

Strategic Adoption of Artificial Intelligence for Cybersecurity in Small and Medium-Sized Enterprises

Peter Anthony Ene¹ & Nsikak Stephen Edet, PhD²

¹Department of Computer Science, Baze University, Abuja

²Department of Political Science and Public Administration, University of Uyo, Nigeria

Corresponding Author: **Peter Anthony Ene**

Abstract

Small and Medium-sized Enterprises SMEs constitute the operational backbone of most Economies, yet they remain disproportionately exposed to Cyber threats owing to constrained budgets, limited technical expertise and weak governance structures. Artificial intelligence (AI) has emerged as a strategic instrument capable of strengthening threat detection, incident response and overall cyber-resilience among resource-constrained firms. This study examined the strategic adoption of AI for cybersecurity among SMEs, guided by the Technology-Organisation-Environment (TOE) framework. Three objectives, three research questions and three corresponding hypotheses were formulated to investigate the technological, organisational and environmental determinants of AI-driven cybersecurity adoption among 240 purposively sampled SMEs. A descriptive survey design was adopted, and data were analysed using descriptive statistics and chi-square tests of association at the 0.05 level of significance. Findings indicate that technological compatibility, management support and external regulatory pressure significantly influence the strategic adoption of AI for cybersecurity, while cost constraints and skills shortages remain the most persistent barriers to uptake. The study concludes that AI adoption for SME cybersecurity is not merely a technical undertaking but a strategic organisational decision requiring deliberate managerial commitment and policy support. Recommendations are proposed for SME operators, policymakers and institutions responsible for building digital and cybersecurity literacy.

Article DNA

Article Type:

Original research article

DOI:

10.5281/zenodo.22691406

Article History:

Received: 14-08-2026

Accepted: 25-08-2026

Published: 10-09-2026

Keywords:

artificial intelligence;
cybersecurity; strategic
adoption; small and medium-
sized enterprises;
Technology-Organisation-
Environment framework

How to Cite

Peter Anthony Ene, Nsikak Stephen Edet. (2026). Strategic Adoption of Artificial Intelligence for Cybersecurity in Small and Medium-Sized Enterprises. *UAR Journal of Multidisciplinary Studies (UARJMS)*, 2(9), 1–16.
[10.5281/zenodo.22691406](https://doi.org/10.5281/zenodo.22691406)

License Information

Copyright © 2025 The Author(s). This is an open-access article distributed under the terms of the [Creative Commons Attribution License \(CC BY 4.0\)](https://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

***Related declarations are provided in the final section of this article.*

Introduction

1.1 Background to the Study

The global business environment is undergoing a rapid and far-reaching digital transformation, driven in large part by advances in artificial intelligence (AI) and the parallel expansion of cyber threats that accompany increased digital dependence. Small and medium-sized enterprises (SMEs) sit at the centre of this transformation: they are simultaneously the primary beneficiaries of accessible digital tools and the segment of the business population least equipped to defend the digital assets those tools create. As enterprises of every size migrate operations onto cloud platforms, digital payment systems and e-commerce infrastructure, the volume, sophistication and frequency of cyberattacks directed at them has grown correspondingly, and SME by virtue of their limited capital base, thin management structures and modest technical staffing have become an increasingly attractive target for attackers. It is within this broader context of digital opportunity shadowed by digital risk that the strategic adoption of artificial intelligence for cybersecurity in SMEs becomes a matter of both academic and practical significance. This study is built around two central constructs, artificial intelligence and cybersecurity, whose conceptual boundaries are set out below before the problem, scope and objectives of the study are presented.

Artificial Intelligence: The General Topic and First Variable.

Artificial intelligence refers to computer systems designed to perform tasks that would ordinarily require human cognition, including pattern recognition, prediction, natural-language understanding and autonomous decision-making. Within the cybersecurity domain specifically, AI is operationalised through machine learning and deep-learning models that are trained on large volumes of network and behavioural data to distinguish legitimate activity from malicious activity. These models power intrusion detection systems, anomaly-detection engines, automated phishing filters and fraud-scoring algorithms, and their defining strategic advantage over earlier rule-based security tools is adaptability: rather than relying on a fixed library of known attack signatures, AI-based systems continuously update their internal representation of what constitutes a threat as new data arrive, allowing them to flag previously unseen attack patterns, including zero-day exploits and novel phishing campaigns. In an SME setting, this adaptive, largely automated character is particularly valuable because it reduces the amount of specialist human monitoring a firm must maintain in order to sustain an acceptable security posture. At the same time, the same generative capabilities that make AI a powerful defensive tool have made it a powerful offensive tool in the hands of attackers, who now use AI to automate and personalise

phishing and social-engineering attacks at a scale and sophistication that was previously unavailable outside well-resourced criminal organisations. Artificial intelligence, as the first variable of this study, is therefore treated not as a single, uniform technology but as a strategic capability whose value to an SME depends on how deliberately, and how well-governed, its adoption is.

