

## Security and Organisational Performance in Small and Medium-Sized Enterprises (SMEs) in South-South Nigeria

**Dr. Kingsley Ikwunga Amadi**

Department of Business Administration, Faculty of Administration and Management, Rivers State University, Port Harcourt

**ABSTRACT:** This study examines the relationship between security and organisational performance in Small and Medium-sized Enterprises (SMEs) in South-South Nigeria. Against a backdrop of significant industrial activity and evolving cyber threats, the research investigated how safe working hours, cyber security, and employees' emergency orientation influence employee safety, product/stakeholder safety, and employee retention. A quantitative survey design was employed, utilising a structured questionnaire administered to a sample of employees. The data collection instrument was validated through a pilot study, demonstrating high reliability with Cronbach's alpha values exceeding 0.89. Contrary to expectations grounded in stakeholder and socio-technical systems theories, the results from simple linear regression analyses revealed no statistically significant relationships between any of the three security dimensions and the measures of organisational performance. The findings suggest a significant disconnect between formal security practices and their tangible outcomes in this specific context, highlighting a critical implementation gap. The study concludes that for SMEs in South-South Nigeria, the value of security is not inherent in its policies but is contingent upon effective, deeply embedded, and contextually relevant execution. Recommendations are offered for managers and policymakers to bridge this gap.

**KEYWORDS:** Security, Organisational Performance, SMEs, Business, South-South Nigeria

---

### 1. INTRODUCTION

Security in contemporary organisational life extends well beyond the physical perimeter of factories, offices and worksites. In the South-South region of Nigeria, where industrial activity, port-related logistics, oil and gas operations and an expanding services sector intersect with fragile infrastructure and evolving regulatory frameworks, security has become a multi-dimensional construct that shapes organisational outcomes in complex ways. The present study, titled “Security and Organisational Performance in South-South Nigeria”, interrogates how three interrelated dimensions of security — safe working hours, cyber security and employees' emergency orientation — influence three measures of organisational performance: employee safety, product design and stakeholder safety, and employee retention. By drawing on an integrated conceptual framework that situates occupational and digital security as antecedents to organisational performance, the study seeks to generate empirically grounded policy and managerial prescriptions suited to the socio-economic particularities of South-South Nigeria. The choice of this case region recognises the concentration of critical infrastructure, heightened occupational hazards in extractive industries, and recent cyber incidents affecting African organisations that together make the study both timely and policy relevant (Ekanem, 2024; Collins, 2024).

Organisations operating in South-South Nigeria confront dual security challenges. First, traditional occupational safety risks—long working hours, exposure to hazardous processes and uneven safety culture—persist despite regulatory instruments and international best practice guidance. Second, digitalisation and rapid technological adoption have introduced cyber security vulnerabilities while many workplaces are yet to fully inculcate emergency preparedness culture among employees. These twin vulnerabilities undermine organisational performance in measurable ways: they increase accident rates and work-related ill-health, compromise product and stakeholder safety through flawed processes or cyber-enabled breaches, and erode employee morale and retention (Kolus, Wells & Neumann, 2023; Behm & Pearce, 2017). At the policy level, Nigeria has made strides toward legal frameworks that strengthen the cyber frontier, but implementation gaps and capacity constraints continue to blunt their effectiveness (Nwankwo, 2025; Njogu, 2020). Within organisations, the absence of coherent linkage between work-schedule design, cyber resilience and emergency orientation weakens internal controls that protect persons and products alike. Consequently, organisations in the South-South face productivity losses, reputational risk and higher staff turnover—outcomes that hinder competitiveness and socio-economic

