FBMS Journal of Family Business and Management Studies
Journal of Family Business and Management Studies
ISSN 2821-9643 (online) Volume 18 Number 1, January-June 2026

Infrastructure Resilience and Performance of Small and Medium Scale Enterprises in Anambra State, Nigeria

Received: 24.12.2024
Revised: 03.03.2025
Accepted: 08.04.2025

Ojukwu Henry Sonna[1*], Iruogu Chinedu[2] and Anyika Michael Ikenna[3]
[1,2] Department of Business Administration, Nnamdi Azikiwe University
[3] Unizik Business School
[1,2,3]Along Onitsha - Enugu Expy, Ifite Road, Awka 420110, Anambra, Nigeria.
[2]iruoguc@gmail.com, [3]anyiksm@yahoo.com
**Corresponding author:* hs.ojukwu@unizik.edu.ng

Abstract

Small and Medium Enterprises (SMEs) often struggle to maintain competitiveness due to infrastructural deficiencies that cannot withstand external shocks and threats. This study examines the impact of infrastructure resilience on the performance of SMEs in the Anambra East Local Government Area of Nigeria. A descriptive research design was utilised, and data were collected from 207 SMEs using a structured questionnaire. Hypothesis testing was conducted through regression analysis, employing E-Views version 10. Cyber resilience significantly influenced operational security, indicated by a coefficient of 1.060231 and an R-squared value of 95.45%, highlighting its role in protecting operational integrity. Furthermore, institutional resilience greatly impacted economic sustainability, with a coefficient of 1.078565 and an R-squared value of 95.72%, underscoring the necessity of resilient institutional structures for economic stability. These findings confirm that cyber and institutional resilience are critical to SME performance in Anambra East. Consequently, the study recommends adopting advanced time management tools, enhancing cybersecurity measures, and establishing robust institutional frameworks to ensure long-term sustainability and operational efficiency. The study provides valuable insights for policymakers and business leaders aiming to enhance infrastructure resilience and support the growth of SMEs in Nigeria.

Keywords: Infrastructure resilience, Cyber Resilience, Institutional Resilience, Time Efficiency, Operational Security, Economic Sustainability.

Introduction

Countries' developmental progress is influenced by the available infrastructure supporting sustainable business growth and enhancing quality of life. Embedded in the infrastructure is an inherent resiliency that enables it to serve the population without revisiting or rebuilding. Infrastructure is the backbone of communities by providing critical services- such as water, transportation, electricity, and communications- and laying a foundation for health, safety, and economic growth to thrive (Cybersecurity & Infrastructure Security Agency, 2025).

Historical events are significant contributors to the study of Infrastructure Resiliency (IR), including the 9/11 attacks in 2001, Hurricane Katrina in 2005, the Fukushima Daiichi nuclear disaster in 2011, Superstorm Sandy in 2012, and the COVID-19 pandemic in 2020 (UNDRR, 2023). IR refers to the ability of infrastructure systems to withstand, adapt to, and recover from natural disasters, cyber-attacks, physical attacks, and other disruptions. It involves designing and building robust, flexible infrastructure that remains functional even when damaged or stressed (OECD, 2024). " The history of IR is characterised by continuous evolution, technological advancements, lessons learned from past failures, and the growing need to adapt to a changing world (Capacci et al., 2022). IR safeguards public health and safety while supporting economic growth and development (Resilience Rising, 2024). Enhancing infrastructure resilience can be achieved by mitigating the exposure of infrastructure assets to natural hazards, reducing their vulnerability, designing systems for continued service delivery when damaged, ensuring that infrastructure prevents catastrophic failure, and enabling users of infrastructure services to manage service disruptions better (Zhao et al., 2022). Resilience demands tackling immediate infrastructure challenges by maintaining and constructing sustainable infrastructure for the future (OECD, 2025). Addressing the complex challenges and opportunities of infrastructure resilience and maintenance requires a multidimensional approach that considers local and global factors, optimises asset performance throughout its lifecycle and network functions, and employs new technologies and nature-based solutions. (OECD, 2025). America's infrastructure is an interconnected system of highways, streets, public buildings, mass transit, ports, airports, inland waterways, water systems, waste facilities, the electric grid, broadband networks, dams, levees, and other public and private facilities (American Society of Civil Engineers, 2025). Maintaining these networks has an impact on public safety and economic prosperity.

