

Strategic Management and Cybersecurity: A Literature Review on Enhancing Organisational Resilience in the Digital Era for Small to Medium-Sized Businesses

Charles Paul Shurland^{1,2}

¹Distance and Blended Learning Program, Universidad Central de Nicaragua, Managua, Nicaragua

²School of Business Management and Public Administration, Texila American University, Georgetown, Guyana

Correspondence to be addressed: E-mail - cpshurland@gmail.com

Cite this article as: Shurland CP. Strategic management and cybersecurity: A literature review on enhancing organisational resilience in the digital era for small to medium-sized businesses. Texila Int J Acad Res. 2026;13(4).

<https://doi.org/10.21522/TIJAR.2014.13.04.Art019>

Received: 23.08.2026

Accepted: 02.10.2026

Published: 30.10.2026

Article Type: Original Research

Abstract This review examines the theoretical and empirical literature at the intersection of strategic management and cybersecurity, and how organisations can strategically manage cybersecurity to strengthen their resilience in the digital era. The review synthesises eight components of the literature, including the theoretical foundations of strategic management; the role of strategic management in cybersecurity; cybersecurity challenges in the digital era; emerging technologies; cybersecurity incidents and business continuity; leadership and organisational culture; building organisational resilience; and best-practice frameworks. The literature consistently indicates that cyber resilience is not achieved through isolated information technology (IT) controls but through integrated strategic management that connects cyber risk, operational priorities, and business continuity. Gaps remain in the contextual literature on developing economies, where empirical evidence on the relationship between strategic management and cybersecurity remains limited.

Keywords Cybersecurity, Cyber Resilience, Governance, Organisational Resilience, SMEs, Strategic Management.

Introduction

This study examines how organisations can integrate cybersecurity and strategic management to strengthen their resilience in the digital era. It highlights the rapid increase in cybersecurity threats that many organisations face due to advances in digital technology. These threats affect not only its operations but reputation and financial stability. This paper highlights the importance of enhancing organisational resilience against these cyber threats with a focus on how it can be applied to the SMEs in Guyana. The acceleration of this digital transformation has fundamentally changed how organisations operate and deliver value.

Cyber threats have evolved from traditional threats due to the rapid increase in technology and complex digital ecosystems. Consequently, SMEs are shifting from traditional practices of prevention to cyber resilience, emphasizing the ability to anticipate, withstand, recover from, and adapt to cyber disruptions. This evolution highlights the need to integrate cybersecurity into strategic management, to ensure alignment between technological innovation, governance, and business continuity objectives [1].

Objectives

The objective of the study is to investigate cybersecurity and strategic management, how they can be integrated to improve the resilience of businesses in Guyana against cyber threats. The primary objectives of the research are:

1. To investigate the role of strategic management in addressing cybersecurity challenges.
2. To identify strategic approaches and best practices businesses can adopt to enhance cybersecurity resilience.
3. To examine the impact of cybersecurity threats on business performance and resilience.
4. To analyse the benefits and challenges of integrating cybersecurity into strategic management processes.

5. To propose possible recommendations for SMEs to develop and implement cybersecurity strategies.

Research Questions

“How can strategically managing cybersecurity enhance the resilience of businesses in Guyana towards cyber threats in the digital era?”

Justification

The businesses in Guyana are growing exponentially and moving towards the digital era just as the rest of the world, and therefore, the reliance on technology is important. In view of this, businesses are exposed to various types of cyber-attacks, thus the need for this research.

This research highlights valuable insights into the following areas:

How to effectively enhance cybersecurity to protect against growing threats.

How the gap between strategic management and cybersecurity can be bridged to foster coordination across all departments of the business, thus ensuring resilience, sustainability and competitive advantage.

As the Guyana's economy grows, developing businesses will require top-tier digital infrastructure in numerous sectors, and cybersecurity measures must align with the corporate goal to not leave businesses vulnerable or susceptible to cyber threats.

The Government and Corporate leaders in Guyana can find practical implications from this research, which identifies best practices for the integration of the two disciplines. The recommendations will be actionable and can be implemented across sectors in the Country. On the other hand, policymakers with insights to create, amend and propose a relevant regulatory framework, were recommended in the results article on the study of SMEs in Georgetown, Guyana (which is under review).

