Cyber Resilience Capabilities and their Impact on Small and Medium-Sized Enterprise Business Continuity in Emerging Economies

Destiny Young[1]*, Osinachi Ozocheta[2]

[1]Oil and Gas Free Zones Authority, Onne, Rivers State, Nigeria

[2]Stowe School Buckingham, United Kingdom

***Corresponding Author**

DOI: https://doi.org/10.51584/IJRIAS.2025.101100129

Received: 08 December 2025; Accepted: 15 December 2025; Published: 25 December 2025

ABSTRACT

Small and Medium sized Enterprises, SMEs, represent the vital economic backbone of emerging economies, yet they contend with an increasingly asymmetric threat environment characterised by sophisticated cyberattacks and severe resource scarcity (Sultan, 2025; Hadap et al., 2025). This paper provides an empirical investigation into the necessary link between robust Cyber Resilience, CR, capabilities and the effective achievement of Business Continuity, BC, in these resource constrained settings. By synthesising existing empirical data on the quantifiable economic and operational risks of cyber incidents, this study asserts that traditional, reactive BC planning is insufficient, robust proactive CR is an indispensable prerequisite for sustainable operational survival (Splunk, 2025; Everbridge, 2025; Sultan, 2025). Findings indicate that successful breaches impose substantial financial losses, averaging $30,000 USD for sampled SMEs post breach, alongside significant operational downtime, evidenced by a mean system disruption of 12.5 hours (Sonkar et al., 2025). This level of disruption is linked to an estimated 60 per cent business failure rate among unprepared small businesses following a major cyber attack (Sonkar et al., 2025). The paper details strategic, cost-effective interventions including risk-based governance, high return on investment employee training, and the leveraging of scalable open-source security stacks, all of which offer a pragmatic pathway for SMEs to enhance their defences and secure long-term viability in the digital economy (Ejaz & Matthew, 2024; Ilca et al., 2023).

Keywords: Cybersecurity, SMEs, Economic Impact, Financial Loss, Business Continuity, Cyber Resilience, Emerging Economies.

INTRODUCTION

Small and Medium sized Enterprises, SMEs, are globally acknowledged as critical engines of economic stability and development, constituting approximately 90 per cent of businesses worldwide and serving as the foundational source of employment and value creation in emerging economies (Sultan, 2025; WEF, 2024; Ejaz & Matthew, 2024). Despite their pivotal socioeconomic function, these enterprises routinely face sophisticated, asymmetrical cyber threats equivalent to those targeting large corporations (Sultan, 2025). This exposure renders them the "overlooked soft underbelly" of the global digital infrastructure, primarily because they lack the comparable financial and technical resources essential for robust defence (Sultan, 2025; Ejaz & Matthew, 2024; Cook, 2017).

This disproportionate vulnerability is exacerbated in emerging markets where structural impediments abound. These challenges include severe budget limitations, a pervasive deficit in specialised cybersecurity skills (Vergara Cobos, 2024), and infrastructural weaknesses that lag behind rapid digitalisation rates (World Bank, 2024). This environment amplifies threat exposure, dictating a mandatory strategic shift away from outdated, reactive crisis management towards proactive, adaptive security (Sultan, 2025). The economic ramifications of failed security are profound, with estimates confirming that nearly two thirds of small businesses fail following a major attack (Sonkar et al., 2025).

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue XI November 2025

This research posits that investing in comprehensive **Cyber Resilience, CR,** capabilities is not an optional operational expense, but a fundamental economic necessity for safeguarding **Business Continuity, BC,** and ensuring long term solvency in the modern digital age. This paper rigorously addresses this strategic imperative by first delineating the key differences between the BC and CR paradigms, second, empirically quantifying the catastrophic operational and financial damages suffered by vulnerable SMEs and third, detailing pragmatic, cost effective solutions designed to close the cyber preparedness gap in resource constrained settings.

LITERATURE REVIEW

The Conceptual Dichotomy: Business Continuity and Cyber Resilience

Effective strategic investment in security requires a precise conceptualisation of the terms Business Continuity, BC, and Cyber Resilience, CR, as they possess distinct underlying philosophies (Splunk, 2025; Everbridge, 2025). Resource constrained SMEs, in particular, must understand this difference to allocate their finite capital efficiently (Sultan, 2025).