In this digital era, cyber resiliency (Cirera et al., 2024) and institutional resiliency (Barin et al., 2015) are expected to be integrated into infrastructure for more sustainable business development. Corruption in Nigeria, evidenced by its low 2023 Transparency Index score of 25 and a ranking of 145 out of 180, has significantly hindered infrastructural growth and can be directly linked to the

country's persistent infrastructure deficit (Oladipo, 2024). The developed infrastructures in Nigeria often lack the resilience to endure beyond the tenures of the administrations that initiated them. This has a daunting negative effect on Nigeria's business performance, particularly among small and medium-sized enterprises (SMEs). The absence of built-in resiliencies in cyber and institutional settings among existing infrastructures undermines the sustainability of SMEs in Nigeria and several other states. With the advancement of artificial intelligence, threat actors continue to perpetrate cyber-attacks on vulnerable businesses that cannot defend themselves against these threats. Key aspects of this problem include the interdependence of physical and cyber systems, the increasing sophistication of cyber threats, limited visibility and control over cyber assets, and insufficient cybersecurity talent and resources (Chatham House, 2024). Institutional resiliency challenges organisations and governmental agencies to uphold the resilience of critical infrastructure systems. These challenges include gaps in governance and leadership, insufficient policies and procedures, inadequate risk management and contingency planning, a weak culture and employee engagement, limited capabilities for learning and improvement, inflexibility, and a lack of adaptability (Barasa, 2018). When focusing on institutional resiliency, attention should be directed toward risk assessment, access to finance, capacity building, business support services, regulatory environment, and infrastructure development (Nkechi et al., 2022).

A historical context that further justifies this study is the impact of the Biafra Civil War (1967–1970) on southeastern Nigeria. This war remains one of the most significant conflicts in Nigeria's history, with far-reaching consequences for infrastructure, economic development, and business sustainability. The devastation wrought by the war was immense, resulting in a fractured economy, destroyed infrastructure, and a marginalized population. However, beyond the immediate destruction, post-war neglect, insufficient government investment, and systematic policy failures have perpetuated the region's infrastructural challenges, further entrenching economic stagnation and business difficulties. The lingering effects of the war continue to shape the economic trajectory of the southeast, making it one of the most underdeveloped and politically marginalised regions in Nigeria. The region's lack of robust infrastructure underscores the need for a comprehensive approach to infrastructure planning, development, and sustainability, ensuring that historical lessons inform future infrastructural advancements.

Small and Medium Enterprises (SMEs) in Anambra East face significant barriers to cyber and institutional resilience. These challenges include weak digital infrastructure, limited cybersecurity awareness, and fragile institutional support systems, all exposing businesses to cyber threats, disrupting operations, and undermining their capacity to adapt and sustain growth in a digital economy. The legacy of the Biafra Civil War (1967–1970) continues to impact the region, as

post-war neglect has resulted in underdeveloped infrastructure and limited business opportunities. Compared to other regions of Nigeria, SMEs in northern Nigeria encounter security threats from insurgency and banditry, which disrupt business activities and deter investment. In contrast, SMEs in urban centres like Lagos and Abuja benefit from better infrastructure and financial opportunities but struggle with high operational costs, regulatory burdens, and severe traffic congestion. Meanwhile, businesses in the South-South region contend with environmental degradation caused by oil exploration, adversely affecting agriculture and fishing industries. Despite these variations, Nigeria's lack of resilient infrastructure that supports long-term business sustainability and economic growth remains a common issue.

Given this background, the study examines the impact of cyber and institutional resilience on the performance of small and medium-sized enterprises (SMEs) in the Anambra East Local Government Area. Addressing these challenges in Anambra East requires adopting global best practices while customising solutions to local conditions, ensuring resilient infrastructure, enhanced financial access, and more substantial institutional support for SMEs. Moreover, the findings from this study can guide policies and practices in other regions facing similar challenges by emphasising the significance of adaptive infrastructure planning, promoting public-private partnerships, and strengthening institutional frameworks to support SME growth and resilience.

Literature review

Infrastructure resilience

Indian Prime Minister Hon. Shri Narendra Modi remarks on infrastructure: "Infrastructure is not only about returns but also about reach and resilience. It must leave no one behind and serve the people even during times of crisis" (Coalition for Disaster Resilient Infrastructure 2024). The European Commission defines resilience as the capacity of a country or region to withstand, adapt to, and swiftly recover from stresses and shocks such as drought, violence, conflict, or natural disasters (Sparf, 2019). Similarly, The National Security Memorandum on Critical Infrastructure Security and Resilience (2024) defines resilience as "the ability to prepare for threats and hazards, adapt to changing conditions, and withstand and recover rapidly from adverse conditions and disruptions.

