabia underpin diversification and digitalization agendas but are exposed to escalating cyber threats. National analyses and sectoral studies show growing incident volumes and evolving attack modalities in the Kingdom during 2012–2024 and beyond (Alharbi, 2025; Al-Hawamleh, 2024; Rawindaran et al., 2023). Within SME contexts, empirical studies report that resource constraints, competing priorities, and limited cyber situational awareness hinder the adoption of effective safeguards (Al-Somali et al., 2024; Renaud & Ophoff, 2021; Almoaigel & Abuabid, 2023).

Saudi Arabia's Vision 2030 has accelerated SME digital adoption, with the Monsha'at authority and financial regulators pushing for broader participation in the digital economy. Yet, this integration exposes SMEs to risks such as phishing, ransomware, data breaches, and supply-chain compromises (Alhejaili, 2024; Asfahani, 2024). National cybersecurity readiness has improved—Saudi Arabia ranked 2nd globally in the UN's Global Cybersecurity Index by mid-2020s (Al-Zahrani & Al-Salloum, 2025)—but SME-specific vulnerabilities persist. For example, organizational studies show that cybersecurity culture and employee responsibility perception strongly affect compliance, yet many SMEs lack structured policies or formal training (Asfahani, 2024; Al-Hawamleh, 2024). To address this issue, it could be useful to know the previous studies and to identify existing gaps that are essential to be investigated in future research.

Previous studies reviewed the recent cybersecurity research (Adriko & Nurse, 2024; Patterson et al., 2023; Naqvi et al., 2023) in global context. However, these articles paid less attention to the Saudi context. This review intends to contribute to this gap, which presents a literature review for a better understanding of the SMES' Resilience Toward Cyberattacks in Saudi Arabia. The aim of this study is to summarize the state of research regarding how small and medium-sized enterprises (SMEs) in Saudi Arabia are building resilience against cyberattacks. By focusing on the period between 2020 and 2025, this review identifies how SMEs engage with technological tools, organizational strategies, policy frameworks, and employee training initiatives, all of which contribute to improving their cybersecurity posture.

This review intends to address five objectives. First, to identify and analyze the body of research addressing Saudi SMEs' resilience to cyberattacks. Second, to highlight key challenges, barriers, and opportunities for SMEs to enhance resilience within the Saudi context. Third, to provide evidence-based insights and recommendations for policymakers, SME leaders, and researchers to strengthen SME cyber resilience under Vision 2030. Fifth, to identify existing gaps that are essential to be investigated in future research.

The remainder of this paper is organized as follows. Section 2 outlines the methodology applied in identifying and selecting the relevant studies, followed by the characteristics of included studies within several themes. Section 3 presents a description of the thematic Synthesis by resilience dimensions. Section 4 synthesizes the findings across the four resilience dimensions—technological tools, organizational strategies, policy support, and employee training—while reflecting on the challenges and opportunities identified in the literature. Section 5 discusses the broader implications for research, policy, and practice. Finally, Section 6 concludes the review by summarizing key insights, acknowledging limitations, and offering directions for future research.

2. Methods

2.1 Search Strategy and Selection Process

To conduct the review, a comprehensive search was conducted in July 2025 across the following electronic databases: Scopus, Web of Science, IEEE Xplore, ACM Digital Library, ScienceDirect, and Google Scholar. The study searched for specialized journals and publishers relevant to cybersecurity and regional studies (e.g. MDPI, Taylor & Francis, and Springer journals known to publish cybersecurity research). To ensure thorough coverage, manual searching of reference lists from key articles was performed (backward citation tracking), and forward citation searching was used to find newer studies citing the key articles.

The search strategy was developed iteratively and tailored for each database. We combined terms reflecting three concepts: SMEs, Cybersecurity, Resilience, and Saudi. For example, in Scopus and Web of Science the query used was:

("cybersecurity" OR "cyber security" OR "cyber-attack" OR "cyber attack" OR "cyber threat" OR "information security") AND ("SME" OR "small business" OR "small enterprise" OR "medium enterprise" OR "small and medium") AND ("Saudi Arabia") AND ("Resilience")

Similar queries were adapted for other databases. We also included specific keywords for known initiatives (e.g. "Essential Cybersecurity Controls", "Saudi NCA") and context terms like "digital transformation", "FinTech", "cyber law", "cyber insurance", paired with country name, to capture studies focused on those aspects. On Google Scholar, which allows full-text search, we used combinations like *"SME cybersecurity resilience Saudi"* and *"cybersecurity SMEs Saudi"*.

After reviewing titles and abstracts, 298 of the 350 potentially eligible papers were considered relevant. Their abstracts were reviewed by the author using predefined criteria. Fifty studies were selected for full paper review, and 19 of these were eligible.

2.2 Inclusion, Exclusion, Data Extraction, and Synthesis

The review focused on studies published between 2020 and 2025 that examined the cybersecurity or cyber resilience of small and medium-sized enterprises (SMEs) in Saudi Arabia across any sector. To be considered, studies need to address at least one of the four core resilience dimensions, technological tools, organizational strategies, policy support, or employee training, and to be peer-reviewed publications, including journal articles, conference papers, case studies, or systematic reviews. Works outside the scope, such as those not related to SMEs, not specific to Saudi Arabia, or published prior to 2020, were not considered. The qualitative coding and thematic organization of the reviewed studies were supported using NVivo software, which facilitated systematic coding, comparison across studies, and the aggregation of findings within and across the four resilience dimensions.

For each article that was included, specific metadata was extracted to support systematic synthesis. These details comprised the author(s) and year of publication, the type of study (such as empirical, theoretical, case study, or doctrinal analysis), the SME sectoral focus, the principal findings related to resilience, and the mapping of those findings to one or more of the four resilience dimensions. This information was consolidated in the Study Characteristics Table (1).