Business Continuity, BC. Traditional BC planning is fundamentally **reactive and event driven** (Everbridge, 2025). Its core purpose is maintaining or restoring critical operations to an acceptable minimum standard during or immediately following a specific, identifiable disruption, such as a fire, natural disaster or defined cyber incident (Splunk, 2025; Everbridge, 2025). BC planning is centred on establishing clear recovery objectives, setting backup procedures and developing formal incident response plans (Splunk, 2025; Everbridge, 2025). The planning and restoration efforts rely on key metrics including the **Recovery Time Objective, RTO,** which defines the maximum acceptable downtime and the **Recovery Point Objective, RPO,** which sets the maximum tolerable data loss (Liuzzo & Bovey, 2025; Kuehm, 2025; Everbridge, 2025). The ultimate measure of BC success is the swift restoration of services back to the baseline operational state (Everbridge, 2025).

Cyber Resilience, CR. In contrast, CR is **continuous, proactive, and strategic** (Splunk, 2025; Everbridge, 2025). CR represents the broader organisational capability to adapt, evolve and effectively prepare for uncertainty, extending beyond mere recovery to anticipate non acute challenges such as sustained threat campaigns or economic downturns (Splunk, 2025; Everbridge, 2025). CR embodies the capacity of an organisation to **absorb the effects of and adapt to a changing environment** (Everbridge, 2025). Resilience capabilities, including flexible systems, continuous threat detection and an adaptive culture, are integrated into continuous operational processes rather than being activated only during a crisis (Splunk, 2025; Everbridge, 2025). CR aims at optimising performance *through* disruption, allowing the entity to respond dynamically to unforeseen challenges (Splunk, 2025).

The Key Differences Between Business Continuity (BC) and Cyber Resilience (CR)

Feature / Dimension	Business Continuity (BC)	Cyber Resilience (CR)
Core Concept	**Event-Driven Recovery:** BC is a defined set of planning protocols designed to restore operations *after* a disruptive event has occurred. It is a "plan B" for when normal operations fail.	**Continuous Adaptation:** CR is an organizational state of being designed to absorb the shock of disruption and adapt operations *during* the event. It is inherent to the system's architecture.
Primary Focus	**Survival and Restoration:** The focus is on survival; ensuring the company does not permanently fail and returning the organization to a pre-defined "business as usual" baseline state as quickly as possible.	**Endurance and Optimisation:** The focus is on absorbing stress while maintaining critical functionality. It aims not just to survive the disruption, but to optimize performance and evolve defenses while under duress.
Activation Trigger	**Reactive / Episodic:** BC plans are typically dormant until triggered by a specific, declared disaster event or outage (e.g., a hurricane, a data center fire, a total ransomware lockdown).	**Proactive / Continuous:** CR is "always on." It assumes that threats and disruptions are constant and inevitable states, requiring ongoing monitoring, defense, and adaptation rather than a single trigger point.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue XI November 2025

Operational Goal	**Minimum Service Levels:** The goal is to achieve minimum acceptable operational levels (often defined by Recovery Time Objectives - RTOs) to keep critical parts of the business functioning until full recovery.	**Optimizing Performance Through Disruption:** The goal is to deliver sustained business outcomes throughout an adverse event, minimizing the impact to the customer and potentially emerging from the disruption in a stronger position.
Scope of Threats	**Broad Spectrum (Physical & Digital):** Historically focused heavily on physical disasters (weather, fire, hardware failure), though now includes high-impact cyber events that stop operations entirely.	**Cyber-Centric & Complex:** Laser-focused on the dynamic, complex, and persistent nature of modern cyber threats, data breaches, and sophisticated attacks that degrade rather than stop operations.
Mindset	**"Bounce Back":** Return to the status quo.	**"Bounce Forward":** Learn, adapt, and improve from the stressor.

Table 1: Key Differences Between Business Continuity and Cyber Resilience

The Convergence of CR and BC

The contemporary cyber threat landscape, characterised by highly adaptive and persistent attacks that often leverage artificial intelligence, AI, renders singular, reactive BC plans insufficient (Sultan, 2025). Without a strategic foundation of CR, conventional BC plans quickly become obsolete and ineffective (Sultan, 2025; Splunk, 2025). CR provides the necessary adaptive infrastructure, including the continuous ability to proactively detect new malware families and internal threats, implement threat intelligence sharing and maintain network protection, all of which are essential preconditions for successful and manageable BC restoration phases (Ilca et al., 2023; Sultan, 2025). Investing in CR directly reduces the frequency and severity of successful intrusions, a key factor that drastically lowers the Total Cost of Ownership, TCO, for business continuity by minimising the necessity of frequent and costly full scale recovery efforts (Sultan, 2025).