Resilient infrastructure (IR) is an essential foundation for sustainable development (UNDER, 2024). As the intensity and frequency of hazards continue to rise, disruptions in infrastructure systems become more common, leading to significant economic and societal costs (UNDRR, 2024). Achieving and maintaining developmental gains requires substantial investment in the resilience of infrastructure systems to withstand shocks and effectively manage severe weather events such as floods, droughts, and extreme temperatures (Ward, 2020). Wu (2024) emphasises that constructing resilient infrastructure systems is estimated to increase the total investment cost by only 3% while ignoring this will

be detrimental to business health and job creation. The Principles for Resilient Infrastructure outline a series of principles, essential actions, and guidelines aimed at achieving national-scale net resilience gains while enhancing the continuity of critical services, including energy, transport, water, wastewater, waste, and digital communications, which support the effective functioning of health and education systems (UNDRR, 2023). These principles include Continuous Learning, which involves developing understanding and insight into infrastructure resilience through monitoring, analysis, learning from past events, stress testing, and adaptation; Proactively Protected, which ensures that infrastructure is designed, built, and maintained to withstand known and emerging hazards through enhanced safety standards and emergency preparedness; Environmentally Integrated, aligning infrastructure development with environmental sustainability and natural systems, leveraging nature-based solutions while minimising ecological impact; Socially Engaged, which involves communities and stakeholders in infrastructure planning and resilience efforts to ensure inclusivity, equity, and local relevance; Shared Responsibility, enhancing infrastructure resilience through coordinated roles and shared accountability, promoting collective action and governance across sectors, organisations, and society; and Adaptively Transforming, where flexible, forward-looking strategies and innovations enable infrastructure systems to evolve in response to changing risks and contexts.

Cyber resilience

The patterns of cyber-attacks are multi-dimensional. Even in technologically advanced countries, businesses are often targeted by cybercriminals, let alone Nigeria, where digital literacy is at its lowest. The United Kingdom government revealed that cybersecurity breaches and attacks remain a common threat, as just over four in ten businesses (43 per cent) reported experiencing some cybersecurity breach or attack in the last 12 months (Ribiero, 2025). Rubin (2025) warns that companies poised to thrive in the next decade will integrate cyber resilience into their core, ensuring security, continuity, and market leadership amid ongoing digital disruption. Cyberattacks in Nigeria are increasing, affecting both public and private sectors. The financial industry is frequently targeted, with banks and fintechs facing threats such as phishing, ransomware, and business email compromise (BEC), during which attackers impersonate executives to mislead employees. Cybercrime continues to be a significant challenge for Nigeria and Africa, where organizations encounter nearly 3,200 attacks each week—73% higher than the global average—with eight African nations listed among the top 20 global hotspots for cyber threats, according to Check Point Software Technologies (Lemos, 2025). As these waves of attacks continue to rise, the need to become cyber resilient becomes pressing.

Cyber resilience is the capacity of organisations to respond to cyber-attacks and to build new robustness following successful breaches (Nnarelli et al., 2020). With recent advancements in artificial intelligence through machine and deep learning, cyber-attacks have become inevitable. To emphasise this point, KPMG (2020) asserts that the era of an efficient, well-tested cybersecurity system rendering a successful cyber-attack unlikely has ended, as cyber breaches are now unavoidable for any technology-driven business. Therefore, enhancing cyber resilience is crucial for SMEs, which often face unique vulnerabilities due to limited cyber defence capabilities. Additionally, due to resource constraints, a lack of awareness, and inadequate cybersecurity measures, SMEs are particularly susceptible to cyber threats such as phishing, malware, data breaches, and ransomware (Bamidele et al., 2024). By adopting cyber resilience strategies, SMEs can protect their information assets and ensure they can quickly recover from incidents, thus maintaining operational continuity and customer trust.

Institutional resilience

Institutional resilience allows organisations to absorb and recover from external shocks while positively adapting and transforming to meet long-term changes and uncertainties (Haider, 2021). Investing in robust, well-functioning, and adaptable social systems, such as health, education, and social protection systems, can strengthen resilience, as these systems help cushion the adverse economic and social impacts of crises (Strupat & Marschall, 2020). Institutional resilience encompasses institutions' internal processes and structures, along with their relationships with external stakeholders and the environment in which they operate. In the context of SMEs, institutional resilience is vital for navigating regulatory environments and responding to market fluctuations. This resilience is significantly relevant to the study of infrastructure resilience and the performance of SMEs. When institutions demonstrate resilience, they can better support SMEs during crises, facilitating access to essential resources and information critical for sustaining operations. This, in turn, nurtures a more favourable environment for SME growth and infrastructure development. Resilient institutions can enhance collaboration among stakeholders, improving the overall infrastructure landscape. Additionally, institutional resilience can encourage partnerships between SMEs, government bodies, and other organisations, leading to coordinated infrastructure development and maintenance efforts.