The synthesis of findings followed a thematic analysis approach. First, the key insights from each study were coded in relation to the four resilience dimensions. Next, these coded findings were collated into a

Thematic Summary Matrix designed to highlight patterns of convergence, divergence, and knowledge gaps. Finally, when studies referred to sector-specific issues such as ransomware in healthcare SMEs, trust and payment security in e-commerce, or regulatory compliance in financial services which were grouped to allow cross-sectoral comparisons.

The decision to code the literature using four core resilience dimensions—technological tools, organizational strategies, policy support, and employee training and awareness—was guided by prior organizational resilience and cybersecurity scholarship, which consistently conceptualizes resilience as a multi-layered construct spanning technical, human, organizational, and institutional levels. These dimensions reflect commonly identified stages and enablers of resilience, including prevention, preparedness, response, and recovery, as discussed in earlier resilience frameworks.

A fully open coding approach was not adopted because the objective of this review was not to generate an entirely new resilience taxonomy, but rather to consolidate and synthesize existing knowledge within a coherent analytical structure. However, inductive coding was used within NVivo to capture sub-themes and contextual nuances emerging within each dimension. This hybrid approach ensured both analytical rigor and flexibility, allowing emergent insights to be incorporated without compromising comparability across studies.

Table 1. Characteristics of Included Studies (2020–2025)

Authors (Year)	Type/Method	SME/Context	Key Findings on Resilience	Resilience Dimension(s)
Adriko & Nurse (2024)	Systematic Literature Review	Global SMEs, with Saudi relevance	Cyber insurance can improve resilience; uptake low due to lack of awareness and complex policies.	Policy; Organizational
Ahmed & Nanath (2021)	Empirical (Survey)	Saudi SMEs	Highlighted digital transformation pressures; SMEs lag in adopting cybersecurity best practices.	Technological; Organizational
Alghamdi & Abuabid (2023)	Empirical	Saudi SMEs (various sectors)	Found gaps in SME IT governance maturity; called for alignment with NCA controls.	Organizational; Policy
Almoaigel & Abuabid (2023)	Empirical (CSA Model)	Saudi SMEs	Higher cyber situational awareness leads to more adoption of security controls.	Employee training; Technological
Alorabi & Abuanzeh (2024)	Empirical (Survey)	Saudi SMEs	Stressed digital literacy and cyber hygiene as critical resilience factors.	Training; Technological
Al-Zahrani & Al-Salloum (2025)	Conceptual/Policy	Saudi SMEs	Traced Saudi Arabia's rise to 2nd in GCI; attributed to NCA policy and Vision 2030.	Policy
Elmaasrawy & Tawfik (2024)	Empirical	Saudi SMEs	Focused on employee awareness training effectiveness during digital adoption.	Training; Organizational

Al Oraini (2024)	Case Analysis	Saudi SMEs (public–private mix)	Found uneven adoption of ECC-1:2018 among SMEs; recommended sectoral support.	Policy; Organizational
Albalawi (2025)	Empirical (Survey)	Saudi SMEs	Linked digital supply chain resilience with cybersecurity investment.	Technological; Organizational
Alghamdi et al. (2024)	Empirical	Saudi SMEs (cross-sector)	Found correlations between IT investment and resilience outcomes.	Technological
Alharbi (2025)	Longitudinal Incident Analysis	National (SMEs included)	Analyzed cyber incidents 2012–24; ransomware spikes during COVID disrupted SMEs.	Technological; Policy
Al-Hawamleh (2024)	Empirical (Survey, SEM)	Saudi e-government (lessons for SMEs)	Employee training + compliance boosted service resilience; culture had mixed impact.	Training; Organizational
Alhejaili (2024)	Legal/Doctrinal	Saudi e-commerce SMEs	Found gaps in enforcement of cyber laws; stressed consumer trust and adaptive regulation.	Policy
Al-Somali et al. (2024)	Empirical (Survey, SEM)	Saudi service/manufacturing SMEs	IT systems boost resilience; culture & resilience strategy had weaker performance links.	Technological; Organizational
Asfahani (2024)	Empirical (Survey)	Saudi organizations	Employees' perception of organizational responsibility drives secure behavior.	Organizational; Training
GCC (Goldani, 2024)	Quantitative (ML Forecast)	GCC incl. Saudi	Projected security indices; underscored importance of economic diversification for cyber stability.	Policy
Rawindaran et al. (2023)	Mixed (Saudi–UK comparative)	Saudi SMEs	Resistance stems from low awareness + cost; adherence to ECC guidelines poor.	Policy; Training
Renaud & Ophoff (2021)	Empirical (Survey, UK SMEs, reference model)	SMEs (UK, comparative relevance)	Situational awareness predicts adoption of controls more than resources do.	Training; Technological
Varma et al.	Empirical	Saudi SMEs	Found digital	Technological;

(2023)	(Survey)		resilience depends on cybersecurity alignment with business models.	Organizational

3. Results

Before presenting the thematic synthesis, it is important to clarify the empirical scope of the reviewed literature. Only a subset of the included studies relied on primary data collected directly from Saudi small and medium-sized enterprises, while the remaining studies were conceptual, policy-oriented, or drew on broader organizational or comparative datasets. As a result, the findings of this review reflect a synthesis of both Saudi-specific empirical evidence and contextualized insights adapted from closely related settings. This reinforces the need for caution in firm-level generalization and highlights the importance of future SME-focused empirical research in the Saudi context.