SME Vulnerability in Emerging Economies: An Asymmetric Threat

SMEs face an asymmetric threat that is structurally amplified in emerging markets by endemic resource constraints and a pervasive lack of expertise (Ejaz & Matthew, 2024; Sonkar et al., 2025). Globally, SMEs are frequently targeted by cyber criminals because they maintain comparably weaker security defences and possess lower awareness levels (Hadap et al., 2025). Research indicates that a large proportion of SMEs allocate less than 5 to 10 per cent of their total IT budget towards security initiatives, reflecting a foundational governance and investment deficit (Ejaz & Matthew, 2024; Sonkar et al., 2025).

This vulnerability is compounded by the structural difficulty in securing specialist talent. The global shortfall of cybersecurity workers, estimated at four million unfilled positions (ISC2, 2023), is acutely felt in developing nations (Vergara Cobos, 2024). This severe talent deficit restricts the capacity of SMEs to hire the requisite expertise necessary to manage advanced defences internally (Ejaz & Matthew, 2024). Furthermore, SMEs increasingly serve as lucrative indirect targets, exploited as the weakest link in larger global supply chains to access more valuable targets within critical infrastructure or regulated industries (Sultan, 2025). This means that a small enterprise integrated into critical systems immediately faces exponential growth in its cyber risk profile (Sultan, 2025).

The Socioeconomic and Regulatory Context of Risk

The susceptibility of SMEs is not purely technical, it is intrinsically linked to broader socioeconomic and political factors prevalent in emerging markets (Vergara Cobos, 2024; Chen et al., 2023).

1. **Macroeconomic Vulnerability:** Research suggests that high levels of political stability and control over corruption correlate with fewer disclosed cyber incidents (Vergara Cobos, 2024). Consequently, environments experiencing political or economic instability face higher exposure to cybercrime, which is often motivated by socioeconomic struggles such as unemployment and the incentive for illegal financial gains (Chen et al., 2023). This threat is particularly acute in developing nations where rapid

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue XI November 2025

digitalisation means a growing number of highly educated yet potentially underemployed computer experts are emerging, increasing the risk of politically or financially motivated cybercrime (Vergara Cobos, 2024).

2. **Regulatory Deficiencies:** The effectiveness of national cyber resilience is significantly hampered by inadequate and inconsistent legal and regulatory enforcement in many emerging markets (Liquid Intelligent Technologies, 2021). The lack of stringent, overarching cybersecurity laws and regulations in many African countries, for example, inadvertently creates an environment conducive to cybercriminals (Liquid Intelligent Technologies, 2021). Regulatory fragmentation, specifically conflicting mandates such as data localisation requirements observed in regions like Southeast Asia, imposes high compliance costs on regional SMEs. These non essential burdens divert scarce capital and IT capacity away from core investments in adaptive CR, thereby weakening the overall security posture (Gatdula, 2025; Sultan, 2025).

The confluence of resource constraints, talent deficits, and structural governance weaknesses mandates a focused research agenda on implementable solutions that empower SMEs to build foundational cyber resilience.

RESEARCH METHODOLOGY

The findings presented in this paper are the result of a rigorous synthesis of empirical research predominantly employing a **mixed methods research design** to assess the financial, economic and operational impacts of cybersecurity breaches and computer fraud on SMEs (Sonkar et al., 2025; Hadap et al., 2025; Ejaz & Matthew, 2024).

Data Collection and Approach

The core quantitative findings draw from studies that collected primary data through structured surveys and analysis of the financial records of sampled SMEs across diverse sectors (Sonkar et al., 2025; Hadap et al., 2025) which are predominantly focused on the economic context of India (Sonkar et al., 2025; Hadap et al., 2025). The research further incorporated qualitative insights gathered via in depth interviews with SME owners, IT managers, and cybersecurity experts, providing a detailed contextual understanding of practical challenges and strategies regarding cost constraints and risk prioritisation (Sonkar et al., 2025; Hadap et al., 2025; Ejaz & Matthew, 2024).