SMEs performance

Performance is a measure of an organisation's status. Opusunju, Akyuz, and Jiya (2017) noted that performance reflects the productivity of an enterprise's members measured in terms of revenue, profit, growth, development, and expansion of the organisation. With over 800 registered SMEs in Anambra state and more springing up almost daily, SMEs stand as one of the significant sources of the wealth Anambra state generates (Anekwe & Nwokediba, 2019). In Nigeria, SMEs constitute most of the business sector and contribute significantly. They will contribute far better to the country's economic growth if allowed and supported. Small and

medium-sized enterprises (SMEs) are advocates of growth and public profitable development because they play a critical role in reducing poverty, increasing gross domestic product (GDP), diversifying, and creating jobs in both developed and developing countries (Okoli &Anugwu, 2022; Okoli, Nwakoby & Adani, 2023). There are more than 39.65 million registered SMEs in Nigeria, which account for about 87.9% of the total workforce, 46.31% of national GDP growth and 6.2% of international gross exports (National Bureau of Statistics, 2021). The National Bureau of Statistics (2021) realised that SMEs in Nigeria continue to face numerous challenges, making them perform below expectations. Infrastructure deficit and frequent changes in public policy are among the top list. In this regard, Adebiyi and Amole (2017) believe that innovation is a strategic issue as it will assist in reducing internal inefficiencies, improve processes, and enhance decision-making processes positively. Relating to this study, time efficiency, operational security, and economic sustainability are the measures of SMES performance. *Time efficiency* refers to the proper use of time by focusing on essential tasks, avoiding distractions, and organising work to accomplish more with less effort without compromising quality (Sreejitha, 2024). Furthermore, improved time efficiency can increase customer satisfaction and loyalty, which is critical for SMEs' long-term success. *Operational security*, commonly called OPSEC, is a risk management strategy and process that helps identify critical information adversaries could use to inflict business (Proof point, 2024). When businesses prioritise security, they protect their assets and contribute to the overall stability of the business environment. *Economic sustainability* refers to practices supporting a company's or nation's long-term economic development while protecting environmental, social, and cultural elements (Bish, 2021). Furthermore, as SMEs become more economically sustainable, their ability to pay taxes and contribute to local economies increases, thereby attracting further investment into infrastructure.

Hypotheses development

H_{01}: The effect of cyber resiliency on the operational security of SMEs in the Anambra East Local Government Area is insignificant.

H_{02}: Institutional resiliency does not affect the economic sustainability of SMEs in the Anambra East Local Government Area.

Methodology

Research design and study area

This study adopted a descriptive research design. The study was conducted in Anambra East Local Government Area of Anambra state, one of the five south-eastern states in Nigeria. The state was created in 1991, and the state capital is Awka. It presently has 21 local governments and three senatorial districts, just like other states of Nigeria. Anambra is bounded by the state of Kogi in the north, Enugu in the east, Abia in the southeast, Imo and rivers in the south, and Delta and Edo in the west. It includes the valley of the lower Anambra River, which is a tributary of the Niger River. The southern part consists of a tropical rainforest along the eastern bank of the

Niger River, which forms Anambra's western boundary. Overall, the people of Anambra state are known for their cultural richness, entrepreneurial spirit and a strong sense of community. They have made significant contributions to various fields and continue to play an important role in Nigeria's social, economic and political landscape.

Study scope

The scope of this study encompasses vital aspects, and they are discussed below: Geographic Scope: The study focuses specifically on Anambra state SMEs. It aims to investigate the relationship between infrastructure resilience and the performance of these micro-businesses within the geographical boundaries of Anambra state, Nigeria. Sector Scope: The study focuses on SMEs, encompassing various micro businesses and institutions operating in Anambra East Local Government Area. It includes organisations involved in service delivery, policy-making, governance, and other relevant areas within the micro sector. Variable Scope: The study concentrates on the effect of infrastructure resilience initiatives within SMEs. It explores adopting and implementing infrastructure technologies, tools, and platforms to enhance organisational processes, service delivery, decision-making, and transparency. While the scope of this study is specific to Anambra state, the research findings and insights can potentially be applied to other similar regions or public sector organisations facing similar infrastructure resilience challenges or priorities.

Study population, sample size determination, and sampling technique

Only tax-paying SMEs were considered in this study to promote due diligence and compliance with state regulations. Accordingly, the list of registered business names with valid tax clearance was obtained from the Anambra State Internal Revenue Service (2024), ensuring the inclusion of legally recognised enterprises. The population frame which emanated from the governmental agency was four hundred thirty (430) small and medium enterprises in the Anambra East Local Government Area. In conducting this research, the sample size was determined using the Taro Yamane sample technique, as shown below;

$$n = \frac{N}{1+N\,(e)^2}$$

Where 1 = constant
N = sample size
N = total population = 430
E = error limit (0.05 or 5%)
n = 207 SMEs

The study adopted a simple random sampling technique, ensuring every SME had an equal chance of being selected. This method minimised selection bias and enhanced the sample's representativeness, reflecting the broader SME population. By giving each SME an equal probability of inclusion, the technique strengthened the validity of the findings and supported generalizability. Furthermore, to ensure the effective distribution of the questionnaire, the Bowley Proportional allocation formula was used, and the result is presented in Table 1 below:

Table 1 Bowley's Proportional Allocation

S/N	Towns	Population	Distributed Questionnaire
1	Aguleri	57	27
2	Umueri	61	29
3	Otuocha	52	25
4	Enugwu-Aguleri	49	24
5	Eziagulu-Otu	39	19
6	Anam	45	22
7	Igbariam	33	16
8	Nando	27	13
9	Nsugbe	28	13
10	Enugwu-Otu	39	19
	Total	**430**	**207**

Source: Field Survey, 2024

Data analysis method

The data analysis for this study involved using E-view version 10 statistical analysis to examine the effect of infrastructure resilience on the performance of SMEs in Anambra East LGA. To achieve this intent, data were analysed using simple regression.