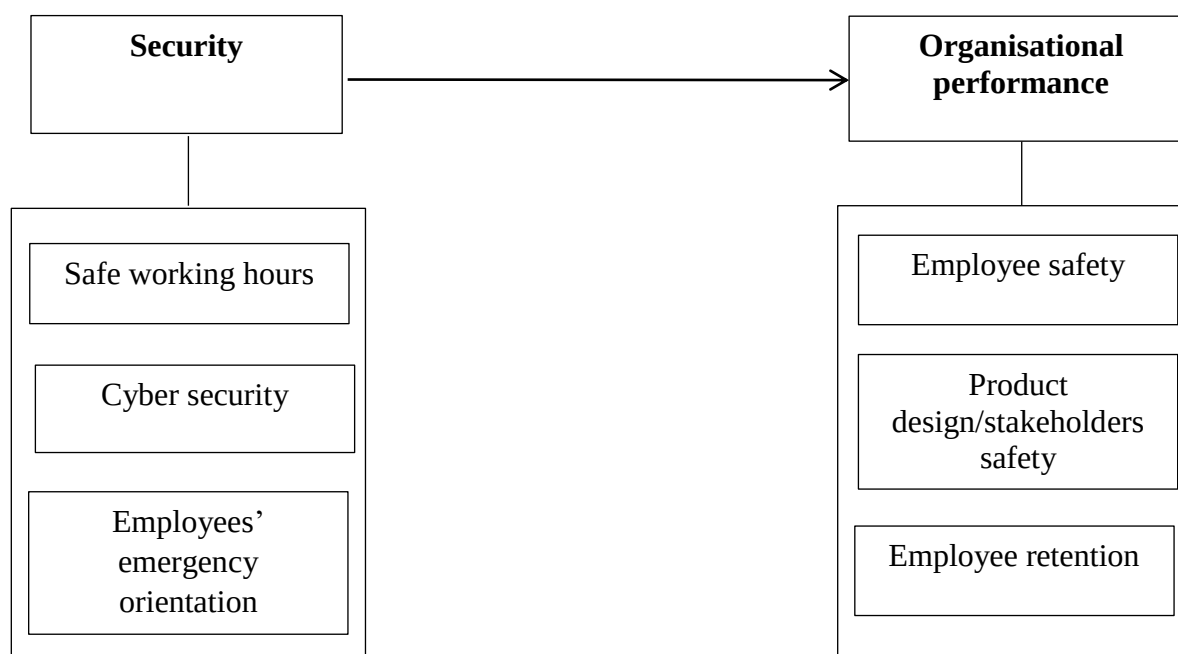
## Security and Organisational Performance in Small and Medium-Sized Enterprises (Smes) in South-South Nigeria

development in a region reliant on stable operations. The problem this study addresses, therefore, is the paucity of empirical evidence that integrates safe working hours, cyber security and employee emergency orientation into a single explanatory model for organisational performance within the South-South context. Existing studies tend to examine these factors in isolation or focus on other regions and industries, leaving a contextual evidence gap for policy-makers and managers in this geopolitically important sub-national region of Nigeria.

Therefore, the aim of this paper is to examine security and organisational performance in South-South, Nigeria, with specific focus on SMEs.

Hence, the conceptual framework was deduced:

**Figure 1: Conceptual Framework for the Relationship between Security and Organisational Performance in South-South, Nigeria**



**Source: Adapted and Modified from Azapagic (2003); Geerts and Dooms (2020); Khan *et al.* (2024a&b); Elbir (2025); Haque *et al.* (2025); Nwankwo (2025)**

Security the predictor variable has the following dimensions (safe working hours, cyber security and employees emergency orientation) adapted and modified from (Elbir, 2025; Haque *et al.*, 2025; Nwankwo, 2025), while the measures of organisational performance – the criterion variable include (employee safety, product design/stakeholders safety and employee retention), adapted and modified from (Azapagic, 2003; Geerts & Dooms, 2020; Khan *et al.*, 2024a&b).

Thus, the hypotheses proposed includes:

- H<sub>01</sub>: Safe working hours does not have a significant relationship with employee safety in SMEs in South-South, Nigeria.
- H<sub>02</sub>: Safe working hours does not have a significant relationship with product design/stakeholders safety in SMEs in South-South, Nigeria.
- H<sub>03</sub>: Safe working hours does not have a significant relationship with employee retention safety in SMEs in South-South, Nigeria.
- H<sub>04</sub>: Cyber security does not have a significant relationship with employee safety in SMEs in South-South, Nigeria.
- H<sub>05</sub>: Cyber security does not have a significant relationship with product design/stakeholders safety in SMEs in South-South, Nigeria.
- H<sub>06</sub>: Cyber security does not have a significant relationship with employee retention safety in SMEs in South-South, Nigeria.
- H<sub>07</sub>: Employees emergency orientation does not have a significant relationship with employee safety in SMEs in South-South, Nigeria.
- H<sub>08</sub>: Employees emergency orientation does not have a significant relationship with product design/stakeholders safety in SMEs in South-South, Nigeria.

## Security and Organisational Performance in Small and Medium-Sized Enterprises (Smes) in South-South Nigeria

H<sub>09</sub>: Employees emergency orientation does not have a significant relationship with employee retention safety in SMEs in South-South, Nigeria.

This study concentrates on organisations within the South-South geopolitical zone of Nigeria. The geographical and sectoral scope includes firms and institutions that span the private and public sectors and formalised non-governmental organisations operating in urban and peri-urban settings across the six states that constitute South-South Nigeria. The temporal scope privileges contemporary dynamics, emphasising post-pandemic shifts to hybrid working, the accelerated adoption of digital tools, and emergent occupational health trends observed in the 2020s. Conceptually, the study is delimited to three security dimensions—safe working hours, cyber security and employees' emergency orientation—and three organisational performance measures—employee safety, product design and stakeholder safety, and employee retention. The operational focus is on how variations in security practices and policies across organisations predict differences in these performance measures. The study excludes detailed technical audits of physical plant and cyber architecture; rather it emphasises organisational practices, policies, employee perceptions and aggregate performance indicators that are amenable to survey and qualitative investigation. While recognising the broader political economy influences (for example, national infrastructure policy and international supply-chain dynamics), the study prioritises organisational-level determinants to ensure actionable managerial recommendations.