The research specifically addresses a significant gap in extant literature where SMEs are often neglected in favour of studying large organisations with extensive IT departments and greater available resources (Sonkar et al., 2025). The quantitative portions employed advanced statistical techniques:

- **Correlation Analysis:** Used to ascertain the relationship between cybersecurity preparedness, measured via a structured score, and the financial resilience of the enterprises (Sonkar et al., 2025).

- **Regression Modelling:** Multiple linear regression was performed to evaluate the efficacy of cybersecurity policies and strategies in strengthening SME resilience, quantifying the variance explained by predictors such as policy adoption, training frequency, incident response mechanisms and financial investment (Hadap et al., 2025).

- **Advanced Analytical Tools:** Machine learning methods, including Artificial Neural Networks, ANNs, were utilised for prediction and simulation of complex outcomes, demonstrating the suitability of high resilience mathematical solutions in situations where survey response rates are traditionally low (Sonkar et al., 2025).

This methodological triangulation of quantifiable economic damage, operational metrics and contextual strategic decision making ensures the robust nature of the conclusions and the relevance of the actionable recommendations (Ejaz & Matthew, 2024; Sonkar et al., 2025).

Data Presentation and Analysis

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue XI November 2025

Empirical evidence consistently demonstrates that deficient cyber resilience leads to quantifiable, severe negative financial and operational outcomes, thereby validating the research hypothesis concerning the positive relationship between preparedness and resilience (Sonkar et al., 2025).

Descriptive Statistics of Cyber Incident Impact on Sampled SMEs

Variable	Mean	Median	Standard Deviation	Minimum	Maximum
Cybersecurity Preparedness Score	75.4	Not reported	Not reported	Not reported	Not reported
Financial Resilience Index	82.6	Not reported	Not reported	Not reported	Not reported
Downtime Due to Breaches, hours	12.5	10.0	Not reported	Not reported	40.0
Financial Loss Due to Breaches, Rs.	25,00,000	Not reported	15,00,000	50,000	75,00,000

Table 2: Descriptive Statistics of Cyber Incident Impact on Sampled SMEs (Mean financial loss and downtime figures are taken from Sonkar et al. (2025).

Quantified Economic and Operational Losses

Analysis of sampled SMEs following cyber incidents reveals a substantial and immediate burden of cost (Sonkar et al., 2025):

1. **Direct Financial Loss:** The mean Financial Loss Due to Breaches was reported at **Rs. 25,00,000** (Twenty-five Lakh Rupees), with the recorded losses ranging dramatically from a minimum of Rs. 50,000 to a maximum of Rs. 75,00,000 (Sonkar et al., 2025). The substantial variability in these losses, evidenced by a large standard deviation of Rs. 15,00,000, highlights the potential for unpredictable and catastrophic financial impacts on the enterprise (Sonkar et al., 2025).

2. **Operational Downtime:** Operational disruption, measured as the loss of system availability, averaged **12.5 hours**, with a median of 10.0 hours (Sonkar et al., 2025). This duration of downtime, which extended up to 40 hours in extreme cases, directly signals inadequate incident response capabilities and severe operational failure (Sonkar et al., 2025).

The Link Between Preparedness and Resilience

The long-term consequences of failing to implement CR measures are severe, with an estimated **60 per cent of small businesses shutting down** within the first six months after a major cyber attack (Sonkar et al., 2025). However, proactive strategic measures are demonstrably effective:

- **Correlation Findings:** Correlation analysis demonstrated a **moderately positive and statistically significant relationship** between Cybersecurity Preparedness and Financial Resilience, with a Pearson correlation coefficient of **0.634** (Sonkar et al., 2025). The associated p value of 0.000, significantly below the 0.05 threshold, confirms that this association is not coincidental. It provides abundant evidence that enhanced cybersecurity preparedness is linked to greater financial resilience against breaches (Sonkar et al., 2025).

Correlation Analysis Between Cybersecurity Preparedness and Financial Resilience

Variables	Cybersecurity Preparedness	Financial Resilience

Cybersecurity Preparedness	1.000	0.634**
Financial Resilience	0.634**	1.000

Table 3: Correlation Analysis Between Cybersecurity Preparedness and Financial Resilience (Source: Sonkar et al. (2025).