3.1 Thematic Synthesis by Resilience Dimension

To provide a structured understanding of how Saudi SMEs address cyber threats, the findings of the reviewed studies were synthesized across four interrelated dimensions of resilience as shown in table (2): technological tools, organizational strategies, policy support, and employee training. This thematic framework not only captures the range of interventions reported in the literature but also highlights the interplay between technical measures, managerial practices, regulatory environments, and human factors. By examining each dimension in turn, the review illustrates both the progress made and the persistent gaps that shape the current resilience landscape of Saudi SMEs.

Table2: Thematic Summary Matrix

Resilience Dimension	Key Themes	Representative Studies	Evidence Strength	Gaps Identified
Technological Tools	Baseline controls (firewalls, MFA, backups); advanced solutions (EDR, cloud security); reliance on affordable tools; integration challenges.	Al-Somali et al. (2024); Varma et al. (2023); Alghamdi et al. (2024); Alharbi (2025); Renaud & Ophoff (2021)	Strong empirical evidence across multiple contexts.	High-cost barriers; lack of in-house expertise; poor configuration practices.
Organizational Strategies	Leadership responsibility; IT governance maturity; proactive culture; adaptability; insurance as risk transfer.	Asfahani (2024); Alghamdi & Abuabid (2023); Al-Somali et al. (2024); Adriko & Nurse (2024); Al-Oraini (2024)	Moderate to strong, though evidence is mostly survey-based.	Limited longitudinal insights: lack of data on SMEs that implemented governance reforms.
Policy Support	NCA ECC controls; e-commerce law; SAMA frameworks; GCC cooperation; role of incentives.	Alhejaili (2024); Rawindaran et al. (2023); Al-Zahrani & Al-Salloum (2025); GCC (2024)	Mixed evidence: policies exist, but adoption remains low among SMEs.	Enforcement challenges; policies often too complex for SMEs; weak monitoring of compliance outcomes.
Employee Training & Awareness	Awareness campaigns; phishing defense; remote work security; linking training to culture.	Al-Hawamleh (2024); Elmaasrawy & Tawfik (2024); Renaud & Ophoff (2021); Almoaigel & Abuabid (2023); Asfahani (2024)	Strong and consistent across multiple studies.	Limited evaluation of training sustainability; lack of evidence on long-term behavior change.

3.1.1. Technological Tools

Technological tools form the backbone of SMEs' defense mechanisms against cyber threats. Across the 19 studies reviewed, the adoption, implementation, and maintenance of technological safeguards consistently emerge as the most visible and measurable elements of resilience. Yet, the literature shows a present a complex view: while many SMEs recognize the importance of investing in cybersecurity technologies, practical barriers such as cost, expertise, and awareness, frequently prevent full implementation (Al-Somali et al., 2024; Alghamdi et al., 2024; Varma et al., 2023).

3.1.1.1. *Core technologies and baseline controls*

Several studies emphasize the necessity of baseline security controls, which include firewalls, antivirus software, regular patch management, and secure password policies. These are often described as "hygiene measures" that every SME must adopt to protect against opportunistic attacks (Renaud & Ophoff, 2021; Almoaigel & Abuabid, 2023). Al-Somali et al. (2024) empirically demonstrated that SMEs with documented and enforced IT security controls reported higher levels of organizational resilience, even when other cultural or strategic elements were weaker. Similarly, Varma et al. (2023) highlighted that SMEs that implemented endpoint protection and basic intrusion detection tools exhibited significantly fewer operational disruptions during attempted cyberattacks.

3.1.1.2. Advanced and Sector-Specific Technologies

Post to 2020, a trend toward advanced cybersecurity technologies among Saudi SMEs is noticeable. Alharbi (2025), in a longitudinal analysis of Saudi cyber incidents from 2012–2024, noted a marked increase in ransomware and phishing attacks during the COVID-19 pandemic. In response, SMEs increasingly deployed advanced tools such as endpoint detection and response (EDR), multi-factor authentication (MFA), and cloud-based security services. These tools, while not always universally adopted, are becoming more common, particularly in fintech and healthcare SMEs, where regulatory pressure is stronger (Alhejaili, 2024; Al-Zahrani & Al-Salloum, 2025).

E-commerce SMEs present a unique case, for example, Alhejaili (2024) argued that despite the legal requirement to secure consumer transactions under Saudi's e-commerce law, many small online vendors still lack strong encryption or secure payment gateways, exposing customers to fraud. This indicates that even where policy mandates technology adoption, enforcement and SME capacity constraints limit effectiveness.

3.1.1.3. Challenges in Technology Uptake

The cost barrier is one of the most repeated themes. SMEs, often operating on narrow margins, hesitate to allocate scarce resources to cybersecurity when the benefits are not immediately visible (Rawindaran et al., 2023; Ahmed & Nanath, 2021). This leads to reliance on outdated systems or free tools, which may lack robustness. Moreover, the expertise gap, the lack of in-house IT, or cybersecurity specialists, means that SMEs may not configure tools properly, which may lead to interpreting them less effectively (Alghamdi & Abuabid, 2023).

Renaud & Ophoff (2021) provide an insightful comparative perspective: in their UK-based survey, SMEs often possessed the necessary tools but failed to implement them effectively due to lack of awareness. This aligns with Almoaigel & Abuabid (2023), who found that in Saudi SMEs, cyber situational awareness was the strongest predictor of technology adoption. In other words, SMEs aware of their vulnerabilities and threats were more likely to use their tools correctly and consistently.