The significance of the study is threefold. First, it bridges an empirical gap by offering an integrated examination of occupational and cyber security dimensions as joint predictors of organisational performance in a Nigerian sub-national context underrepresented in scholarly discourse. Policymakers and regulatory agencies will benefit from the region-specific evidence base when designing compliance frameworks and enforcement strategies that account for both physical and digital risks (African Development Bank, 2020; African Legal Support Facility, 2019). Second, the study advances managerial practice by identifying which security investments and organisational routines are most strongly associated with improved employee safety, product and stakeholder protection, and staff retention. This has practical implications for human resource management, operations planning and information-security governance: measures such as regulated shift design, employee cyber awareness programmes and routine emergency drills can be prioritised on the basis of demonstrated performance returns (Behm & Pearce, 2017; Haque *et al.*, 2025). Third, by anchoring the analysis within a multi-theoretical literature base that includes stakeholder and systems perspectives, the study contributes theoretically to discussions on how security functions as an antecedent to broader organisational sustainability and resilience, thus informing future research agendas concerning infrastructure-led development and institutional adaptation in volatile economies (Agénor, 2010; Haque *et al.*, 2024).

Two theoretical lenses guide this study: stakeholder theory and socio-technical systems theory. Stakeholder theory posits that organisations perform well when they deliberately identify, consider and manage the legitimate interests of groups that can affect or are affected by organisational activities (Freeman, 1984; Clarkson, 1995). In the present context, stakeholders include employees, consumers, regulators, community members and supply-chain partners. A stakeholder-informed approach reframes security investments—not merely as compliance costs but as strategic actions that secure stakeholder trust, protect the social licence to operate and ultimately enhance performance outcomes (Geerts & Dooms, 2020). Product design and stakeholder safety, therefore, are not peripheral outcomes but central to stakeholder relations: when organisations design products and services with safety in mind and protect stakeholder data and welfare, they strengthen market position and mitigate litigation and reputational risks (Font, Guix & Bonilla-Priego, 2016).

Socio-technical systems theory complements the stakeholder perspective by emphasising the interplay between social (human), technical (tools, processes, digital infrastructure) and organisational elements. Socio-technical thinking highlights that changes in cyber architecture or scheduling policies have cascading effects on worker behaviour, ergonomic risk, and emergency responsiveness (Azapagic, 2003; Kolus *et al.*, 2023). For instance, digital systems that automate shift rostering can reduce fatigue-related incidents only if they are integrated with human-centred scheduling rules and training. Conversely, poorly designed cyber-security systems that frustrate employees may inadvertently encourage unsafe workarounds. Socio-technical systems theory thus provides a conceptual scaffold for investigating how safe working hours, cyber security and employee emergency orientation are co-constitutive determinants of employee safety, product/stakeholder protection and retention. Hence, the following conceptual review:

Security in organisations is a multi-faceted construct encompassing physical, organisational and informational domains. In this study, three operational dimensions are foregrounded: safe working hours, cyber security and employees' emergency orientation. Safe working hours refer to organisational scheduling policies, overtime management, and practices that prevent fatigue and overwork. Safe working hours are a recognized determinant of occupational health; excessive work hours have been linked to musculoskeletal disorders, reduced cognitive functioning and higher accident incidence (Kolus, Wells & Neumann, 2023). Behm and Pearce (2017) have argued that occupational design and scheduling are core to achieving healthy work environments, especially in high-risk industries.

## Security and Organisational Performance in Small and Medium-Sized Enterprises (Smes) in South-South Nigeria

Cyber security denotes the suite of organisational policies, technical safeguards and human-capacity programmes designed to protect information assets, ensure data integrity and secure operational continuity. Cyber threats have become material business risks, and guidance from organisations such as the Cybersecurity and Infrastructure Security Agency emphasises preparedness, basic hygiene and training as critical first-line defences (Cybersecurity and Infrastructure Security Agency, 2023). In the African context, scholars have highlighted the imperative of harmonizing legal instruments with organisational practises to shore up cyber resilience (Njogu, 2020; Nwankwo, 2025). Cyber security intersects with product and stakeholder safety when information breaches or system failures undermine product integrity, end-user safety or supply-chain reliability (Sarkar *et al.*, 2024).

Employees' emergency orientation refers to the degree to which staff are prepared for and responsive to emergent events such as fires, spills, cyber incidents and civil disturbances. This dimension encompasses regular emergency drills, clear evacuation procedures, accessible safety equipment and training that builds situational awareness. Emergency orientation is a behavioural and procedural construct; its efficacy depends on management commitment, clear communication channels and routine practice (Elbir, 2025). Effective emergency orientation reduces response times, minimises harm and helps maintain continuity during crises.