More importantly, this paper will guide and support directors, shareholders and business

owners on how to anticipate, prepare, respond, and recover from cyberattacks by providing best practices, practical and actionable recommendations, all together building their resilience.

Limitations

There was limited availability of data as the data and empirical evidence were compiled to support the basis of the research, noting its sensitive nature to cybersecurity and management strategies on cyber incidents. The research could not find telling data for SMEs located in Guyana. The depth and breadth of the data collected relating to actual cyber incidents and the effectiveness of the implemented strategies will be affected when tailored to Guyana.

Hypotheses

It is the assumption that integrating strategic management with cybersecurity measures directly influences organisational resilience against digital threats.

As such, there is a significant gap revolving on the integration of the two disciplines in order to build business resilience among SMEs.

Materials and Methods

A mixed method research design was adopted to include a quantitative component to measure patterns, relationships and statistical associations among strategic management practices, cybersecurity integration and organisational resilience. The qualitative component explored the experiences and perceptions of cybersecurity practitioners and national stakeholders.

Inclusion – Exclusion Criteria

The literature reviewed was selected and included if they addressed the relationship between strategic management and cybersecurity, or cybersecurity's contribution to organisational resilience and business continuity. The literature being peer-reviewed or otherwise authoritative was included; and

was relevant to small and medium-sized enterprises (SMEs). The sources that were peer-reviewed journal articles were spread across various International Journal of Business, Economic, Financial Reviews and Information Systems along with conference papers, scholarly textbook, a doctoral dissertation, ISO/IEC 27001:2022, Guyana's Cyber Crime Act 2018 and Data Protection Act 2023, and reputable trade publications. Sources were excluded if not peer-reviewed or unavailable in full text, English, treated cybersecurity purely as a technical function with no strategic dimension, or fell outside the review's thematic scope. These criteria ensured the information was relevant, methodologically sound evidence base and credible.

State of the Art

The current state highlights strategic management and cybersecurity as a vital component for building cyber resilience in business in the digital era while most still view cybersecurity as a technical function only. However, as businesses are facing frequent and complex cyber challenges, this makes cybersecurity a strategic priority rather than a technical function. While digital transformation is rapidly accelerating, cybersecurity maturity still remains an emerging concern. This creates a critical need for businesses in to align cybersecurity with strategic management processes.

Further, several articles/journals reviewed, highlighted relationships with digital transformation, cybersecurity, its framework and strategic management only in SMEs. The study focused a range of articles across various sectors, including financial services, government and public services, manufacturing, healthcare, education and other activities. This provided an appropriate context for examining how organisations that depend on digital technologies manage cybersecurity and organisational resilience.

There is limited research on how the integration of both can enhance organisational resilience especially in Guyana since, as a country, they are way behind on technological advancement. This gap involving the strategic role of cybersecurity in strengthening business resilience against cyber challenges/threats in Guyana, post-pandemic was addressed in the results article on the study of SMEs in Georgetown (under review). The acceleration of digital adoption in Guyana, its oil-driven economic modernisation, and an emerging national cybersecurity governance architecture led by the National Data Management Authority (NDMA), the national Computer Incident Response Team (CIRT.GY), the Data Protection Act 2023 and the Cyber Crime Act 2018 were addressed.

Theoretical Perspective

The study adopts a mixed theoretical perspective, combining positivism and interpretivism, to comprehensively address the research question. The positivist perspective supports the quantitative aspect of the study to examine the measures of strategic management process integrated into cybersecurity to enhance organisational resilience. The following theories included, supports the research variables and hypotheses;

1. Resource-Based View
2. Dynamic Capabilities Theory
3. Risk Management Theory
4. Organisational Resilience Concept
5. Strategic Management Theory

Conceptual Framework: Literature Review

Theoretical Foundation of Strategic Management

Strategic Management's foundation encompasses many fundamental business concepts and involves formulating, implementing, and evaluating strategies to achieve an organisation's vision and mission. Each concept comprises processes,

frameworks, and theories to guide businesses in making decisions aligned with their vision and mission, thereby optimising their competitive advantage. According to the authors [2], strategy competes differently to obtain and maintain a competitive advantage in the respective industry or business sector. They argued that 'Company strategy is the actions managers take to outperform their competitors and achieve superior profitability.