*Note. Values are Pearson correlation coefficients. The significance value for the correlation between Cybersecurity Preparedness and Financial Resilience is 0.000.

$p < 0.01$.

Policy Efficacy: Multiple linear regression analysis confirmed that cybersecurity factors collectively explain **72.9 per cent** of the variance in SMEs' resilience scores (Hadap et al., 2025). All predictor variables, including policy adoption, financial investment and training frequency, were found to positively and significantly affect resilience (Hadap et al., 2025). Crucially, the **Incident Response Mechanism** emerged as the strongest predictor of resilience (B = 0.415, $p < 0.001$), underscoring the vital importance of having documented procedures to swiftly manage and mitigate incidents (Hadap et al., 2025).

The following sample table presents the results of a multiple linear regression analysis conducted to assess the predictive power of various cybersecurity measures on the resilience score of Small and Medium sized Enterprises, SMEs. The analysis confirms that the dependent variable, SMEs' Resilience Against Cyber Threats, is significantly predicted by the included independent variables, collectively explaining **72.9 per cent** of the variance in resilience.

The statistical outputs confirm the model's strength and significance, suggesting that investments in structured cybersecurity frameworks lead to enhanced resilience.

Predictor Variables	Unstandardised Coefficients (B)	Standardised Coefficients (Beta)	t Value	p Value
Incident Response Mechanisms	**0.415**	0.398	5.214	0.000***
Cybersecurity Policy Adoption	0.325	0.312	4.112	0.000***
Frequency of Cybersecurity Training	0.278	0.289	3.765	0.001***
Financial Investment in Cybersecurity	0.210	0.198	2.965	0.004**
Constant (Intercept)	1.152		6.732	0.000***

Table 4: Multiple Linear Regression Results: Predictors of SME Resilience (Hadap et al., 2025)

Model Summary	Value
R^2	**0.729**
F statistic	48.215
p Value (Model Significance)	0.000***

*Note: ***p<0.001, **p<0.005

The regression analysis highlights that **Incident Response Mechanisms** had the **strongest positive impact** on SMEs' resilience (B = **0.415**), emphasising the critical nature of having established protocols to respond quickly and minimise disruption (Hadap et al., 2025; Sonkar et al., 2025).

Significantly, the factor **Incident Response Mechanisms** was identified as having the **strongest impact** on SMEs' resilience, with an unstandardised coefficient, B, of **0.415** ($p < 0.001$), followed by cybersecurity policy adoption and cybersecurity training. These results reinforce the conclusion that strong, structured cybersecurity

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue XI November 2025

frameworks, including policies, frequent training, and robust incident response protocols, are essential for enhancing the security posture of SMEs against cyber threats.

The collected data confirms that enterprises sampled achieved a high mean Cybersecurity Preparedness

Score of 75.4, alongside a mean Financial Resilience Index of 82.6, suggesting that those enterprises demonstrating resilience are those that have already adopted proactive measures (Sonkar et al., 2025).

DISCUSSION OF FINDINGS

The research findings provide robust empirical support for the assertion that Cyber Resilience must be treated as a strategic investment, rather than a secondary cost, for SMEs in emerging economies. The quantified impacts establish that inadequate preparedness poses an existential threat, often culminating in the 60 per cent business failure rate observed (Sonkar et al., 2025).

The discussion synthesises the empirical evidence, confirming that CR is the foundation for ensuring business continuity in emerging economies. The quantified impacts, such as the mean financial loss of Rs. 25,00,000 (Sonkar et al., 2025), underscore the urgency of strategic intervention to avoid the terminal 60 per cent failure rate (Sonkar et al., 2025).

CR as a Strategic Solvency Mechanism

The inverse relationship between high preparedness scores and catastrophic outcomes confirms the central importance of proactive CR (Sonkar et al., 2025). Cyber Resilience acts as the essential mechanism for ensuring long term solvency because it drastically reduces the probability of requiring an immediate, high-cost BC activation (Sultan, 2025). Enterprises displaying resilience typically demonstrate a high correlation between robust internal controls and strong financial reserves, validating the hypothesis that CR investment enables BC (Sonkar et al., 2025). The core strategic challenge for SMEs lies in overcoming resource limitations, given that security spending is often minimal, demanding highly optimised and effective allocation (Ejaz & Matthew, 2024).