Organisational performance is conceptualised beyond narrow financial metrics to include employee safety, product design and stakeholder safety, and employee retention. Employee safety reflects the organisation's effectiveness in preventing work-related injuries and sustaining worker well-being. Safety outcomes are direct indicators of operational excellence and often serve as proxies for the quality of managerial systems (Behm & Pearce, 2017). Product design and stakeholder safety capture the extent to which products and services are engineered and delivered to prevent harm to consumers and other external actors. This measure integrates quality assurance, compliance with regulatory standards and stakeholder engagement processes (Freeman, 1984; Geerts & Dooms, 2020). Employee retention denotes the organisation's capacity to keep talent and institutional knowledge; it is influenced by job satisfaction, perceived organisational support and the quality of the work environment, including safety and digital-security practices (Kolus *et al.*, 2023).

Linking security dimensions to performance, the argument advanced in this study is that well-governed safe working hours reduce fatigue-related incidents, thereby improving employee safety and supporting retention. Cyber security safeguards prevent disruptions that could compromise product integrity or leak stakeholder-sensitive information, thus protecting stakeholder safety and organisational reputation. Employee emergency orientation reduces the severity of incidents and keeps operations resilient, with downstream benefits for product safety and retention because staff feel cared for and confident in management's crisis competence. These linkages are supported by prior theoretical and empirical work that connects human factors, systems design and stakeholder management to safety and retention outcomes (Kolus *et al.*, 2023; Geerts & Dooms, 2020; Behm & Pearce, 2017).

The empirical literature on security and organisational performance is extensive but fragmented across domains and geographies. Studies on occupational scheduling demonstrate that poorly designed shift systems and excessive overtime raise the risk of musculoskeletal disorders, cognitive errors and workplace injuries (Kolus, Wells & Neumann, 2023). Research on prevention through design suggests that managerial integration of safety at the design stage reduces downstream occupational hazards (Elbir, 2025). In the Nigerian and broader African context, infrastructural inadequacies and sector-specific hazards (such as in oil and gas and logistics) compound the risks associated with unsafe working hours, making regionally tailored approaches necessary (Adeyemo, 2025; Agénor, 2010).

Cyber security scholarship has recently proliferated in response to rapid digital transformation. A systematic literature review by Haque *et al.* (2025) synthesises contemporary cyber risk management approaches in the digital era, emphasising the central role of governance, continuous monitoring and workforce training. Complementary studies highlight the contribution of AI-driven predictive analytics and edge computing to reinforcing cyber defences and enabling real-time protective measures (Islam *et al.*, 2024; Paul *et al.*, 2024). In contexts with nascent regulatory enforcement, such as some African markets, scholars warn that technological solutions must be accompanied by legal innovation and institutional capacity building (Njogu, 2020; Nwankwo, 2025). Empirical reports of notable cyberattacks on African organisations in 2024 illustrate the materiality of these threats and the urgent need for organisational readiness (Ekanem, 2024).

Research on emergency orientation indicates that regular drills, clear signage and accessible equipment are positively associated with reduced incident severity and improved employee confidence (Behm & Pearce, 2017; Elbir, 2025). Studies that adopt a socio-technical lens show that emergency preparedness is most effective when supported by participatory training and integrated with technological systems for detection and alarm (Sufian *et al.*, 2024; Hossain *et al.*, 2024). Cross-cutting empirical evidence also links employee perceptions of safety and organisational trust to retention outcomes. Workers who perceive their organisations as committed to safety — including digital safety — are more likely to remain, reducing turnover costs and preserving institutional knowledge (Kolus *et al.*, 2023; Agénor, 2010).

Despite this growing body of evidence, several empirical gaps persist. First, most studies approach occupational safety, cyber security and emergency preparedness separately. Few investigations adopt an integrated approach that examines how these dimensions jointly influence multiple performance measures within a single organisational setting. Second, there is scant empirical

## Security and Organisational Performance in Small and Medium-Sized Enterprises (Smes) in South-South Nigeria

work that is geographically specific to South-South Nigeria, a region with unique industrial and socio-political characteristics. Third, while global and pan-African reviews highlight the importance of legal and infrastructural foundations for cyber resilience, fewer micro-level organisational studies examine the interaction between legal frameworks, managerial practice and employee-level outcomes in Nigeria (Njogu, 2020; Nwankwo, 2025; Adeyemo, 2025). The present study addresses these gaps by offering an empirically testable model that integrates the three security dimensions and links them to three performance measures, using organisations in South-South Nigeria as an empirical setting.