There are several frameworks developed by scholars in the field that help to craft the foundation of Strategic Management. Classical Management Theories, developed by thinkers such as Fredrick Taylor and Henri Fayol, primarily focused on operational efficiency and organisational structure, outlined as fundamental groundwork for future thinkers in the field, and emphasised the importance of planning and control. Industrial Organisation Economics was introduced by Michael Porter, who promoted the concepts of Porter's Five Forces and the Competitive Advantage framework, highlighting the competitive forces shaping an industry and how firms can position themselves strategically to gain a competitive advantage. The Resource-Based View, introduced by Jay Barney and others, focuses primarily on internal resources and capabilities instead of external industry factors, surrounding the firm's unique resources, namely its brand, human capital, technology, and others, to provide a sustainable competitive advantage. Institutional theorists DiMaggio and Powell posited that institutions and societal norms have a role in shaping organisational strategies.

Strategic Management encompasses concepts such as Strategy Formulation, Implementation and Control. Strategy Formulation involves the identification of a firm's mission, vision, and goals, analysing its internal and external environment, and formulating strategies to achieve those goals; SWOT, PESTEL, and scenario planning are used during strategy formulation. Strategy Implementation includes allocating resources

and designing the organisational structure and all processes and systems to support the firm's strategies. Strategic control involves monitoring and adjusting strategies to ensure they remain relevant and practical; strategic control mechanisms help firms stay on course with strategy formulation and adapt to changing circumstances faced by the business.

Moreover, strategic management has evolved in the digital era to address the challenges posed by rapidly advancing technology and the digital landscape. Some contemporary trends include (1) Digital Transformation, where many firms leverage digital technologies to streamline operations, enhance customer experiences, and create new business models, and (2) Cybersecurity Integration, as this research suggests, integrating cybersecurity into strategic management is vital and protecting digital assets and data is essential for businesses in today's interconnected world. Strategic management is a multifaceted field that draws on a rich theoretical foundation; it has continued to evolve by adapting to the challenges and opportunities presented in the digital era. Therefore, this research into the intersection of Strategic Management and Cybersecurity is particularly timely, as businesses must navigate the complex terrain of digital threats while pursuing their strategic goals.

The Role of Strategic Management in Cybersecurity

In this evolving digital era, businesses face an increasing array of cyber threats that can undermine its operations, reputation, and, in some instances, existence. However, for companies to protect their assets effectively, the concept of integrating strategic management into cybersecurity processes emerged. Cybersecurity has become increasingly a concern for many firms worldwide, and Guyana is no exception.

The Role of Strategic Management in Cybersecurity covers two broad spectrums, namely Organisational Cybersecurity and Broader Cybersecurity Policy and Planning. At the Organisational level, companies are faced with cybersecurity risks, and in mitigating these risks, it is prudent to consider risk assessment and management, evaluating possible cyber threats, the company's vulnerabilities to attacks, and how such attacks may impact the company's operations, finances and reputation.

Cybersecurity Challenges in the Digital Era

In this digital era, many organisations worldwide face a plethora of challenges associated with technological integration, lack of or poor management policies, exposure to risks, malware, attacks and vulnerabilities in the Internet of Things (IoT), as well as the human element. Cybersecurity challenges are the risks and constraints that organisations face when protecting digital platforms, data, and operations from evolving cyber threats. Cybersecurity challenges encompass not only the defence against malicious digital attacks but also the management of systemic vulnerabilities arising from rapid digital transformation [3].

Cybersecurity challenges have grown rapidly since organisations rely heavily on digital systems, networks, cloud platforms, and other online technologies. According to Sithole, Odette and Munzhelele [4], many Small and Medium Enterprises (SMEs) adopted digital platforms and tools after COVID-19 but lacked cybersecurity knowledge and were prone to attacks of all kinds. The evolution of technology has led to new variants of cyber threats that leave organisations and individuals vulnerable to financial theft and compromised information, especially personal data that can be used as leverage in the wrong hands. Corporate governance ought to be strategic in tackling cybersecurity, by adopting a realistic framework that takes into consideration its

resources (both financial and human). According to Kumar et al. [5], it was identified that the expansion of digitally enabled infrastructure for small scale organisations was exposed to risks such as legacy-system vulnerabilities, interconnected network failures, and emerging threats like AI-driven or drone-enabled attacks. In a similar article by Sithole et al. [4], SMEs faced threats specific to digital financial platforms, which resulted in mobile money fraud, phishing, ransomware, and insider collusion, where cybersecurity controls were limited. These tell us that cyber challenges exist even in developing countries, which are caused by their technological capabilities and constraints (institutional and resource), therefore it affects organisations' ability to maintain resilience.