3.1.1.4. Linking Technology to Resilience Outcomes

The reviewed literature consistently links technological adoption to positive resilience outcomes, though with caution. Al-Somali et al. (2024) demonstrated a direct positive relationship between IT system investments and SME resilience and business performance. Albalawi (2025) extended this by showing that supply chain resilience among SMEs was strengthened by investments in digital tools that enhanced both operational efficiency and cybersecurity.

Nevertheless, the effectiveness of these tools depends on integration with organizational practices. Alorabi and Abuanzeh (2024) stated that SMEs with poor digital literacy may adopt technologies superficially, failing to realize their potential. Elmaasrawy and Tawfik (2024) also note that technology adoption without corresponding employee training leads to minimal resilience gains, since staff continue to introduce vulnerabilities (e.g., weak passwords, unsafe browsing).

3.1.1.5. Conclusion for Technological Tools

Technological adoption is essential but insufficient in isolation. Saudi SMEs are adopting a growing mix of baseline and advanced tools, particularly under the influence of government policy and sectoral regulation. Yet challenges of cost, expertise, and awareness persist. The literature stresses that resilience requires not only acquiring the right technologies but also ensuring proper configuration, continuous updating, and integration into daily operations. Technological resilience is strongest when accompanied by informed users and supported by organizational and policy frameworks (Al-Somali et al., 2024; Alharbi, 2025; Rawindaran et al., 2023).

3.2.2. Organizational strategies

Organizational strategies represent the "soft infrastructure" of resilience: the policies, leadership decisions, and cultural elements that shape how SMEs perceive, prioritize, and respond to cybersecurity. Several of the reviewed studies stress that even with robust technological investments, SMEs often remain vulnerable if organizational governance is weak (Al-Somali et al., 2024; Asfahani, 2024; Alghamdi & Abuabid, 2023).

3.2.2.1 Leadership and Responsibility.

A recurring theme is the role of leadership. Asfahani (2024) found that employees' secure behavior was most strongly influenced by their perception of whether the organization itself took cybersecurity responsibility seriously. This confirms that SME leadership, often the owner or a small management team, sets the tone. When leaders model compliance, allocate resources, and communicate that cybersecurity is a business priority, employees are far more likely to follow safe practices. Conversely, if leaders neglect cyber issues, employees often assume it is not important.

3.2.2.2 Policies and Governance Maturity.

Alghamdi & Abuabid (2023) documented how many Saudi SMEs lack mature IT governance structures, such as formal cybersecurity policies, risk assessments, and designated security roles. This immaturity undermines resilience, since incidents are handled ad hoc rather than via prepared responses. Al-Somali et al. (2024) found that SMEs with documented resilience strategies (e.g., incident response or continuity plans) had better long-term stability, even though short-term performance effects were weaker. Such findings indicate that resilience planning is a long-term investment that requires patience.

3.2.2.3 Organizational Culture.

Cybersecurity culture refers to employees shared values and attitudes toward secure practices, was examined by multiple studies. Al-Somali et al. (2024) showed that culture alone did not immediately boost business performance, but they stressed its importance as a foundation for resilience. When combined with technological investments, culture reinforced compliance and vigilance. In addition, Rawindaran et al. (2023) highlighted that cultural apathy was a resistance factor limiting SME engagement with NCA guidelines.

3.2.2.4 Dynamic Capabilities and Adaptability.

SMEs differ from large firms in that they have limited safeguards. Studies emphasize the importance of dynamic capability which means that an organization's ability to adapt quickly to new threats. Albalawi (2025) linked resilience in digital supply chains to organizational adaptability, where SMEs that integrated cybersecurity into broader supply chain strategies bounced back faster after disruptions. Al-Oraini (2024) also noted that SMEs with flexible governance could more effectively comply with the ECC-1:2018 controls, while rigid or poorly resourced SMEs lagged.

3.2.2.5 Risk Transfer and Insurance.

Adriko & Nurse (2024) added a novel organizational strategy: cyber insurance. Their review found that insurance can improve resilience by offsetting losses and encouraging SMEs to adopt baseline controls (since insurers require them). However, uptake in Saudi SMEs is very low due to limited understanding of cyber risk and the complexity of insurance policies. This suggests that insurance should be framed not as a luxury, but as a risk management tool added to internal strategies.

In summary, organizational strategies such as leadership commitment, formal policies, a strong culture, adaptability, and risk transfer mechanisms are critical complements to technology. The evidence shows that SMEs with proactive governance weather cyber challenges better than those that rely on reactive responses.

3.2.3. Policy support

Policy frameworks provide the external scaffolding for SME resilience. In Saudi Arabia, the National Cybersecurity Authority (NCA) and sector regulators have issued controls and guidelines, yet several studies find persistent gaps in enforcement and SME compliance (Alhejaili, 2024; Rawindaran et al., 2023; Al-Zahrani & Al-Salloum, 2025).

3.2.3.1. National and Sectoral Policies.

Al-Zahrani & Al-Salloum (2025) attribute Saudi Arabia's rise to 2nd place in the UN Global Cybersecurity Index to strong national frameworks. The NCA's Essential Cybersecurity Controls (ECC-1:2018) set a baseline for organizations, including SMEs, covering governance, asset management, and technical safeguards. In finance, the Saudi Central Bank (SAMA) enforces a strict cybersecurity framework; in healthcare, data protection policies are emerging.

3.2.3.2. Policy–Practice Gap.

Despite strong frameworks, SMEs often fail to implement them. Alhejaili (2024) found that while Saudi e-commerce law mandates consumer data protection, enforcement is weak, and many SMEs still neglect secure payment gateways or encryption. Rawindaran et al. (2023) confirmed that SME adherence to ECC-1:2018 remains poor, with resistance due to cost, lack of expertise, and competing business priorities.