This study fills an integrative empirical gap by concurrently examining safe working hours, cyber security and employees' emergency orientation as joint predictors of employee safety, product/stakeholder safety and employee retention. In doing so, it responds to calls for socio-technical analyses that connect human factors, digital governance and design-for-safety in contexts of infrastructural volatility and legal transition (Kolus *et al.*, 2023; Haque *et al.*, 2025). By situating the research within South-South Nigeria the study provides contextualised evidence where industrial hazards, port logistics and energy-sector operations intersect with cyber vulnerabilities and governance challenges. Moreover, the study operationalises stakeholder theory in conjunction with socio-technical systems thinking to demonstrate how security investments generate tangible stakeholder benefits—ranging from safer products to higher employee loyalty—thereby re-framing security as a strategic competence rather than a compliance burden (Freeman, 1984; Geerts & Dooms, 2020). The research also contributes to policy debates by mapping where legal and infrastructural reforms (such as those discussed by Nwankwo, 2025, and procedures recommended by the Cybersecurity and Infrastructure Security Agency, 2023) can best complement organisational practices to achieve measurable performance gains.

The theoretical synthesis and empirical review presented above underscore that security, conceived in both occupational and digital terms, is central to organisational performance. Safe working hours reduce fatigue and injury; cyber security safeguards operational integrity and stakeholder trust; and robust emergency orientation mitigates incident severity and sustains operational continuity. These dimensions, deployed coherently, contribute to improved employee safety, safer product design and stakeholder protection, and stronger employee retention. For managers in South-South Nigeria, the implications are pragmatic. Investments in human-centred scheduling, cyber-hygiene and routine emergency drills should be framed as strategic interventions with measurable returns in safety and employee stability. For policymakers, the study suggests that supportive legal innovation, infrastructure investment and capacity building will amplify organisational efforts and reduce systemic vulnerabilities (African Development Bank, 2020; Nwankwo, 2025). For scholars, the integrated conceptual model advanced here opens avenues for mixed-method and longitudinal research that can quantify causal pathways and inform scalable interventions.

In sum, by weaving together stakeholder and socio-technical theoretical lenses with empirical insights drawn from the broader literature, this study offers a comprehensive foundation for empirical investigation of security and organisational performance in South-South Nigeria. The subsequent methodological chapters will operationalise the constructs, articulate hypotheses derived from the conceptual framework, and describe the sampling, instrument and analysis strategies that will produce evidence capable of guiding managerial action and informing policy reform in a region where security and performance are inextricably linked.

## 2. METHODOLOGY

This study adopts a quantitative survey research design to investigate the relationship between security and organisational performance among selected firms in South-South Nigeria. The design is appropriate because it allows for the collection of quantifiable data from a large population to establish correlations between the predictor variable—security—and the criterion variable—organisational performance (Obiwuru *et al.*, 2011). The study population consists of 200 employees across different sectors, including manufacturing, telecommunications, and oil and gas industries, which are major employers within the region. A structured questionnaire based on a 5-point Likert scale is employed as the primary data collection instrument, enabling the measurement of respondents' perceptions regarding security practices and their influence on performance outcomes (Opara *et al.*, 2023).

The questionnaire is divided into two sections. Section A captures demographic information such as gender, age, educational qualification, and years of experience. Section B is divided into six constructs—three dimensions of security (safe working hours, cyber security, and employees' emergency orientation) and three measures of organisational performance (employee safety, product design/stakeholders' safety, and employee retention)—with four items per construct, yielding a total of twenty-four items. A simple random sampling technique is used to select respondents, ensuring equal representation and reducing bias in the selection process (Noor, Tajik & Golzar, 2022).

Data collected was analysed using descriptive and inferential statistics. Descriptive analysis (mean and standard deviation) will summarise respondents' views, while Pearson correlation and simple linear regression analysis through the aid of SPSS v.27 determined the strength and direction of the relationship between security dimensions and organisational performance measures (Elbir, 2025). A pilot study on 68 respondents showed that the validity and reliability of the instrument was established. The reliability was confirmed using Cronbach's alpha, which demonstrated strong internal consistency for the constructs measured. For

## Security and Organisational Performance in Small and Medium-Sized Enterprises (Smes) in South-South Nigeria

instance, the security construct exhibited a Cronbach's alpha of 0.892, with loading factors for its items ranging from 0.701 to 0.849. Similarly, the organisational performance construct showed a high alpha of 0.915, and its item loadings varied between 0.723 and 0.881. These values, all exceeding the accepted threshold of 0.7, confirm that the questionnaire is both a reliable and valid tool for data collection, ensuring the robustness of the subsequent analysis. Ethical considerations such as confidentiality, voluntary participation, and anonymity of responses was strictly adhered to throughout the study (Opara *et al.*, 2023).

### 3. FINDINGS

The simple linear regression analysis provided a rigorous framework for testing the hypothesised relationships. Table 1 gives details the results for each hypothesis, with the  $R^2$  values indicating the proportion of variance explained and the p-values determining statistical significance against the standard benchmark of  $p < 0.05$ .