It was noted by Kumar et al. [5] that cybersecurity challenges are embedded within socio-technical ecosystems thereby requiring coordinated responses whereas fragmented governance structures and insufficient coordination across agencies weaken the ability to respond to critical cyber incidents. Similarly, Sithole et al. [4] identified the key drivers of cyber challenges in SMEs as insufficient digital knowledge, limited skilled personnel, and weak regulatory enforcement. Consequently, cybersecurity becomes a strategic priority that enhances organisational resilience, ensuring organisations can withstand and recover from challenges in the digital era.

Emerging Technologies and Cybersecurity

The increasing rate of emerging technologies such as artificial intelligence (AI), cloud computing, IoT and interconnected digital systems has significantly intensified organisational cybersecurity risks and challenges. Alnaabi and Al Mahruqi [6] demonstrated that AI is a transformative cybersecurity technology with direct implications for organisational resilience. It highlighted that AI-driven approaches, such as

anomaly detection and predictive analytics, significantly improve the ability to identify and respond to cyber threats in almost real time. However, a strategic management perspective would be the proposed Oman Cybersecurity AI Framework (OCAIF) which emphasised that the effectiveness of these technologies depends on organisational readiness, including the capability of the workforce, infrastructure modernisation, and organisational regulatory alignment. Adopting the AI approach should be managed strategically with long-term resilience goals in mind rather than as a standalone technical upgrade. This reinforces that technological potential alone does not translate into resilience without coordinated strategic execution [6].

According to Agyemang et al. [7], their Cybersecurity Readiness Assessment (CSRA) framework represented an emerging methodological innovation that leveraged evaluation models to inform strategic decision-making. The integration of environmental awareness and organisational capabilities is likely to strategically align with cybersecurity initiatives and organisational risk management. Readiness itself is an enabler of technology resilience, allowing prioritised investments, identifying capability gaps, and implementing continuous improvement cycles. The CSRA framework operationalises resilience as a dynamic capability that evolves through iterative assessment and adaptation rather than static compliance [7].

According to Khresat [8], cybersecurity technologies are linked to the practices of regulatory compliance, which incorporate advanced technical controls and standards. By integrating advanced technologies into compliance regimes, this will enhance resilience by strengthening business continuity mechanisms. Strategic management plays a crucial role in aligning technological adoption with regulatory requirements, ensuring that cybersecurity investments contribute to both compliance and operational stability. This

would enable organisations to leverage those mandated controls as pathways for resilience building, particularly in sectors where regulatory frameworks embed technological standards for risk mitigation and recovery [8].

The study by Albustanji and Paulovics [9] highlighted that emerging cybersecurity capabilities are shaped by advances done at the international level of legal and cooperative infrastructures. This relies on digital technologies to share evidence and increased cross-border coordination. Organisational resilience is contingent on the availability of such mechanisms, especially when it involves cyber threats of any kind. There must be inclusion of strategic management to align with internal technological adoption to include engagement with external legal and institutional ecosystems to build resilience. The article suggested adopting frameworks such as the Budapest Convention since it reflects on the growing importance of technologically enabled cooperation (e.g., rapid information exchange systems) in enhancing resilience. This reinforces the view that with emerging technologies in cybersecurity, resilience can be amplified by broader governance structures [9]. Emerging technologies in cybersecurity contribute to organisational cyber resilience however, through strategic management and not in isolation. By employing a strategic perspective, cyber resilience will enable how effective organisations can align their technological capabilities with proper governance, effective resource allocation, and external collaboration.

Cybersecurity Incident and Business Continuity

Strategic management decisions play a crucial role in strengthening cyber resilience to ensure business continuity. Writers von Solms and Upton [10] proposed that resilience is not just a technical function, but is dependent on organisational governance and policies, which should align with modern frameworks such as

the NIST Cybersecurity Framework (CSF) 2.0 [10]. The National Institute of Standards and Technology provides voluntary guidelines that organisations can adopt to improve their management of cybersecurity. NIST CSF 2.0 provides a structured approach to identifying, protecting, detecting, responding to and recovering from cyber threats. NIST CSF's recent addition of the 'Govern' function in 2.0 speaks to the said aligned executive strategy with cybersecurity resilience rather than an IT issue.