Model Specification

Objective 1: To assess cyber resiliency's effect on SMEs' operational security in Anambra East Local Government Area.

Model Specification:

$$OS=\beta0+\beta1CR+\epsilon \text{ ----------2}$$

Where:

OS = Operational Security of SMEs

CR = Cyber Resiliency

β0 = Intercept (constant term)

β1= Coefficients for respective variables

ϵ = Error term

Objective 2: To examine institutional resiliency's effect on the economic sustainability of SMEs in Anambra East Local Government Area.

Model Specification:

$$ES=\alpha+\gamma1IR+\epsilon$$

Where:

ES = Economic Sustainability of SMEs

IR = Institutional Resiliency

α = Intercept (constant term)

γ1 = Coefficient for Institutional Resiliency

ϵ = Error term

Analysis and presentation of findings

Data presentation

This study's sample size is 207; the researcher distributed 207 questionnaires to the target population. In the process, 189 were retrieved back in good order, on which the findings of this study are based.

Test of hypotheses

Hypothesis 1: The effect of cyber resiliency on the operational security of SMEs in the Anambra East Local Government Area is insignificant.

Table 2 Cyber Security and Operational Efficiency Regression
Dependent Variable: OPERATIONAL_SECURITY
Method: Least Squares
Date: 08/26/24 Time: 06:09
Sample: 1 189
Included observations: 189

Variable	Coefficient	Std. Error	t-Statistic	Prob.
Cyber_Resiliency	1.060231	0.016928	62.63099	0.0000
C	-1.912025	0.357201	-5.352799	0.0000
R-squared	0.954497	Mean dependent var		19.73016
Adjusted R-squared	0.954254	S.D. dependent var		5.815990
S.E. of regression	1.243943	Akaike info criterion		3.284975
Sum squared resid	289.3628	Schwarz criterion		3.319280
Log-likelihood	-308.4302	Hannan-Quinn criteria.		3.298873
F-statistic	3922.642	Durbin-Watson stat		0.188041
Prob(F-statistic)	0.000000			

Source: E-view 10

Table 2 displays the regression analysis results, with operational security as the dependent variable and cyber resiliency as the independent variable. The coefficient for cyber resiliency is 1.060231, indicating a strong positive relationship between cyber resiliency and operational security. The t-statistic for cyber resiliency is 62.63099, with a p-value of 0.0000, showing that this relationship is statistically significant at the 1% level. The R-squared value of 0.954497 implies that about 95.45% of the variance in operational security is explained by cyber resiliency, indicating a highly reliable model.

The null hypothesis (H_0) suggests no relationship between cyber resiliency and operational security, implying the coefficient of cyber resiliency is zero. The alternative hypothesis (H_1) suggests a significant relationship, implying the coefficient is not zero. Given that the p-value for cyber resiliency is significantly less than 0.05 ($p = 0.0000$), we reject the null hypothesis and accept the alternative hypothesis, concluding that cyber resiliency significantly impacts the operational security of SMEs in Anambra East LGA.

Hypothesis 2: Institutional resiliency does not significantly affect the economic sustainability of SMEs in the Anambra East Local Government Area.

Table 3 Institutional Resiliency and Economic Sustainability

Dependent Variable: ECONOMIC_SUSTAINABILITY
Method: Least Squares
Date: 08/26/24 Time: 06:10
Sample: 1 189
Included observations: 189

Variable	Coefficient	Std. Error	t-Statistic	Prob.
Institutional_Resiliency	1.078565	0.016679	64.66604	0.0000
C	-2.422814	0.353867	-6.846678	0.0000

R-squared	0.957195	Mean dependent var	19.72487
Adjusted R-squared	0.956967	S.D. dependent var	5.897932
S.E. of regression	1.223496	Akaike info criterion	3.251828
Sum squared resid	279.9284	Schwarz criterion	3.286132
Log-likelihood	-305.2978	Hannan-Quinn criteria.	3.265726
F-statistic	4181.697	Durbin-Watson stat	0.161321
Prob(F-statistic)	0.000000		

Source: E-views10

Table 3 provides the regression analysis results where economic sustainability is the dependent variable, and institutional resiliency is the independent variable. The coefficient for institutional resiliency is 1.078565, indicating a strong positive relationship between institutional resiliency and economic sustainability. The t-statistic for institutional resiliency is 64.66604, with a p-value of 0.0000, demonstrating that this relationship is statistically significant at the 1% level. The R-squared value of 0.957195 indicates that approximately 95.72% of the variance in economic sustainability is explained by institutional resiliency, suggesting that the model is highly reliable and effective in predicting economic sustainability based on institutional resiliency.