**Table 1: Regression Results for the Study Examining the Relationship between Security and Organisational Performance in South-South Nigeria**

| Hypothesis            | $R^2$ | F-statistic | p (F-test) | $\beta$ (Coefficient) | t-statistic | p (t-test) | Interpretation                                                                                                                                  |
|-----------------------|-------|-------------|------------|-----------------------|-------------|------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>H<sub>01</sub></b> | 0.013 | 2.56        | 0.111      | 0.111                 | 1.60        | 0.111      | No significant relationship between <i>Safe Working Hours</i> and <i>Employee Safety</i> . Hence, the null hypothesis is retained.              |
| <b>H<sub>02</sub></b> | 0.000 | 0.09        | 0.771      | 0.021                 | 0.29        | 0.771      | No significant relationship between <i>Safe Working Hours</i> and <i>Product/Stakeholders' Safety</i> . Hence, the null hypothesis is retained. |
| <b>H<sub>03</sub></b> | 0.000 | 0.00        | 0.976      | 0.002                 | 0.03        | 0.976      | No significant relationship between <i>Safe Working Hours</i> and <i>Employee Retention</i> . Hence, the null hypothesis is retained.           |
| <b>H<sub>04</sub></b> | 0.000 | 0.08        | 0.775      | -0.020                | -0.29       | 0.775      | No significant relationship between <i>Cyber Security</i> and <i>Employee Safety</i> . Hence, the null hypothesis is retained.                  |
| <b>H<sub>05</sub></b> | 0.006 | 1.12        | 0.292      | 0.077                 | 1.06        | 0.292      | No significant relationship between <i>Cyber Security</i> and <i>Product/Stakeholders' Safety</i> . Hence, the null hypothesis is retained.     |
| <b>H<sub>06</sub></b> | 0.000 | 0.01        | 0.919      | -0.007                | -0.10       | 0.919      | No significant relationship between <i>Cyber Security</i> and <i>Employee Retention</i> . Hence, the null hypothesis is retained.               |

## Security and Organisational Performance in Small and Medium-Sized Enterprises (Smes) in South-South Nigeria

| Hypothesis      | R <sup>2</sup> | F-statistic | p (F-test) | β (Coefficient) | t-statistic | p (t-test) | Interpretation                                                                                                                                                |
|-----------------|----------------|-------------|------------|-----------------|-------------|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| H <sub>07</sub> | 0.001          | 0.11        | 0.741      | -0.023          | -0.33       | 0.741      | No significant relationship between <i>Employees' Emergency Orientation</i> and <i>Employee Safety</i> . Hence, the null hypothesis is retained.              |
| H <sub>08</sub> | 0.003          | 0.58        | 0.446      | 0.056           | 0.76        | 0.446      | No significant relationship between <i>Employees' Emergency Orientation</i> and <i>Product/Stakeholders' Safety</i> . Hence, the null hypothesis is retained. |
| H <sub>09</sub> | 0.001          | 0.25        | 0.618      | 0.034           | 0.50        | 0.618      | No significant relationship between <i>Employees' Emergency Orientation</i> and <i>Employee Retention</i> . Hence, the null hypothesis is retained.           |

Source: Researcher's Survey Data (2025); SPSS v.27 Output

### 4. DISCUSSION

#### The Relationship between Safe Working Hours and the Measures of Organisational Performance in South-South Nigeria

The results indicate that safe working hours do not significantly influence employee safety, product/stakeholder safety, or retention in South-South Nigerian SMEs. This finding, contrary to established theory (Kolus *et al.*, 2023), suggests that within this specific context, formal scheduling policies may be overshadowed by more pressing socio-economic realities. In an environment characterised by high unemployment and informal work arrangements, employees may prioritise income over well-being, accepting excessive hours without complaint. Consequently, the theoretical link between regulated hours and performance is disrupted, implying that managerial interventions must extend beyond policy to address foundational labour market conditions and economic pressures to be effective.

#### The Relationship between Cyber Security and the Measures of Organisational Performance in South-South Nigeria

The analysis reveals no significant relationship between cyber security and the organisational performance measures. This is particularly striking given the increasing digital threats highlighted by scholars like Nwankwo (2025). A plausible explanation for the South-South context is a widespread "compliance gap," where cybersecurity is perceived as a technical or luxury concern, detached from core operational safety and human resource outcomes. For many SMEs, immediate physical challenges and operational costs may overshadow investments in digital hygiene. This finding suggests that the theoretical benefits of cyber resilience are not yet materialising in practice, indicating a need for awareness campaigns that directly connect cyber investments to tangible business continuity and trust.