Cyber resilience depends on strategic governance that is woven into its policy, skills, technology, culture and its people [10]. With this approach, organisations especially SMEs will be better equipped to handle cyber threats/challenges given our technological advancement, with little to no loss of company data. The framework serves as decision support tool to guide organisations systematically to enhance their cyber resilience.

It is important to note that strategic design choices directly influence operational resilience. The 'Westport (WPRT) Cybersecurity Breach' case [11] highlighted that due to the network segmentation of Information Technology systems and manufacturing environments, it limited the operational impact of the cyber incident, causing uninterrupted production. This proved that strategic alignment to redundancy and segmentation eliminated single points of failure and maintained service availability during disruptions [11]. Similarly, geographically distributed data replication confirmed that cyber strategic infrastructure is rooted in long-term managerial planning aimed at ensuring business continuity especially under adverse conditions [12]. These examples contribute to the phenomenon of proper strategic management decisions translated into a cyber resilience system to protect core business functions. By segregating systems (IT versus manufacturing), this will limit cyber-attacks/threats from spreading therefore, a

allowing operations continuity. The NIST CSF provides detailed guidelines on how to manage the segmentation by separating critical operational systems. It also depicts how to deal with cyber breaches in progress, not only prevention.

A conference report from the 2005 Storage Networking World conference featured IT executives who were in discussions about challenges in managing, securing, and recovering hundreds of terabytes to petabytes of data. Ralph Barber, CIO of Holland & Knight, describes replicating data between two data centres (Tampa and Denver) for disaster recovery, and the business impact when Hurricane Wilma knocked out branch offices. This resulted in lost data and no means of generating income from the loss of the clients' information. There should have been primary and secondary core theme backups and replication of data kept offsite at another location for business continuity. This indicated that many organisations still struggle with a gap between cybersecurity priorities and strategic business objectives which weakens its resilience and increases operational exposure.

Conversely, organisations that adopt risk-based approaches and cyber strategies aligned to strategic management can prioritize vital assets while minimizing disruption to revenue generating operations. This supports the argument that resilience is not achieved through isolated IT controls but through integrated strategic management that connects cyber risk, operational priorities, and building business continuity. There should be consistent emphasis placed on resilience-focused strategic management than prevention to maintain continued operations despite inevitable cyber incidents/attacks. Cyber resilience in the digital era is having the ability to anticipate, withstand and recover from disruptions, rather than simply prevention. Therefore, correlation exists between strategic management decisions and business continuity with the alignment of governance and risk management practices,

enabling operations to flow with normalcy even in the face of evolving cyber threats. This will ensure fast recovery and less downtime, which ultimately results in little to no financial loss.

Leadership and Organisational Culture

In the digital era, cyber resilience is not only technical acquisition, but also a cultural acquisition of the organisation. In the research studies submitted by Grant [13], information security awareness and training (ISAT) programs were seen as a low priority in the defence sector, as social engineering and employee negligence rose. The research found that organisational culture is a structural driver of whether security programs are taken seriously, resourced, effectively implemented. It also highlighted that people are the 'weakest link,' but cultural conditions often prevent the said training that could strengthen them. The author Grant in his article demonstrated that resilience could not be achieved by standard security awareness because of the cultural diversity, which ought to be addressed first. When there is a mismatch with the prevailing culture, then it will be deprioritized, under-resourced, and ignored. It is important to diagnose the culture type in order to prevent mismatch.

Andronache [14] framework on organisational culture was that resilience was not only built from non-episodic awareness but from an embedded culture. He rallied that around the notion of prescribing a periodic training check box to cultivating an embedded security mindset. In the digital era, threats are continuous and ever changing, thus an annual training module cannot generate resilience. Research data shows that cybersecurity governance, its people, and resources account for the bulk of cultural effectiveness. Resilience can only be embedded when security is woven into our daily norms, assumptions, and decisions. The digital era amplifies both speed of threats and cost of human error. As such, technological defences while necessary are

insufficient to cyber resilience. Cybersecurity should be structurally integrated into the culture in the norms, daily operations, hypothetical scenarios, and in our daily behaviour, not just in the policy document on the intranet.