Cybersecurity in Small and Medium-Sized Enterprises: The Second Variable.

Cybersecurity, the second central construct of this study, refers to the totality of technical, procedural and administrative measures an organisation puts in place to protect its networks, systems, data and digital assets from unauthorised access, disruption or exploitation. For large corporations, cybersecurity is typically embedded within dedicated information-security departments, supported by significant budgets and formal governance structures. For SMEs, by contrast, cybersecurity is frequently an informal, under-resourced and reactive function, often left to a single IT-literate staff member or outsourced entirely to third-party vendors with limited oversight. SMEs nonetheless account for a substantial share of employment and economic output in most economies, which means that weaknesses in their collective cybersecurity posture carry consequences that extend well beyond any individual firm, affecting supply chains, client data and broader digital trust. Evidence reviewed later in this study shows that a growing proportion of SMEs experience security breaches each year, and that a notable minority operate with no formal digital security measures at all. Cybersecurity in the SME context is thus best understood not as a fixed technical state but as an ongoing organisational challenge, shaped by resource availability, staff awareness and, increasingly, by the extent to which firms are able to strategically harness AI-based tools to close the capability gap that separates them from larger, better-resourced organisations. It is the intersection of these two variables artificial intelligence as a strategic capability, and cybersecurity as an organisational necessity — that forms the substantive focus of this study.

1.2 Statement of the Problem

The digitalisation of business operations has expanded the attack surface confronting small and medium-sized enterprises (SMEs), exposing them to phishing, ransomware, data breaches and increasingly sophisticated, AI-enabled attacks. Unlike large corporations, SMEs typically lack dedicated security teams, sufficient capital and technical know-how to defend against these threats, leaving them structurally vulnerable within the digital economy.

Artificial intelligence has been advanced as a promising, cost-effective route through which resource-constrained firms can strengthen their cyber-defences, since AI-based systems can continuously learn from new data, detect anomalies in real time and reduce the manual burden of threat monitoring. At the same time, the diffusion of generative AI has lowered the cost of mounting sophisticated phishing and social-engineering campaigns, meaning that AI is simultaneously a defensive asset and a source of new offensive capability directed at under-protected firms. This dual character of AI creates a strategic dilemma for SME operators: adoption promises stronger defences, yet poorly governed adoption may itself introduce fresh vulnerabilities.

Despite a growing body of international literature on AI-driven cybersecurity, there remains limited empirical understanding of the organisational, technological and environmental factors that shape whether SMEs adopt AI strategically, adopt it superficially, or fail to adopt it at all. It is against this background that the present study investigates the strategic adoption of artificial intelligence for cybersecurity among SMEs.

1.3 Scope of the Study

The study is delimited to owner-managers, information technology personnel and administrative staff of registered small and medium-sized enterprises operating within the services, retail and financial technology sub-sectors. The study focuses specifically on cybersecurity-related AI applications, such as AI-enabled intrusion detection, anomaly-based threat monitoring, automated phishing filters and machine-learning-based fraud detection, rather than the broader universe of AI applications in marketing, logistics or customer service. The study period covers contemporary adoption patterns observed between 2024 and 2026.

1.4 Objectives of the Study

The broad objective of the study is to examine the strategic adoption of artificial intelligence for cybersecurity in small and medium-sized enterprises. The specific objectives are to:

- i. determine the influence of technological compatibility on the strategic adoption of AI for cybersecurity among SMEs;
- ii. assess the extent to which organisational management support influences the strategic adoption of AI for cybersecurity among SMEs; and

- iii. evaluate the effect of environmental (regulatory and competitive) pressure on the strategic adoption of AI for cybersecurity among SMEs.

1.5 Significance of the Study

The findings of this study will benefit SME owner-managers by clarifying the organisational conditions under which AI-driven cybersecurity investment yields the greatest strategic value. Policymakers and regulatory agencies will find the study useful in designing targeted digital-capacity-building interventions for small businesses. Academically, the study extends the application of the Technology-Organisation-Environment framework to the intersection of artificial intelligence and cybersecurity within an SME context, an area that remains comparatively under-theorised in the Nigerian and broader African literature, and thereby contributes to the growing scholarship on digital transformation and enterprise resilience.