#### The Relationship between Employees' Emergency Orientation and the Measures of Organisational Performance in South-South Nigeria

The study found that employees' emergency orientation does not significantly affect safety or retention outcomes. This contradicts socio-technical systems theory, which posits that preparedness is integral to operational resilience (Azapagic, 2003). In the Nigerian business environment, this may be due to perfunctory or poorly implemented drills that are seen as tokenistic rather than genuine capacity-building exercises. If training is irregular, poorly communicated, or lacks management commitment, it fails to engender the situational awareness and confidence needed to influence performance metrics. Therefore, the absence of a significant relationship likely points to an implementation deficit rather than the unimportance of preparedness, urging managers to move from box-ticking to embedding a robust safety culture.

### 5. CONCLUSION

This study set out to investigate the critical links between security dimensions—safe working hours, cyber security, and employees' emergency orientation—and organisational performance in SMEs within South-South Nigeria. Contrary to the propositions of

## Security and Organisational Performance in Small and Medium-Sized Enterprises (Smes) in South-South Nigeria

stakeholder and socio-technical systems theories, and despite a methodologically robust instrument, the regression analysis revealed no statistically significant relationships for any of the nine hypotheses tested. The findings suggest that within the unique socio-economic context of South-South Nigeria, the presumed direct pathways from formal security practices to performance outcomes are not operative. This does not necessarily negate the importance of security but indicates a significant implementation gap. It appears that for these SMEs, security measures may be superficial, poorly integrated, or so overshadowed by more immediate operational and survival challenges that their theoretical benefits on safety and retention are not realised. The study concludes that the mere presence of security policies is insufficient; the critical differentiator for performance lies in the depth of implementation, management commitment, and the contextual adaptation of these practices to the complex Nigerian business environment. Based on the findings, the following were recommended:

1. **Move Beyond Policy to Embedded Practice:** Managers should focus on genuinely embedding security cultures rather than just drafting policies. This includes leadership demonstrating commitment to safe working hours, conducting meaningful and regular emergency drills that involve all employees, and integrating cyber hygiene into daily routines to make its relevance clear.
2. **Contextualise Security Investments:** For policymakers and support organisations, initiatives should be designed to help SMEs adapt security practices to local challenges. This could involve developing tailored, low-cost cyber security toolkits and demonstrating through case studies how effective safety protocols directly prevent financial losses, thereby framing security as a strategic investment rather than a compliance cost.
3. **Bridge the Perceptual Gap through Communication:** Organisations must actively communicate the purpose and benefits of security measures to employees. This involves transparently linking safe working practices to personal well-being, explaining how cyber security protects jobs, and ensuring emergency training is engaging and practical to foster buy-in and translate formal procedures into genuine organisational resilience.

## REFERENCES

- 1) Adeyemo, A. (2025). Prospects 2035: Reimagining the Future of Work in Africa (Nigeria as a Case Study). Available at SSRN 5200760.
- 2) African Development Bank. (2020). African Economic Outlook 2020. [www.afdb.org](http://www.afdb.org). <https://www.afdb.org/en/documents/african-economic-outlook-2020>.
- 3) African Legal Support Facility (2019). PPP Country Profile-Nigeria. [www.aflsf.org](http://www.aflsf.org). <https://www.aflsf.org/sites/default/files/PPP%20Country%20Profile%20-%20Nigeria.pdf>.
- 4) Agénor, P.-R. (2010). A theory of infrastructure-led development. *Journal of Economic Dynamics and Control*, 34(5), 932-950.
- 5) Azapagic, A. (2003). Systems approach to corporate sustainability: A general management framework. *Process Safety and Environmental Protection*, 81(5), 303-316.
- 6) Behm, M., & Pearce, A. (2017). Occupational safety and health in green buildings: LEED PtD pilot credit analysis. CPWR Small Study Final Report.
- 7) Clarkson, M. B. E. (1995). A stakeholder framework for analyzing and evaluating corporate social performance. *Academy of Management Review*, 20(1), 92-117.
- 8) Collins, J. (2024, January 27). Nigerian man extradited to the U.S. over sextortion case linked to South Carolina teenager's death. *AP News*. <https://apnews.com/article/832b99698558ccc37beb80d15ea4d83b>
- 9) Cybersecurity and Infrastructure Security Agency (2023). Shields up: Guidance for organizations. [www.cisa.gov](http://www.cisa.gov). <https://www.cisa.gov/shields-up>.
- 10) Ekanem, S. (2024, January 2). 10 major cyberattacks that targeted African organizations in 2024. *Business Insider Africa*. <https://africa.businessinsider.com/local/lifestyle/10-major-cyberattacks-that-targeted-african-organizations-in-2024/qsqgmlq>
- 11) Elbir, U. (2025). The role of human resource management in implementing 'prevention through design' (PtD) strategies to enhance occupational health and safety in the construction industry: A thematic analysis approach. *Business & Management Studies: An International Journal*, 13(3), 1391-1413.
- 12) Font, X., Guix, M., & Bonilla-Priego, M. J. (2016). Corporate social responsibility in cruising: Using materiality analysis to create shared value. *Tourism Management*, 53, 175-186.
- 13) Freeman, R. E. (1984). *Strategic management: A stakeholder approach* [eBook]. Pitman.
- 14) Geerts, M., & Dooms, M. (2020). Sustainability reporting for inland port managing bodies: A stakeholder-based view on materiality. *Sustainability*, 12(5), 1726.