Building Organisational Resilience

Organisational resilience is the ability to anticipate, respond and recover from disruptions while preserving its fundamental purpose and values [15]. This refers to the organisation's capacity to respond to crises and adapt to change. Resilience builds strength especially during unexpected technological disruptions (cyber attacks) but can continue to operate effectively while improving from the situation. This capability is essential in today's complex and uncertain business environment, as it enables organisations to remain sustainable over the long term.

An article on cybersecurity capabilities by Malatji et al. [16] highlighted how critical infrastructure cybersecurity capability frameworks are developed to function with five NIST framework components, which include Identify, Protect, Detect, Respond and Recover. These five functions should be included in the organisation's risk management and corporate governance. It is vital to include cybersecurity resilience in corporate governance because of an organisation's heavy reliance on digital technology. Therefore, put provisions in place to build resilience, ensuring that organisations are better prepared for a cyber attack/threat system failure, reducing downtime, loss of company data, and ultimately any financial loss.

According to research studies [17], building organisational cyber resilience requires sharing information (external) in conjunction with the organisation's readiness (internal) to act on that information captured in a synergy dependency (Network Flattening, Alert Paralysis, Operational Coupling, and Relational Weaponization), which refers to how external governance effectiveness is contingent on

internal controls. While this theory reinforces cross-boundary governance to counter the escalation of cyberattacks, the need for governance is identified as essential to cyber resilience. It adds to the fact that building resilience is not just an IT function but an organisational function to ensure business continuity. Similarly, a recent study conducted by the Design Science Research [7] highlighted a two-tier assessment framework that evaluated the external cybersecurity environment, including its regulation, national strategy and institutional support, in conjunction with an organisation's internal readiness across governance, technical controls, awareness and culture. Again, this study reemphasizes that resilience is built on cybersecurity integrated into corporate governance through external capabilities.

However, a study was conducted on the digital paradox in China's construction sector [17], highlighting that heavy digital investment often fails due to organisational resilience. The study argued that while digital investment improves the performance of an organisation, it is also important to strengthen its ability to withstand and recover from disruptions. The study found that organisational resilience is built on three capacities; an organisation's intelligence, connectivity and analytics proving, connectivity to be the largest. This is a long-term effect that increases organisations' performance, its capacity for robustness, data-driven risk prediction for agility, and strategic alignment for integrity [17]. While this study specifically speaks to organisational resilience, it is imperative to ensure that organisations are in a state of strength digitally in order to withstand cyber-attacks and it starts with proper strategic decisions aligned with cyber resilience. To build organisational resilience it is prudent to have the right cybersecurity capabilities in place, and to ensure the capabilities are operational while taking note of their readiness. These elements contribute to a

better organisational performance while leveraging resilience in the digital era.

Cybersecurity Best Practices Framework

Adopting a best practice cybersecurity framework will help organisations achieve the best outcomes in protecting systems, data/information, and networks from cyberattacks/threats by utilising proven methods and managing their risks. The best-practice framework tells organisations how to stay secure and how to align their security measures in a consistent manner to ensure resilience. There are several research studies with a number of best practices highlighting the following frameworks: Artificial Neural Network Interpretive Structural Modelling Framework (ANN-ISM); National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF); Critical Infrastructure Capability Framework; MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK); Cyber Kill Chain; Zero Trust Architecture (ZTA); European Cybersecurity Skills Framework (ECSF); NIST + ATT&CK + Cyber Kill Chain [18]; and ISO/IEC 27001.

The NIST CSF provides guidelines that organisations can adopt to improve their cybersecurity management. NIST CSF 2.0 presents a structured approach to detect, identify, respond to, recover from and protect against cyber threats. ISO/IEC 27001 is an internationally recognized standard focused on the creation, maintenance, and continual improvement of an Information Security Management System (ISMS). ISO/IEC 27001 is an information security management standard that provides organisations with a structured framework to safeguard their information assets and ISMS, covering risk assessment, risk management and continuous improvement [19].

Results: Existent Gaps in the Literature

The findings revealed from the literature indicated that cybersecurity is a function that is managed in isolation. The related papers reviewed on cybersecurity's readiness assessment frameworks [7] identified gaps such as limited readiness interpretability, maturity models with weak contextualisation, and awareness measurement isolated from governance [7].