The null hypothesis (H_0) posits that there is no relationship between institutional resiliency and economic sustainability, implying the coefficient of institutional resiliency is zero. The alternative hypothesis (H_1) posits that there is a significant relationship, meaning the coefficient is not equal to zero. Given that the p-value for institutional resiliency is far below 0.05 ($p = 0.0000$), we reject the null hypothesis and accept the alternative hypothesis, concluding that institutional resiliency influences the economic sustainability of SMEs in Anambra East LGA.

Discussion of results

Hypothesis one indicates a significant positive impact of cyber resiliency on operational security, as shown by a coefficient of 1.060231. The relationship is statistically significant, with a t-statistic of 62.63099 and a p-value of 0.0000. The high R-squared value of 0.954497 suggests that 95.45% of the variance in operational security is explained by cyber resiliency, highlighting the critical importance of cyber resilience in

safeguarding operational integrity. This finding aligns with the work of Akpan (2015), who observed and concluded that Nigeria has suffered dramatically in cyber – attacks and that cyber security and resilience have become valuable tools for checking and stopping cyber risks.

Hypothesis two demonstrates a robust positive relationship between institutional resiliency and economic sustainability, with a coefficient of 1.078565. The statistical significance is supported by a t-statistic of 64.66604 and a p-value of 0.0000, indicating a highly reliable model. The R-squared value of 0.957195 suggests that 95.72% of the variance in economic sustainability is explained by institutional resiliency, emphasising institutions' critical role in economic stability. This agrees with the findings of Eke and Eke (2024), who reveal that institutional quality was found to positively and significantly influence the effect of resilience on economic growth in countries within the region and thus recommends strengthening the institutional framework for countries in the region through the ECOWAS community strategy.

Conclusion, recommendations, and study implications

The findings of this study underscore the crucial role of infrastructural resiliency in SMEs' performance in Anambra State, Nigeria. These findings align with prior research emphasising the importance of resilient infrastructures in fostering business continuity and sustainability. The study further highlights the growing necessity for SMEs to protect their digital assets against cyber threats to maintain operational security. This study's strong positive correlation between cyber resiliency and operational security reinforces the understanding that cybersecurity measures are integral to preserving organisational integrity in an increasingly digital environment. Additionally, the relationship between institutional resiliency and economic sustainability resonates with the broader recognition of institutional frameworks' role in supporting economic stability and long-term growth. Institutional resiliency ensures that SMEs can navigate regulatory challenges and adapt to economic shifts, reinforcing the need to strengthen institutional support structures to bolster SME sustainability.

In conclusion, this study provides compelling evidence that infrastructural resiliency is a crucial determinant of SME performance in Anambra State. The significant relationships identified between cyber resiliency, and institutional resiliency with their respective outcomes emphasize the need for SMEs to prioritize the development of resilient infrastructures to enhance their overall performance and sustainability. As SMEs continue to face evolving challenges in the technological, cyber, and institutional landscapes, policymakers and business leaders must invest in strengthening these areas to secure the future growth and stability of SMEs in the region.

Among other things, the study suggested the under-listed;

Immediate actions for SMEs:

Adopting advanced time management tools is essential for SMEs to optimize operations and reduce downtime. Furthermore, implementing employee

training programs can enhance technological competencies and strengthen system resiliency, contributing to a more efficient and adaptable workforce.

Small and medium-sized enterprises (SMEs) should perform regular vulnerability assessments to identify and mitigate security gaps. Furthermore, it is essential to provide employees with training on recognizing and responding to cyber threats. Implementing advanced security technologies is also crucial to enhancing protection against potential breaches.

SMEs must focus on implementing effective governance structures to enhance decision-making and accountability. Ensuring compliance with regulatory standards reduces legal risks and strengthens organisational credibility. Additionally, fostering strong stakeholder relationships is crucial for gaining support and promoting collaborative efforts in operational activities.

Long-term strategies for policymakers:

Supporting SMEs requires establishing institutional frameworks that enhance access to technology and training. Encouraging initiatives to improve technological infrastructure is equally vital for ensuring long-term business growth and resilience.

Enhancing SME cybersecurity involves creating customised guidelines and fostering public-private partnerships to improve access to security tools and training. Incentivising the adoption of strong cybersecurity measures can further bolster resilience.