## Security and Organisational Performance in Small and Medium-Sized Enterprises (Smes) in South-South Nigeria

- 15) Haque, G. M. M., Akula, D. K., Mohammed, Y. S., Syed, A., & Arafat, Y. (2025). Cybersecurity risk management in the age of digital transformation: A systematic literature review. *Emerging Frontiers Library for The American Journal of Engineering and Technology*, 7(8), 126-150.
- 16) Haque, S., Sufian, M. A., Al-Samad, K., Faruq, O., Hossain, M. A., Talukder, T., & Shayed, A. U. (2024). Business management in an unstable economy: Adaptive strategies and leadership. *AIJMR*, 2(5). Doi:10.62127/aijmr.2024.v02i05.1084.
- 17) Hossain, S., Khadka, U., Sarkar, S., & Khan, N. (2024). Cyber-physical systems and IoT: Transforming smart cities for sustainable development. *AIJMR*, 2(5). Doi:10.62127/aijmr.2024.v02i05.1106.
- 18) Islam, S. A. M., Sarkar, A., Khan, A. J. M. O., Islam, T., Paul, R., & Bari, M. S. (2024). AI-driven predictive analytics for enhancing cybersecurity in a post-pandemic world: A business strategy approach. *IJFMR*, 6(5). Doi:10.36948/ijfmr.2024.v06i05.28493.
- 19) Khan, M. N., Haque, S., Azim, K. S., Al-Samad, K., Jafor, A. H. M., Aziz, M., Faruq, O., & Khan, N. (2024). Strategic adaptation to environmental volatility: Evaluating the long-term outcomes of business model innovation. *AIJMR*, 2(5). Doi:10.62127/aijmr.2024.v02i05.1079.
- 20) Khan, M. N., Shuv, T., Ont, M. R. H., Khan, N., & Rahman, A. (2024). Artificial intelligence and machine learning as business tools: A framework for diagnosing value destruction potential. *IJFMR*, 6(1). Doi:10.36948/ijfmr.2024.v06i01.23680.
- 21) Kolus, A., Wells, R. P., & Neumann, W. P. (2023). Examining the relationship between human factors related quality risk factors and work related musculoskeletal disorder risk factors in manufacturing. *Ergonomics*, 66(7), 954-975.
- 22) Njogu, M. (2020). Assessing the impact of the Computer Misuse and Cybercrimes Act in Kenya. *Kenyan Journal of Law and Technology*, 4(1), 33–48.
- 23) Noor, S., Tajik, O., & Golzar, J. (2022). Simple random sampling. *International Journal of Education & Language Studies*, 1(2), 78-82.
- 24) Nwankwo, I. S. (2025). Strengthening Nigeria's cyber frontier: building cybersecurity resilience through legal innovation. *The Commonwealth Cyber Journal*, 27.
- 25) Obiwuru, T. C., Okwu, A. T., Akpa, V. O., & Nwankwere, I. A. (2011). Effects of leadership style on organizational performance: A survey of selected small scale enterprises in Ikosi-Ketu council development area of Lagos State, Nigeria. *Australian journal of business and management research*, 1(7), 100-111.
- 26) Opara, V., Ahiauzu, B. E., & Oladipupo, R. O. (2023). Awareness and Use of Big Data Management Systems by Lecturers in Universities in Rivers State, Nigeria. *Library Philosophy and Practice (e-journal)*, 7777, 1-13.
- 27) Paul, R., Islam, S. A. M., Sarkar, A., Khan, A. J. M. O., Islam, T., & Bari, M. S. (2024). The role of edge computing in driving real-time personalized marketing: A data-driven business perspective. *IJFMR*, 6(5). Doi:10.36948/ijfmr.2024.v06i05.28494.
- 28) Sarkar, A., Islam, S. A. M., Khan, A. J. M. O., Islam, T., Paul, R., & Bari, M. S. (2024). Leveraging blockchain for transparent and efficient supply chain management: Business implications and case studies. *IJFMR*, 6(5). Doi:10.36948/ijfmr.2024.v06i05.28492.
- 29) Sufian, M. A., Haque, S., Al-Samad, K., Faruq, O., Hossain, M. A., Talukder, T., & Shayed, A. U. (2024). IoT and data science integration for smart city solutions. *AIJMR*, 2(5). Doi:10.62127/aijmr.2024.v02i05.1086.