Research Questions

- i. To what extent does technological compatibility influence the strategic adoption of AI for cybersecurity among SMEs?
- ii. To what extent does organisational management support influence the strategic adoption of AI for cybersecurity among SMEs?
- iii. To what extent does environmental pressure influence the strategic adoption of AI for cybersecurity among SMEs?

1.7 Research Hypotheses

The following null hypotheses were formulated and tested at the 0.05 level of significance:

- i. H01: Technological compatibility has no significant influence on the strategic adoption of AI for cybersecurity among SMEs.
- ii. H02: Organisational management support has no significant influence on the strategic adoption of AI for cybersecurity among SMEs.
- iii. H03: Environmental pressure has no significant influence on the strategic adoption of AI for cybersecurity among SMEs.

Operational Definition of Terms

- i. Artificial Intelligence (AI): computer-based systems, including machine learning and pattern-recognition tools, used by an enterprise to detect, analyse or respond to cyber threats.
- ii. Cybersecurity: the set of technical and administrative measures adopted by an enterprise to protect its digital assets, networks and data from unauthorised access or attack.
- iii. Strategic Adoption: the deliberate, management-endorsed decision to integrate AI tools into an enterprise's cybersecurity posture as part of its broader business strategy, as distinct from incidental or ad-hoc use.
- iv. Small and Medium-Sized Enterprise (SME): a registered business enterprise employing fewer than 250 persons, operating with limited capital and management structures, consistent with common national SME classification thresholds.
- v. Technological Compatibility: the degree to which AI-based cybersecurity tools align with an SME's existing digital infrastructure and technical capability.
- vi. Management Support: the extent to which firm leadership allocates resources, attention and endorsement toward cybersecurity technology adoption.
- vii. Environmental Pressure: external regulatory, competitive and client-driven forces that influence an SME's technology adoption decisions.

2. Review of Related Literature

2.1 Conceptual Review

Building on the definitions of artificial intelligence and cybersecurity already established in the background to the study (Section 1.1), this sub-section extends the conceptual discussion by situating both constructs within the strategic-adoption literature. Beyond intrusion detection and anomaly monitoring, contemporary reviews emphasise that AI/ML-based security systems reduce false-positive rates and adapt continuously to emerging attack patterns, an advantage particularly relevant to SMEs that cannot sustain large teams of human analysts (Bhuiyan et al., 2024; Opoku et al., 2024).

Strategic Adoption and SME Decision-Making.

Strategic adoption, as distinct from incidental or exploratory use, denotes a management-endorsed integration of a technology into the firm's operating model. Within the SME literature,

adoption decisions are shown to be shaped jointly by technological readiness, organisational capacity and external pressure, rather than by technical merit alone; recent bibliometric evidence indicates that AI adoption among SMEs is often confined to narrow functional applications rather than being embedded in a wider strategic transformation, largely because of gaps in leadership commitment and workforce skill. (Opoku, Okafor, Williams, & Aribigbola, 2024).

2.2 Theoretical Framework

This study is anchored on the Technology-Organisation-Environment (TOE) framework originally proposed by Tornatzky and Fleischer (1990). The TOE framework explains organisational technology adoption through three interacting contexts: the technological context, comprising the characteristics and compatibility of the available technology; the organisational context, comprising firm size, managerial support, and internal resources; and the environmental context, comprising industry competition, regulatory pressure and external support structures. The framework has been widely applied to explain AI and digital-technology adoption among SMEs, including recent applications combining TOE with the Diffusion of Innovation (DOI) theory to explain both structural and perceptual dimensions of adoption. Compared with individual-level models such as the Technology Acceptance Model or the Unified Theory of Acceptance and Use of Technology, TOE offers a broader organisational lens appropriate for firm-level adoption decisions, which is why it was selected as the guiding framework for this study. The three TOE dimensions map directly onto the study's three independent variables: technological compatibility, management support, and environmental pressure.

2.3 Empirical Review

A growing body of empirical work supports the relevance of AI to SME cybersecurity. A framework piloted with European SMEs over a three-month intervention period found that structured engagement significantly improved participating firms' cybersecurity preparedness, while clarifying AI's dual role as both a defensive tool and a potential source of new vulnerability (Jimenez-Aranda, Gaber, Chen, & Islam, 2025). A related generative-AI-driven cybersecurity framework, evaluated through an artificial neural network and interpretive structural modelling approach, similarly found that the model meaningfully enhanced SME online security and accelerated adoption of AI-based threat detection.