In addition, this hypothesis is untested and therefore, the literature relative to its specificity is limited and/or non-existent. While the literature on resource-based view is estimated, the empirical data is not validated in the context of cybersecurity. This is a significant gap between the theoretical and practical integration of strategic management with cybersecurity in SMEs. Most literature addresses either one or the other. However, the objective is to bridge this gap through the information gathered from the small to medium enterprises targeted in the urban area of Guyana; Georgetown and demonstrate how the alignment between these two domains enhances resilience.

In addition, SMEs were forced to move their operations to a digital platform during and post-COVID and lacked the cybersecurity knowledge to match. As a result, this highlights a practical gap that was addressed in the results article on a study of SMEs in Georgetown, Guyana on how to enhance cyber resilience (under review).

Discussion

A consistent finding across the eight strands of literature is that the possibility of cyber resilience is through strategic management rather than technical controls alone [10]. The theoretical strand shows the field arriving at this position through a natural extension of its foundations, where classical and industrial organisation theories emphasized its positioning and planning, the Resource-Based

View directs attention to governance, internal capabilities, culture and readiness that determine whether technology investments translate into resilience [2, 17].

Evidence on cyber challenges reinforces this as well, as the threats confronting developing-economy SMEs are socio-technical rather than purely technical. Kumar et al. [5] found that challenges are embedded within socio-technical ecosystems which require coordinated, tested responses, whilst Sithole et al. [4] identified insufficient digital knowledge, limited skilled personnel and weak regulatory enforcement as key drivers in SMEs that digitised rapidly after COVID-19. This places cybersecurity in a strategic emergency as fragmented governance and under-resourced institutions cannot be fixed only at the IT level.

The emerging technology and framework strands carry the review's vital focus, technological potential does not become resilience without strategic execution. Alnaabi and Al Mahruqi [6] demonstrated that AI-driven approaches improve threat detection in near real time, yet their effectiveness depends on organisational readiness, regulatory alignment, and workforce capability. This was a condition formalised by Agyemang et al. [7], whose Cybersecurity Readiness Assessment framework operationalises resilience as a dynamic capability rather than compliance. The incident evidence points the same in both directions, the Westport (WPRT) breach showed that strategic design choices such as network segmentation preserved operations during an active attack [11], whereas the Hurricane Wilma data-loss episode depicted the gap between cybersecurity priorities and business objectives, which converted disruption into business failure [12].

Leadership and culture emerge as the binding constraints and Grant [13] found that information security awareness and training programmes were deprioritised and under-resourced where organisational culture was mismatched. On the other hand, Andronache

[14] argues that annual, check the box training cannot generate resilience against those continuously evolving threats; as security must be integrated into daily norms and decisions. Malatji et al. [16] similarly situated the five NIST functions within corporate governance and risk management, and Zhang et al.'s evidence of a digital paradox, in which heavy investment fails without organisational capacities on intelligence, connectivity and analytics, confirms that investment without strategic integration is wasted.

These findings are coherent but small in context, since the reviewed studies address Oman, Uganda, Jordan, India and China, and empirical evidence on strategic management and cybersecurity in developing economies, and in the Caribbean in particular, remains limited. The research addressed this gap. The small to medium-sized businesses in Georgetown, Guyana, operate within an emerging regulatory environment including the Cyber Crime Act 2018 and the Data Protection Act 2023 [20, 21]. The literature predicts that resilience will track the quality of strategic integration rather than the volume of technology, a proposition the empirical phase of the study tested.

Conclusion

Strategic management is a complex field that draws on a rich theoretical foundation and continues to evolve by adapting to its challenges and opportunities presented in this digital era. Across all eight strands of literature, the consistent position is that cyber resilience depends on strategic governance integrated into policy, skills, technology, culture and people, and not simply on information technology function. Therefore, integrating strategic management with cybersecurity, is essential to build organisational resilience especially when cybersecurity is aligned with strategic planning. This can strengthen businesses' capacity to prepare for, respond to and recover from

cyberattacks while maintaining its business continuity, reputation and financial stability.

Conflict of Interest

The author declares no conflict of interest.

Ethical Approval

This study forms part of a doctoral research programme conducted in accordance with the ethical standards of Universidad Central de Nicaragua and Texila American University. The manuscript is a review of published literature, therefore no primary data involving human participants were included and all sources are publicly available and duly acknowledged.