3.2.3.3. International and Comparative Lessons.

Rawindaran et al. (2023) contrasted Saudi SMEs with UK SMEs, showing that while both countries have SME-specific guidance (Saudi's ECC vs. UK's Cyber Essentials), Saudi SMEs face greater barriers in awareness and resources. This underscores the importance of adapting policy to local realities. Furthermore, Alhejaili (2024) noted that the need for international cooperation, as cross-border e-commerce exposes Saudi SMEs to global risks that domestic laws alone cannot mitigate.

3.2.3.4. Incentives and Public–Private Partnerships.

Adriko and Nurse (2024) recommended incentives for SMEs to adopt cyber insurance, such as tax breaks or simplified policies. Rawindaran et al. (2023) called for public–private partnerships to engage SMEs, suggesting that government, industry associations, and large corporations work together to create affordable solutions. The GCC-wide analysis (GCC, 2024) also emphasized that regional cooperation could help harmonize policies, reducing fragmentation for SMEs operating across borders.

3.2.3.5. Legal Evolution.

Al-Oraini (2024) observed that while Saudi policies are comprehensive on paper, SMEs often find them complex. Simplification such as sector-specific guidelines in plain Arabic would improve acceptance. Elmaasrawy and Tawfik (2024) added that employee-level awareness of policies is often low, so organizational translation of policy into practice is necessary.

In summary, policy support in Saudi Arabia has advanced rapidly, but enforcement and practical commitment by SMEs remain inconsistent. Policies must not only exist but also be accessible, incentivized, and supported by partnerships that make compliance achievable for SMEs.

3.2.4. Employee training and awareness

If technology is the backbone and policy the framework, employees are the frontline of SME cyber resilience. Seven of the nineteen studies directly examined employee awareness, and all underscored its decisive role (Al-Hawamleh, 2024; Renaud & Ophoff, 2021; Almoaigel & Abuabid, 2023; Elmaasrawy & Tawfik, 2024).

3.2.4.1. Awareness as a Predictor of Control Adoption.

Renaud and Ophoff (2021) found that situational awareness predicted the adoption of controls more strongly than financial resources. This was resonated in Saudi contexts by Almoaigel and Abuabid (2023), who empirically showed that SMEs with higher employee awareness levels had significantly greater implementation of cybersecurity controls.

3.2.4.2. Training Programs.

Al-Hawamleh (2024) demonstrated that structured training improved not only cybersecurity practices but also the quality of e-services, underscoring that training benefits extend beyond security. Elmaasrawy and Tawfik (2024) confirmed that continuous employee education, especially during digital transformation projects improved SME resilience outcomes.

3.2.4.3. Human Error and Culture.
Many cyber incidents in SMEs stem from human error such as weak passwords, falling for phishing, and unsafe downloads. Studies highlight that training reduces these errors. Asfahani (2024) noted that personal experience with cyber incidents did not automatically improve behavior, thus, structured organizational responsibility and training were necessary.

3.2.4.4. Pandemic Lessons.
Alharbi (2025) reported that a surge of ransomware during COVID-19, exploiting remote work practices. SMEs that trained employees on secure home networks, VPN use, and phishing defense coped better. This illustrates that training must evolve with the threat landscape.

3.2.4.5. Organizational Integration.
Training is most effective when embedded into organizational culture. Al-Somali et al. (2024) stressed that culture reinforces training, while Rawindaran et al. (2023) observed that apathy toward awareness campaigns reduced SME compliance. Integrating training into onboarding, performance reviews, and daily routines creates sustainable awareness.
In conclusion, employee training is the most cost-effective resilience strategy for SMEs. It empowers staff as active defenders, reduces reliance on technology alone, and complements organizational and policy frameworks. The evidence strongly supports regular, adaptive, and organization-wide awareness initiatives as a cornerstone of SME resilience.

4. Discussion
The synthesis of 19 studies reveals that Saudi SMEs' cyber resilience is a multidimensional construct that cannot be reduced to technological adoption alone. Instead, resilience is achieved when technological tools, organizational strategies, policy support, and employee training are integrated into a holistic framework. This discussion interprets the evidence, highlights challenges, and proposes practical pathways forward.

4.1. Technology–Human Integration
While technological safeguards remain foundational (Al-Somali et al., 2024; Varma et al., 2023), they are only as effective as the people and organizations behind them. Several studies (Almoaigel & Abuabid, 2023; Renaud & Ophoff, 2021) demonstrate that awareness and situational understanding determine whether tools are properly configured and used. This suggests that SMEs that invest in awareness programs may get better returns on their technological investments. Moreover, Alharbi (2025) indicated that during the COVID-19 pandemic, many SMEs quickly adopted remote access technologies but failed to secure them adequately, illustrating the dangers of tech adoption without human readiness.

4.2. Leadership and Organizational Culture
The reviewed studies consistently show that leadership shapes resilience outcomes. Asfahani (2024) highlighted how employees internalize indications about cybersecurity from management, while Alghamdi and Abuabid (2023) found that governance immaturity often left SMEs reactive instead of proactive. These findings imply that even in resource-constrained environments, leadership's role in embedding security into organizational routines is decisive. Building a security culture requires SMEs to normalize cybersecurity practices, thus, policies must be lived values, not just documents.

4.3. Policy–Practice Gaps
Policy frameworks in Saudi Arabia are comprehensive, yet evidence shows a persistent gap between formal requirements and SME compliance. Alhejaili (2024) documented a weak enforcement of e-commerce protections, and Rawindaran et al. (2023) observed resistance to ECC-1:2018 guidelines. This suggests that policy effectiveness depends not only on design but also on implementation strategies. SMEs often lack the

capacity to interpret complex regulations; hence, simplification and SME-focused toolkits are essential. Al-Oraini (2024) further stresses the need for practical sectoral adaptations, while Adriko and Nurse (2024) highlight how insurance could complement policy by incentivizing compliance.