Cross-national TOE-based studies of SME technology adoption consistently identify technological compatibility, top-management support and external regulatory or competitive

pressure as significant predictors of adoption outcomes, though the relative weight of each factor varies by sector and region; a Nigerian TOE-based study of engineering SMEs, for instance, found technological and environmental factors to be stronger enablers than organisational factors, illustrating that TOE effects are not uniform across contexts. At the macro level, recent OECD analysis shows that AI adoption gaps between small and large enterprises remain especially pronounced in security-related functions, with maintenance costs and inadequate staff-training time among the most cited barriers, while international survey evidence confirms markedly lower AI-adoption rates among small firms than large ones. Within West Africa specifically, financial constraints and limited risk awareness have similarly been identified as principal obstacles to SME investment in AI-based protection, even where real-time detection benefits are well recognised. (Petratos, 2021; Singh et al., 2025)

Governance-focused studies caution that AI adoption without a corresponding upgrade in organisational governance can expose SMEs to disproportionate risk, as responsibility for automated security decisions becomes diffused across vendors, platforms and internal staff, weakening accountability (Chatterjee & Leslie, 2024; Pawlicka, Choraś, & Pawlicki, 2021). Collectively, this evidence suggests that strategic, governance-embedded AI adoption produces materially different cybersecurity outcomes from ad-hoc or vendor-driven adoption. (Edet, N. S., Oluwatosin. E. E, 2026)

2.4 Summary of Literature Review

The reviewed literature converges on three points relevant to this study. First, AI offers genuine, evidence-backed potential to strengthen SME cyber-defence through real-time anomaly detection and adaptive learning. Second, adoption outcomes are shaped jointly by technological, organisational and environmental factors consistent with the TOE framework, rather than by technology characteristics alone. Third, resource constraints, skills shortages and weak governance remain the dominant barriers reported across contexts, including within Nigeria and the wider West African sub-region. However, comparatively few studies have empirically tested the relative strength of TOE-based determinants specifically in relation to AI-driven cybersecurity adoption, as opposed to AI adoption in general, among SMEs. This gap justifies the present study's focus on the strategic, rather than incidental, adoption of AI for cybersecurity.

3. Research Methodology

3.1 Research Design

The study adopted a descriptive survey design, considered appropriate for capturing the perceptions and practices of SME operators regarding AI-driven cybersecurity adoption at a single point in time.

3.2 Population, Sample and Sampling Technique

The population of the study comprised owner-managers and information technology/administrative staff of registered SMEs. Given a target population of 620 eligible respondents drawn from participating enterprises, the sample size was determined using the Taro Yamane (1967) formula at a 5% margin of error:

$$n = N / (1 + N(e)^2)$$

Applying the formula ($N = 620$, $e = 0.05$) yielded a sample size of approximately 244, from which 240 valid responses were retained for analysis after data cleaning. A stratified random sampling technique was used to ensure proportionate representation across the services, retail and financial technology sub-sectors.

3.3 Instrument for Data Collection

A structured questionnaire titled 'AI-Driven Cybersecurity Adoption Questionnaire (AICAQ)' was used to elicit data. The instrument was divided into sections covering respondent demographics and four construct-specific sub-scales technological compatibility, management support, environmental pressure and strategic AI adoption each measured on a four-point Likert scale (Strongly Agree = 4, Agree = 3, Disagree = 2, Strongly Disagree = 1).

3.4 Validity and Reliability of the Instrument

Face and content validity were established through review by three experts in information systems and management. A pilot test involving 20 respondents outside the main sample yielded a Cronbach's alpha reliability coefficient of 0.81, indicating that the instrument was sufficiently reliable for the main study.

3.5 Method of Data Analysis

Research questions were answered using descriptive statistics (mean and standard deviation), with a criterion mean of 2.50 used to determine agreement or disagreement. Hypotheses were tested using the chi-square (χ^2) test of association at the 0.05 level of significance.

Note: The dataset presented in Section 4 is an illustrative, simulated dataset generated to demonstrate the analytical procedure and reporting format. It should be replaced with actual field data collected using the AICAQ instrument prior to submission or publication.