1. Strategic Resource Allocation: Optimising RPO and RTO

Due to resource constraints, where many SMEs allocate less than 5 per cent of their IT budgets to security, investment must be precisely targeted (Ejaz & Matthew, 2024).

Risk Based Prioritisation: The key metrics of RPO, Recovery Point Objective, and RTO, Recovery Time Objective, serve as essential tools for budgetary management (Kuehm, 2025; Liuzzo & Bovey, 2025). By conducting a **Business Impact Analysis, BIA,** an SME identifies and prioritises its core systems, Tier 1, quantifying potential financial, operational and legal impacts, such as lost revenue, which averages $5,600 per minute of IT downtime (Kuehm, 2025; Liuzzo & Bovey, 2025; Kuehm, 2025). This strategic approach allows SMEs to focus investment on securing quick recovery mechanisms solely for mission critical systems, thereby maximising the effect of limited resources on business continuity (Kuehm, 2025).

Minimum Baseline Controls: Despite the proven effectiveness of policy and structured security, SMEs consistently demonstrate critical failures in implementing foundational technical controls (Munster, 2025). This deficiency is illustrated by low adoption rates for core security measures.

Critical Weakness	Percentage of SMEs with Solution Implemented	Source Data Reference
Automated Data Backup Process	26%	(Munster, 2025)
Multi Factor Authentication (all critical apps)	39%	(Munster, 2025)
Cyber Incident Response Plan (or tested plan)	22%	(Munster, 2025)
Documented Cybersecurity Policy	12%	

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue XI November 2025

Training in the last year	26%	

Table 5: Top Cyber Resilience Weaknesses in SMEs (Munster, 2025)

The failure to consistently implement measures such as **Multi Factor Authentication, MFA,** and automated, tested **Data Backups** directly exposes the enterprise to higher risk and slower recovery times (Munster, 2025).

2. The Criticality of Human and Organisational Factors

The structural scarcity of skilled cybersecurity talent in emerging markets necessitates a reliance on affordable human centric solutions and external providers (Vergara Cobos, 2024; Ejaz & Matthew, 2024).

High ROI of Training: Investment in employee training provides one of the highest returns on investment for SMEs (Ejaz & Matthew, 2024). The significant statistical relationship between training frequency and reduced incident rates confirms that human focused interventions, which are typically low cost, are highly scalable and effective (Hadap et al., 2025; Ejaz & Matthew, 2024). Training programmes must be **regular, practical, and tailored** to the local business environment, using relatable, real-life examples to ensure efficacy (KPMG/FCDO, 2023; Ugbebor et al., 2024).

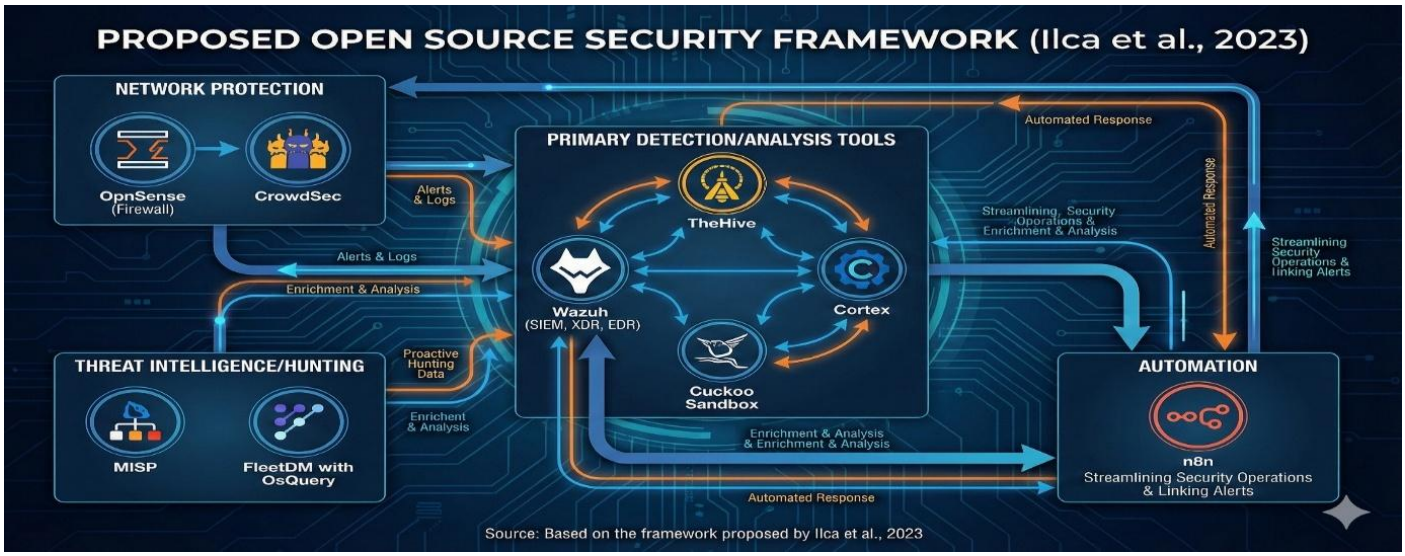
Strategic Outsourcing and Liability: Given the talent deficit, SMEs benefit significantly from engaging **third party Managed Security Service Providers, MSPs,** for infrastructure services and cyber protection (Cook, 2017). This reliance is often viewed by successful SME owners as a **cost-effective** strategy that limits the SME's liability and risk exposure in the event of a data breach (Cook, 2017). These external providers offer essential expert technical support, overcoming internal manpower shortfalls (Cook, 2017).