Data Availability

This manuscript reviewed published literature; of which no new datasets were

generated. All data supporting the findings were drawn from the published sources cited in the reference list, which are publicly available.

Author Contributions

Charles Paul Shurland is the sole author responsible for the conceptualization, literature search, synthesis, scribing and review of the manuscript.

Funding

The author funded this research.

Acknowledgements

Sincere gratitude is extended to family, Dr. Narayanasamy Siddaiyan Santhi, the Research Committee, members of Thesis Guidelines Formulation Committee and the research scholars who graciously assisted with the completion of this research.

References

- [1]. Dal Cin P. State of cybersecurity resilience 2025. Accenture; 2025. Available from: <https://www.accenture.com/en/insights/security/state-of-cybersecurity-2025>
- [2]. Thompson A, Peteraf M, Gamble J, Strickland AJ III. Crafting and executing strategy: The quest for competitive advantage. New York: McGraw Hill Education; 2016.
- [3]. European Union Agency for Cybersecurity. ENISA threat landscape 2021. 2021. Available from: <https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202021.pdf>
- [4]. Sithole M, Odette S, Munzhelele F. Cybersecurity challenges and a conceptualised maturity typology in Ugandan SMEs: A qualitative analysis. *Int J Bus Ecosyst Strateg*. 2026;8:105-19.
- [5]. Kumar S, Gangwar SP, Singh N, Pagaria R, Garg A, Das S. Securing the skies: Innovating cybersecurity governance for India's emerging small airports. *Eur Conf Cyber Warf Secur*. 2025;24:318-27.
- [6]. Alnaabi AAH, Al Mahruqi AAH. Artificial intelligence methods for enhancing cybersecurity in Oman: A comprehensive review. *J Cloud Comput*. 2026;15.
- [7]. Agyemang R, Furnell S, Muller T. A context-aware cybersecurity readiness assessment framework for organisations in developing and emerging environments. *Future Internet*. 2026;18:178.
- [8]. Khresat O. Compliance with regulatory, legislative and contractual requirements for cyber security and its impact on the continuity of the Jordanian banking sector. *Asian Econ Financ Rev*. 2025;15:1592-603.
- [9]. Albustanji H, Paulovics A. A critical review of the Jordanian legal frameworks on international cooperation in combating cybercrime. *AAU J Bus Law*. 2026;10.
- [10]. von Solms B, Upton D. Cyber security capacity governance. *Bus Manag Rev*. 2016;7(4):35-9.
- [11]. GuruFocus. Westport (WPRT) faces cybersecurity breach but ensures business continuity. *Newstex Finance Account Blogs*. 2026 Mar 20.
- [12]. Mearian L. Data security key to business continuity. *CIO Canada*. 2005;13(12).

- [13]. Grant RL. Exploring effects of organizational culture upon implementation of information security awareness and training programs within the defense industry located in the Tennessee Valley region [doctoral dissertation]. Melbourne (FL): Florida Institute of Technology; 2017.
- [14]. Andronache A. Increasing security awareness through lenses of cybersecurity culture. *J Inf Syst Oper Manag.* 2021;15:1-16.
- [15]. BCM Institute. What is organizational resilience? BCM Institute Blog. 2023 May 17. Available from: <https://bcm-institute.org>
- [16]. Malatji M, Marnewick AL, Von Solms S. Cybersecurity capabilities for critical infrastructure resilience. *Inf Comput Secur.* 2021;30:255-79.
- [17]. Zhang X, Ba X, Li B. Cyberattacks in supply chains: A multi-case study. *PLoS One.* 2026;21:e0350010.
- [18]. Ramage X, Lebea K, Sithungu S. Cyber warfare and critical infrastructure. *Eur Conf Cyber Warf Secur.* 2025;24:566-75.
- [19]. International Organization for Standardization. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection: Information security management systems: Requirements. Geneva: ISO; 2022. Available from: <https://www.iso.org/standard/27001.html>
- [20]. Parliament of Guyana. Cyber Crime Act 2018 (Act No. 16 of 2018). 2018. Available from: <https://www.parliament.gov.gy/publications/acts-of-parliament/cyber-crime-act-2018>
- [21]. Parliament of Guyana. Data Protection Act 2023 (Act No. 18 of 2023). 2023. Available from: <https://www.parliament.gov.gy/publications/acts-of-parliament/dataprotectionact18of2023>