4.4. Employee Training as Cornerstone

Perhaps the strongest consensus across studies is the centrality of employee training. Training is repeatedly linked with improvements in cyber hygiene, compliance, and even service quality (Al-Hawamleh, 2024; Elmaasrawy & Tawfik, 2024). Yet, as Asfahani (2024) stated, experience alone does not change behavior, thus, structured training and reinforcement are required. The pandemic demonstrated this intensely, SMEs that trained staff in secure remote practices were less affected by ransomware (Alharbi, 2025). Thus, training is not a marginal add-on but the essential key of SME resilience.

4.5. Sector-Sensitive Patterns

Although SMEs across Saudi Arabia share common cybersecurity challenges such as limited resources, awareness gaps, and compliance burdens, however, the reviewed studies reveal that resilience patterns differ across sectors.

4.5.1. Financial and fintech SMEs.

SMEs operating in finance-related activities are subject to stricter regulations by the Saudi Central Bank (SAMA). This regulatory pressure has pushed fintech and financial SMEs to adopt stronger baseline controls, including multi-factor authentication, transaction monitoring, and encryption standards (Al-Somali et al., 2024). These SMEs typically report higher maturity in governance and risk management but face challenges in integrating compliance with innovation speed, especially in emerging digital payment systems.

4.5.2. E-commerce SMEs.

E-commerce SMEs experience high exposure to trust and payment fraud issues. While Saudi Arabia's e-commerce law provides a framework for consumer data protection, weak enforcement and resource constraints leave smaller online vendors vulnerable (Alhejaili, 2024). Many rely on third-party payment platforms rather than investing in secure gateways, creating gaps in accountability and consumer confidence.

4.5.3. Manufacturing and industrial SMEs.

Saudi manufacturing SMEs, particularly those integrating Industry 4.0 technologies, encounter dual challenges: securing traditional IT systems while also protecting operational technology. Albalawi (2025) noted that disruptions in digital supply chains can cascade into broader operational breakdowns, making supply chain cybersecurity an urgent priority. However, SMEs often lack the budgets and skills to manage vendor-related risks.

4.5.4. Healthcare-adjacent SMEs.

SMEs supporting healthcare services face heightened risks due to the sensitivity of medical data. Alharbi (2025) recognized how ransomware attacks during COVID-19 disproportionately disrupted smaller healthcare providers and suppliers. These SMEs require stronger data protection, backup, and recovery systems, but many lag in compliance with emerging healthcare data regulations.

In short, sectoral differences underscore that resilience strategies must be tailored: fintech SMEs need compliance-innovation balance, e-commerce SMEs require trust-building mechanisms, manufacturing SMEs must secure supply chains, and healthcare SMEs must prioritize data integrity and recovery.

4.6. Theoretical Contributions

Although this review is motivated by a practical policy and managerial problem, it also makes several theoretical contributions to the literature on SME cybersecurity and organizational resilience. First, the study extends the cyber-resilience literature by contextualizing resilience within small business environments, which differ fundamentally from large organizations in terms of resources, governance structures, and decision-making autonomy. While prior resilience research often assumes formalized processes and dedicated security functions, this review highlights how resilience in SMEs is shaped by managerial judgment, informal practices, and external institutional support.

Second, the findings contribute to organizational resilience theory by reinforcing the multidimensional nature of resilience. By synthesizing the literature into four interrelated dimensions—technological tools,

organizational strategies, policy support, and employee training and awareness—this review provides a structured lens for examining how resilience emerges from the interaction between technical, human, and institutional factors. Rather than viewing resilience as a purely technical capability, the evidence underscores its socio-technical character, where technology adoption is mediated by leadership commitment, organizational culture, and regulatory context.

Third, this review contributes to the SME cybersecurity literature by demonstrating how national institutional environments shape resilience outcomes. The Saudi context, characterized by strong state involvement, centralized cybersecurity governance, and Vision 2030–driven digital transformation, illustrates how institutional pressure and policy infrastructure can compensate, to some extent, for SMEs' internal resource limitations. This insight extends prior SME resilience studies conducted in Western contexts by highlighting the moderating role of government-led digital ecosystems.

Finally, the study advances methodological contributions by applying a structured thematic synthesis to consolidate fragmented findings across empirical, conceptual, and policy-oriented studies. By mapping existing evidence onto a unified resilience framework, the review offers a foundation for future theory-building and hypothesis development in SME cyber resilience research beyond country-specific settings.

4.7 Future Research Directions

Although this review consolidates important insights into the resilience of Saudi SMEs against cyberattacks, it also reveals areas where further scholarly attention is required. One clear gap lies in the absence of longitudinal studies capable of tracking how resilience evolves over time, particularly in response to regulatory initiatives such as the NCA's Essential Cybersecurity Controls or the introduction of sustained employee training programs. Current evidence is largely cross-sectional, limiting the ability to establish causal relationships. There is also a need for deeper sectoral investigations. While finance, e-commerce, and manufacturing SMEs are relatively well represented, other vital sectors such as tourism, education, hospitality, and oil and gas supply chains remain underexplored, even though they play an increasingly important role in Saudi Arabia's economy under Vision 2030.