3. Cost Effective Technical Implementation

SMEs must adopt innovative, scalable technical solutions to build a reliable infrastructure without incurring prohibitive costs (Ejaz & Matthew, 2024).

Open-Source Security Stacks: Open-source software provides a cost effective, adaptable, and flexible alternative to expensive proprietary solutions (Ilca et al., 2023; Ejaz & Matthew, 2024). SMEs can utilise integrated open-source solutions such as **Extended Detection and Response, XDR/EDR,** and **Security Information and Event Management, SIEM,** to create a functional, **prescriptive Security Operations Centre, SOC, capability** (Ilca et al., 2023). This integrated approach enhances malware detection and response efficiency, significantly reducing the Mean Time to Detect, TTD, and thereby improving RTO (Ilca et al., 2023).

This prescriptive model enhances security operations through automation and flexible deployment using containerisation, reducing dependence on highly skilled internal staff (Ilca et al., 2023).



ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue XI November 2025

Figure 1: Proposed Open-Source Security Framework (Ilca et al., 2023)

SUMMARY, CONCLUSION AND RECOMMENDATIONS

Summary

This paper has rigorously established that robust Cyber Resilience is a **strategic imperative** for the operational survival and sustainable Business Continuity of SMEs in emerging economies (Sultan, 2025). The data confirms a statistically significant positive correlation (0.634) between preparedness and financial resilience (Sonkar et al., 2025). Failure to implement CR leads to severe consequences, including mean financial losses of **Rs. 25,00,000** and operational downtime averaging **12.5 hours** (Sonkar et al., 2025). Strategic countermeasures must focus on cost effective, high ROI interventions: applying risk based RPO/RTO metrics (Kuehm, 2025), promoting contextual staff training (KPMG/FCDO, 2023), and adopting scalable open-source security stacks (Ilca et al., 2023).

Conclusion

The existence of documented and tested **Incident Response Mechanisms** proved to be the single most potent predictor of resilience (Hadap et al., 2025), confirming that proactive policy implementation is key to survival. For SMEs, tackling the dual challenges of budget limitations and talent scarcity requires strategic reliance on external MSPs and continuous focus on improving the foundational controls identified as critically deficient (Cook, 2017; Munster, 2025). Governments must address the structural deficiencies of **regulatory fragmentation** and the **digitalisation skill debt** to ensure national cyber stability (Vergara Cobos, 2024; Gatdula, 2025).

Recommendations

A. Recommendations for Small and Medium sized Enterprises, SMEs:

1. **Prioritise Risk Based Investment:** Conduct a **Business Impact Analysis, BIA,** to define realistic **RPO and RTO targets** exclusively for mission critical systems, Tier 1, ensuring that limited resources are directed to mechanisms that guarantee rapid recovery in the most vital areas (Kuehm, 2025; Liuzzo & Bovey, 2025).