Crafting policies that build resilient frameworks aligned with SME needs is essential for sustainable growth. Reinforcing regulatory structures and providing platforms for stakeholder collaboration can promote economic stability and trust.

Future research implication

Future studies could explore the long-term impact of infrastructural resiliency on SME performance across different regions, enabling comparative analysis. Investigating sector-specific resiliency strategies could offer tailored insights for diverse industries. Additionally, research on the effectiveness of public-private partnerships in enhancing cybersecurity resilience would be valuable. Examining the role of digital literacy in strengthening technological resilience could further inform training initiatives. Finally, future work could assess the impact of evolving regulatory frameworks on institutional resilience and SME sustainability.

References

Adebiyi, S., & Amole, B. (2017). Innovation as a strategic tool for improving SME performance. International Journal of Business Innovation, 12(3), 150-165.

Anekwe, G., & Nwokediba, E. (2019). SMEs as a significant source of wealth in Anambra state: An empirical study. African Journal of Business and Economic Research, 15(4), 99-114.

American Society of Civil Engineers (2025). A Comprehensive Assessment of America's Infrastructure.https://infrastructurereportcard.org/wpcontent/uploads/2025/03/ Full-Report-2025-Natl-IRC-WEB.pdf

Bamidele, B., Ayodeji, A., Amajuoyi, P., Mayokun, D., & Kudirat, B. (2024). Digital transformation in SMEs: Identifying cybersecurity risks and developing effective mitigation strategies. Global Journal of Engineering and Technology Advances, 2024, 19(02), 134–153

Barasa, E., Mbau, R., & Gilson, L. (2018). What Is Resilience and How Can It Be Nurtured? A Systematic Review of Empirical Literature on Organizational Resilience. International journal of health policy and management, 7(6), 491–503. https://doi.org/10.15171/ijhpm.2018.06

Barin Cruz, L., Aguilar Delgado, N., Leca, B., & Gond, J.-P. (2015). Institutional resilience in extreme operating environments: The role of institutional work. Business & Society, 55(1), 10-43.

Bish, J. (2021). Economic Sustainability Examples that Inspire Change. https://www.populationmedia.org/the-latest/what-is-economic-sustainability

Capacci, L., Biondini, F., & Frangopol, D. M. (2022). The resilience of ageing structures and infrastructure systems with an emphasis on seismic resilience of bridges and road networks: Review, Resilient Cities and Structures. 1(2), 23-41.

Chatham House. (2024). The interdependence of physical and cyber systems. Retrieved from [https://www.chathamhouse.org] (https://www.chathamhouse.org)

Cirera, X., Comin, D., Cruz, M., Lee, K. M., & Torres, J. (2024). Technological and cyber resilience in critical infrastructure. Cyber Resilience Journal.

Coalition for Disaster Resilient Infrastructure (2024). PARTNERING FOR A RESILIENT FUTURE. https://cdri.world/upload/pages/1804258240189785_202407110512 cdri-booklet-2024.pdf

Cybersecurity & Infrastructure Security Agency (2025). Infrastructure Resilience Planning Framework (IRPF). https://www.cisa.gov/sites/default/files/2025-03/IRPF_3.17. 2025.pdf

Eke, I. C., & Eke, F. A. (2024). Institutional Quality and Economic Resilience: Panacea For Potential Long-Term Economic Growth In West Africa. Gusau Journal Of Economics And Development Studies, 5(1), 123–143. Https://Doi.Org/ 10.57233/ Gujeds.V5i1.08

Haider, H. (2021). Mainstreaming institutional resilience and systems strengthening in donor policies and programming. https://reliefweb.int/report/world/mainstreaming-institutional-resilience-and-systems-strengthening-donor-policies-and

Jaiswal, G. (2023). Understanding Technology Resilience: A Regulatory Focus for IT Leaders. https://medium.com/deloitte-uk-cloud-blog/understanding-technology-resilience-a-regulatory-focus-for-it-leaders-80fc167d3495

KPMG (2020). CyberResilience Guide. https://assets.kpmg.com/content/dam/kpmg/in/pdf/2020/03/cyber-resilience-guide.pdf

Lathabhavan, R. & Kuppusamy, T. (2024). "Examining the role of digital leadership and organisational resilience on the performance of SMEs during the COVID-19 pandemic", International Journal of Productivity and Performance Management, 73(8), 2365–2384. https://doi.org/10.1108/IJPPM-02-2023-0069

Lemos, R. (2025). Nigeria Touts Cyber Success, Even as Cybercrime Rises in Africa. https://www.darkreading.com/cyber-risk/nigeria-touts-cyber-success-african-cybercrime-rises

Liu, W. (2020). Quantitative measures of resilience in infrastructure systems. Quantitative Infrastructure Research.

National Bureau of Statistics. (2021). SME statistics and economic contributions report—National Bureau of Statistics, Nigeria.