Future research would also benefit from detailed case study analyses of SMEs that have experienced and recovered from significant cyber incidents. Such accounts could provide practical lessons about response and recovery strategies that survey data alone cannot capture. Another underdeveloped area concerns the role of cyber insurance in SME resilience. Although existing studies recognize its potential value, empirical evidence regarding adoption, barriers, and tangible outcomes for Saudi SMEs remains limited. Additionally, as digital transformation accelerates, SMEs are adopting advanced technologies such as artificial intelligence, cloud computing, and the Internet of Things. These technologies both enhance resilience through improved detection and response and introduce new vulnerabilities that must be carefully studied. Finally, cultural and behavioral dimensions warrant closer attention. Understanding how local attitudes, language, and perceptions of risk influence the adoption of cybersecurity practices could provide nuanced insights into how to design more effective interventions for SMEs in Saudi Arabia.

4.7. Limitations

While this review provides valuable insights into the resilience of Saudi SMEs against cyberattacks, several limitations must be acknowledged. First, the evidence base was restricted to 19 studies published between 2020 and 2025 that were provided for analysis. Although this ensures a well-defined scope, it may have excluded other relevant works outside the dataset. Second, the review is geographically specific to Saudi Arabia region, which strengthens contextual relevance but limits the generalizability of findings to SMEs in other settings with different regulatory, cultural, or economic environments. A third limitation lies in the methodological concentration of the included studies mostly relied on cross-sectional survey designs and structural equation modeling, which, while valuable, do not permit strong causal inferences or track resilience development over time. Moreover, the distribution of research across sectors was uneven. While finance, e-commerce, and manufacturing SMEs were represented, sectors such as tourism, education, and hospitality received little to no empirical attention, leaving gaps in the understanding of resilience in those domains. Finally, publication bias may have influenced the findings, as studies with positive or significant results are more likely to be published than those reporting neutral or negative outcomes, potentially skewing the synthesis toward successful practices and interventions.

While many of the resilience factors identified in this review—such as awareness, training, and governance—are consistent with findings from international SME cybersecurity studies, the Saudi context introduces distinctive characteristics. Unlike many settings where SMEs operate with limited institutional support, Saudi SMEs are embedded within a centralized cybersecurity governance framework and an ambitious national digital transformation agenda. This institutional environment shapes resilience not through technological superiority alone, but through regulatory alignment, policy incentives, and coordinated national initiatives. However, the review also reveals that these advantages do not automatically translate into uniform SME resilience, highlighting the continued importance of internal organizational capabilities and human factors.

5. Practical Implications And Recommendations

This review offers several practice-oriented implications for small business owners, SME advisors, and entrepreneurship educators in Saudi Arabia.

5.1. Implications for SME Owners and Managers.

The findings suggest that cybersecurity should be treated as a strategic business risk rather than a purely technical issue. SME owners should prioritize foundational security controls, develop basic incident response and recovery plans, and embed cybersecurity responsibilities into daily operations. Employee training emerges as a cost-effective resilience lever, particularly for SMEs with limited technological budgets. Engaging with national initiatives and regulatory guidance can further strengthen preparedness while reducing compliance uncertainty.

5.2. Implications for SME Advisors and Support Organizations.

Business advisors, consultants, and chambers of commerce play a critical role in translating complex cybersecurity requirements into actionable guidance for SMEs. Advisory services should integrate cybersecurity risk assessments into standard business consulting practices and promote incremental, scalable solutions aligned with SME capabilities. Public–private partnerships can help reduce cost barriers and expand access to shared cybersecurity services.

5.3 Implications for Entrepreneurship Educators.

Entrepreneurship and business education programs should incorporate cybersecurity and digital resilience as core competencies. Integrating real-world SME case studies, cyber incident simulations, and risk management exercises can better prepare future entrepreneurs to operate in digitally intensive environments. Educators can also emphasize the strategic alignment between cybersecurity resilience and business sustainability under Vision 2030.

Together, these implications highlight the need for a coordinated ecosystem approach, where SMEs, advisors, educators, and policymakers collectively contribute to strengthening cyber resilience in the Saudi small business sector.

6. Conclusion

This review has brought together evidence from 19 peer-reviewed studies published between 2020 and 2025 to evaluate how Saudi Arabian SMEs are building resilience against cyberattacks. The synthesis demonstrates that resilience is not the product of a single factor but rather the interplay of four interconnected dimensions: technological adoption, organizational strategies, supportive policy frameworks, and employee training. Technology provides the baseline for defense, yet its effectiveness depends on leadership commitment, governance maturity, and a culture that encourages secure practices. Policy frameworks, particularly those advanced under the National Cybersecurity Authority and sectoral regulators, have raised national cybersecurity capacity, but gaps remain in enforcement and SME compliance. Above all, employee training emerges as the most consistent and cost-effective intervention, reducing vulnerabilities associated with human error and strengthening the integration of technology and organizational strategies.

Despite these advances, the findings point to uneven progress across sectors and highlight that SMEs continue to face barriers in terms of resources, awareness, and compliance. Strengthening resilience therefore requires not only technical investment but also simplified and accessible policies, stronger

leadership engagement, and sustainable training programs that evolve alongside the threat landscape. The review underscores that SMEs are indispensable to the realization of Saudi Arabia's Vision 2030, and their ability to withstand and recover from cyberattacks is vital for economic stability and growth. Continued collaboration among policymakers, practitioners, and researchers will be essential to ensure that the lessons from existing studies translate into practical outcomes, thereby embedding resilience as a core element of SME operations in the Kingdom.

Author Bio

Saleh Alarifi, Ph.D., B.Sc., is an Associate Professor at the College of Business, Taif University, Saudi Arabia, where he teaches and conducts research on cybersecurity governance, risk management, and digital resilience strategies for organizations, including small and medium enterprises (SMEs). Dr. Alarifi holds a Ph.D. and B.Sc. and has authored several peer-reviewed articles on topics such as cyber preparedness, digital transformation, and organizational performance in digitally intensive environments. His research bridges academic inquiry and practical guidance, with a focus on how businesses can enhance resilience against evolving cyber threats within the Saudi and broader Middle Eastern context. He is active in academic and professional communities that promote cybersecurity awareness and capacity building among leaders, educators, and practitioners.