2. **Mandate Foundational Controls:** Immediately implement **Multi Factor Authentication, MFA,** across all business-critical applications and establish **automated, tested, and offsite data backups** (Munster, 2025). Develop and practice a **formal Incident Response, IR, plan** to reduce RTO (Hadap et al., 2025).

3. **Invest in Human Capital and Outsourcing:** Utilise **strategic outsourcing** to Managed Security Service Providers, MSPs, to access scalable expertise (Cook, 2017). Invest in **regular, practical, and locally contextualised cybersecurity awareness training** for all staff to reduce human error related incidents (Ejaz & Matthew, 2024; KPMG/FCDO, 2023).

B. Strategic Recommendations for Policymakers and Development Agencies:

1. **Treat CR as a Public Good:** Subsidise foundational CR capabilities, such as secure offsite backup storage and basic MFA services, particularly for micro enterprises, to mitigate the systemic risk posed by insecure SMEs (Vergara Cobos, 2024).

2. **Invest in Regulatory Harmonisation:** Support regional bodies to standardise cyber laws and streamline compliance mandates, specifically working to eliminate the burden of costly regulatory fragmentation on SMEs (Gatdula, 2025).

3. **Address the Digitalisation Skill Debt:** Ensure that investment in cybersecurity R and D and talent development runs parallel to national digital transformation efforts to mitigate the critical shortage of skilled professionals (Vergara Cobos, 2024).

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue XI November 2025

REFERENCES

1. Cook, K. D. (2017). Effective Cyber Security Strategies for Small Businesses. Doctoral Dissertations, ScholarWorks, Walden University Research.
2. Ejaz, U., & Matthew, B. (2024). Cost effective cybersecurity solutions for SMEs: Balancing security needs and budget constraints. ResearchGate.
3. Everbridge Team, The. (2025). Business resilience vs business continuity. Everbridge Blog.
4. FACTS Asia. (2025). Cybersecurity and Cyber Resilience in the Global South. FACTS Asia Center Inc.
5. Gatdula, J. R. (2025). The PRC's Evolving Cyber Laws and Implications for Southeast Asia's Digital Economy and Integration. New Perspectives on Asia, CSIS.
6. Hadap, M. K., Mehta, A. K., Narsimlu, G., Jawarkar, P., Kaluvala, V., & Chaturvedi, A. K. (2025). An empirical study on the economic impact of cybersecurity breaches and computer fraud on SMEs. Metallurgical and Materials Engineering, 31(2).
7. Ilca, L. F., Lucian, O. P., & Balan, T. C. (2023). Enhancing cyber resilience for small and medium sized organizations with prescriptive malware analysis, detection and response. Sensors, 23(15), 6757.
8. KPMG/FCDO. (2023). Cybersecurity toolkits for SMEs – Strengthening the cybercrime defences of Nigerian small businesses. Cybil Portal.
9. Kuehm, K. (2025). How to optimize RPO and RTO in disaster recovery plans. MightyID.
10. Liuzzo, M., & Bovey, K. (2025). RPO and RTO: What's the difference? Veeam Blog.
11. Liquid Intelligent Technologies. (2021). The evolving Cyber Security threat in Africa. Liquid Intelligent Technologies Cyber Security Report.
12. Munster Technological University Cybersecurity Research Group. (2025). SME cyber resilience: State of the sector 2025.
13. Sonkar, N., Verma, N., Kumar, A., Naqvi, D., & Nisa, Z. (2025). An empirical study on the economic impact of cybersecurity breaches and computer fraud on SMEs. Journal of Information Systems Engineering and Management, 10(7s).
14. Splunk Team, The. (2025). Business continuity vs. business resilience: What's the difference? Splunk Blogs.
15. Sultan, N. (2025). The nexus of cyber resilience and business continuity: A strategic imperative for small and medium enterprises in emerging economies.
16. Ugbebor, F., Aina, O., Abass, M., & Kushanu, D. (2024). Employee cybersecurity awareness training programs customized for SME contexts to reduce human error related security incidents. Journal of Knowledge Learning and Science Technology, 3(3), 382–409.
17. Vergara Cobos, E. (2024). Cybersecurity economics for emerging markets (World Bank e Book).
18. World Bank. (2024). Digital Transformation Drives Development in Africa. World Bank Results Briefs.
19. World Economic Forum (WEF). (2024). SMEs can turn cybersecurity risk into opportunity. Here's how. World Economic Forum.