National Security Memorandum on Critical Infrastructure Security and Resilience, The White House, (2024). https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/

Nkechi, O. C., Akonu, S., & Ezemba, E. N. (2022). Challenges in institutional resilience and infrastructure development. African Journal of Development Studies.

Nnarelli, A., Nonino, F., & Palombi, G. (2020). Understanding the Management of Cyber Resilient Systems. Comput. Ind. Eng. 2020, 149,106829

OECD (2025). Why is this important? https://infrastructure-toolkit.oecd.org/infragov-theme/resilience/

Okafor, P. (2023). Benefits and Adoption of Internet of Things (IoT) to Nigeria's Small and Medium-Sized Enterprises (SMEs). https://www.researchgate.net/publication/372910392_Benefits_and_Adoption_of_Internet_of_Things_IoT_to_Nigeria's_Small_and_Medium-Sized_Enterprises_SMEs

Okoli, C., & Anugwu, A. (2022). SMEs and their role in economic growth and poverty reduction in Nigeria. Journal of Economic Perspectives, 36(1), 45-61.

Okoli, C., Nwakoby, E., & Adani, O. (2023). The contribution of SMEs to Nigeria's GDP and workforce. Nigerian Economic Review, 27(2), 77-91.

Oladipo, V. (2024). Corruption's Footprint on Infrastructure in Nigeria. https://www.verivafrica.com/insights/corruptions-footprint-on-infrastructure-in-nigeria

Opusunju, A., Akyuz, A., & Jiya, J. (2017). Performance measurement in enterprises reflects productivity, revenue, and growth. Journal of Business Research, 34(2), 56-73.

Organisation for Economic Co-operation and Development. (2024). Understanding infrastructure resilience. Retrieved from [https://www.oecd-ilibrary.org] (https://www.oecd-ilibrary.org)

Proofpoint. (2024). What Is Operational Security (OPSEC)? https://www.proofpoint.com/us/threat-reference/operational-security-opsec#:~:text=Operational%20Security%2C%20commonly%20called%20OPSEC, controlling%20access%20to%20sensitive%20data.

Resilience Rising. (2024). The role of infrastructure resilience in economic growth. Retrieved from [https://www.resiliencerising.org] (https://www.resiliencerising.org)

Ribiero, A. (2025). UK Cyber Security Breaches Survey 2025 reveals persistent threats in evolving digital landscape, bats for enhanced cyber resilience. https://industrialcyber.co/reports/uk-cyber-security-breaches-survey-2025-reveals-persistent-threats-in-evolving-digital-landscape-bats-for-enhanced-cyber-resilience/

Rubin, S. (2025). The Rising Stakes of Cyber Resilience: What the 2025 Global Incident Response Report Means for Business Leaders. https://www.paloaltonetworks.com/perspectives/the-rising-stakes-of-cyber-resilience-what-the-2025-global-incident-response-report-means-for-business-leaders/

Sparf, J. (2019). Defining resilience: European perspectives. European Resilience Studies.

Sreejitha, A. (2024). What is Time Efficiency? Here are tips and proven strategies. https://desklog.io/blog/time-efficiency/

Strupat C, & Marschall P.(2020). Strengthening Social Systems. Development Co-Operation Report 2020 Learning from Crises, Building Resilience: Learning from Crises, Building Resilience. Vol. 195. OECD iLibrary; 2020. Available from: https://www.oecd-ilibrary.org/development/development-co-operation-report2020_5f8f7af9-en

United Nations Office for Disaster Risk Reduction. (2022). Investment in resilient infrastructure. Retrieved from https://www.undrr.org

United Nations Office for Disaster Risk Reduction. (2023). Overview of key historical events in infrastructure resiliency. Retrieved from [https://www.undrr.org] (https://www.undrr.org)

UNDRR. (2023). Principles for resilient infrastructure. https://www.undrr.org/publication/principles-resilient-infrastructure

United Nations Office for Disaster Risk Reduction. (2024). The importance of infrastructure resilience for sustainable development. Retrieved from [https://www.undrr.org] (https://www.undrr.org)

Ward, P. J. (2020). Investment in resilient infrastructure for sustainable development. Journal of Sustainable Infrastructure.

World Bank. (2019). Economic impact of infrastructure disruptions. Retrieved from https://www.worldbank.org

Wu, D. (2024). Building Climate Resilience in Infrastructure Projects: A Brief for Investors. https://climate.axa/building-climate-resilience-infrastructure/#:~:text=Studies%20show%20that%20making%20infrastructure,in%20climate%20adaptation%20and%20resilience.

Zhao, X., Zhang, L., Li, H., & Wu, J. (2022). Enhancing infrastructure resilience: Strategies and recommendations. Infrastructure and Disaster Management.

Zio, E. (2016). Challenges in maintaining technological resilience. Systems Engineering Journal.