References

1. Adriko, A., & Nurse, J. R. C. (2024). Opportunities for cyber insurance to address the challenges of cyberattacks: Repercussions for SMEs. University of Sharjah Journal of Law Sciences, 22(1), 560–607. https://doi.org/10.36394/jls.v22.i1.20
2. Ahmed, N. N., & Nanath, K. (2021). Exploring cybersecurity ecosystem in the Middle East: Towards an SME recommender system. *Journal of Cyber Security and Mobility*, 511-536.
3. Albalawi, K. (2025). Opportunities for Cyber Insurance to Address the Challenges of Cyber Attacks: Repercussions for SMEs, University of Sharjah Journal for Law Sciences, *22*(1). https//:doi.org/10.36394/jls.v22.i1.20
4. Alghamdi, S., & Abuabid, A. (2023). IoT Safeguarding in Saudi Tourism Sector: Crafting a Preliminary Security Model for Enhancing Cyber Resilience. *International Journal on Recent and Innovation Trends in Computing and Communication*, *11*(9), 3847-3859.
5. Alghamdi, M., Alomari, S., & Alkatheri, M. (2024). Adopting Government Cyber Security Initiatives-A study of SMEs in Saudi Arabia. *INTERNATIONAL JOURNAL*, *3*(10), 251-319.
6. Alharbi, F. (2025). Twelve Years of Cyber Resilience: Analyzing Cyberattacks in Saudi Arabia (2012-2024). *TEM Journal*, *14*(2).
7. Al-Hawamleh, A. M. (2024). Investigating the multifaceted dynamics of cybersecurity practices and their impact on the quality of e-government services: evidence from the KSA. *Digital Policy, Regulation and Governance*, *26*(3), 317-336.
8. Alhejaili, M. O. M. (2024). SECURING THE KINGDOM'S E-COMMERCE FRONTIER: EVALUATION OF SAUDI ARABIA'S CYBERSECURITY LEGAL FRAMEWORKS. *Journal of Governance and Regulation/Volume. virtusinterpress. Org*

9. . Almoaigel, M. F., & Abuabid, A. (2023). Implementation of Cybersecurity Situation Awareness Model in Saudi SMES. *International Journal of Advanced Computer Science & Applications*, *14*(11).
10. Alorabi, S., & Abuanzeh, R. (2024). The Role of Risk Management in Enhancing Cybersecurity for Small and Medium Enterprises (SMEs) in Saudi Arabia "Applied Study". International Journal of Financial, Administrative and Economic Sciences, London Vol (3), No (10), 2024. https://doi.org/10.59992/IJFAES.2024.v3n10p7
11. Al Oraini, B. (2024). The moderating role of organizational readiness on the blockchain adoption in supply chain among Saudi SMEs. Uncertain Supply Chain Management 12 (2024) 2479–2488. doi: 10.5267/j.uscm.2024.5.021
12. Al-Somali, S. A., Saqr, R. R., Asiri, A. M., & Al-Somali, N. A. (2024). 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*, *16*(5), 1880.
13. Al-Zahrani, A. A., & Al-Salloum, O. I. (2025). Success Factors in Achieving Excellence in Cybersecurity (A Case Study of the Kingdom of Saudi Arabia). *International Journal of Research and Studies Publishing*, *6*(68), 59-87.
14. Asfahani, A. M. (2024). Perceptions of organizational responsibility for cybersecurity in Saudi Arabia: a moderated mediation analysis. *International Journal of Information Security*, *23*(4), 2515-2530.
15. Elmaasrawy, H. E., & Tawfik, O. I. (2025). Impact of the assertive and advisory role of internal auditing on proactive measures to enhance cybersecurity: Evidence from GCC. *Journal of Science and Technology Policy Management*, *16*(1), 68-93.
16. GCC, A. (2024). Forecasting cybersecurity indices for GCC countries: Implications for SMEs. Arabian Journal of Information Security, 5(2), 89–104. https://doi.org/10.1109/AJIS.2024.10234
17. Naqvi, B., Perova, K., Farooq, A., Makhdoom, I., Oyedeji, S., and Porras, J. (2023). Mitigation strategies against the phishing attacks: A systematic literature review. Computers & Security, 132:103387.
18. Patterson, C.M., Nurse, J.R.C., and Franqueira, V. N. L. (2023). Learning from cyber security incidents: A systematic review and future research agenda. Computers & Security, 132:103309.
19. Rawindaran, N., Nawaf, L., Alarifi, S., Alghazzawi, D., Carroll, F., Katib, I., & Hewage, C. (2023). Enhancing cyber security governance and policy for SMEs in industry 5.0: a comparative study between Saudi Arabia and the United Kingdom. *Digital*, *3*(3), 200-231.
20. Renaud, K., & Ophoff, J. (2021). A cyber situational awareness model to predict the implementation of cyber security controls and precautions by SMEs. *Organizational Cybersecurity Journal: Practice, Process and People*, *1*(1), 24-46.
21. Varma, A. J., Taleb, N., Said, R. A., Ghazal, T. M., Ahmad, M., Alzoubi, H. M., & Alshurideh, M. (2023). A roadmap for SMEs to adopt an AI based cyber threat intelligence. In *The effect of information technology on business and marketing intelligence systems* (pp. 1903-1926). Cham: Springer International Publishing.