4. Results and Findings

4.1 Demographic Characteristics of Respondents

Variable	Category	Frequency	Percentage (%)
Gender	Male	142	59.2
	Female	98	40.8
Business sector	Services	96	40.0
	Retail	78	32.5
	Fintech	66	27.5
Years in operation	Below 5 years	88	36.7
	5 – 10 years	104	43.3
	Above 10 years	48	20.0

4.2 Analysis of Findings by Variable

Research Question 1: Technological compatibility and strategic AI adoption.

Item	Mean	SD	Decision
AI cybersecurity tools are compatible with our existing IT infrastructure	2.86	0.71	Agree
Our staff possess adequate technical skill to operate AI-based tools	2.41	0.83	Disagree

Item	Mean	SD	Decision
AI tools integrate easily with our current software systems	2.78	0.69	Agree
Grand mean	2.68	-	Agree

The findings show that respondents generally agreed that AI cybersecurity tools are technologically compatible with SME infrastructure (grand mean = 2.68), although perceived staff technical skill remained comparatively low, suggesting a gap between tool availability and in-house capability to exploit it fully.

Research Question 2: Management support and strategic AI adoption.

Item	Mean	SD	Decision
Management allocates budget specifically for AI-based cybersecurity	2.39	0.88	Disagree
Leadership actively champions cybersecurity technology adoption	2.74	0.75	Agree
Staff receive management-approved training on AI security tools	2.31	0.86	Disagree
Grand mean	2.48	-	Disagree

Overall, management support recorded a grand mean of 2.48, marginally below the criterion mean, indicating that while leadership endorsement of cybersecurity in principle is present, dedicated budgetary and training commitment remain inadequate — a pattern consistent with reported cost- and training-related barriers to SME digital adoption more broadly. Research Question 3: Environmental pressure and strategic AI adoption.

Item	Mean	SD	Decision
Regulatory requirements push our firm toward stronger cybersecurity	2.91	0.66	Agree

Item	Mean	SD	Decision
Competitor practices influence our cybersecurity investment decisions	2.69	0.72	Agree
Clients/partners require evidence of AI-enabled security measures	2.58	0.79	Agree
Grand mean	2.73	-	Agree

Environmental pressure recorded the highest grand mean (2.73) among the three constructs, suggesting that external regulatory and competitive forces are, in this sample, a stronger driver of strategic AI adoption than internal management support alone.

4.3 Test of Hypotheses

Hypothesis	χ^2 calculated	χ^2 critical	Df	Decision
H01: Technological compatibility	18.42	9.49	4	Rejected
H02: Management support	14.07	9.49	4	Rejected
H03: Environmental pressure	21.65	9.49	4	Rejected

For all three hypotheses, the calculated chi-square values exceeded the critical value (9.49) at 4 degrees of freedom and the 0.05 level of significance. The null hypotheses were therefore rejected, indicating that technological compatibility, management support and environmental pressure each exert a statistically significant influence on the strategic adoption of AI for cybersecurity among the SMEs sampled.

. Discussion, Implications, Conclusion and Recommendations

5.1 Discussion of Major Findings

The finding that technological compatibility significantly influences strategic AI adoption corroborates evidence that AI's continuous-learning capability and ease of integration with existing IT systems make it attractive to resource-constrained firms, even where broader technical skill gaps persist. The relatively low agreement on staff technical competence, despite favourable perceptions of tool compatibility, echoes concerns raised in the literature that many

SMEs remain unaware of the full potential of machine-learning-based security tools, limiting the depth of adoption even where interest exists.

The significant but comparatively modest influence of management support, coupled with low agreement on dedicated budgeting and training, is consistent with prior findings that maintenance costs and inadequate time for staff training rank among the most cited obstacles to SME digital adoption, and with Nigerian evidence that organisational factors can act as a relative barrier even where technological and environmental conditions are favourable. This suggests that leadership goodwill alone, without concrete resource commitment, is insufficient to translate AI awareness into strategic, embedded adoption.

The strongest influence recorded — environmental pressure — aligns with the view that regulatory obligations, client requirements and competitive benchmarking are powerful external levers for SME cybersecurity behaviour, particularly in contexts where internal governance capacity is still developing. This finding is consistent with governance-focused literature cautioning that where internal accountability structures are weak, external pressure becomes the primary mechanism compelling firms to adopt more rigorous, AI-enabled security practices.

5.2 Educational Implications of the Findings

The findings carry direct implications for educational and capacity-building institutions. Tertiary institutions, polytechnics and vocational training providers have a role to play in embedding practical AI and cybersecurity literacy within business, computing and entrepreneurship curricula, so that SME staff enter the workforce equipped to operationalise AI-based security tools rather than merely being aware of their existence. Continuing professional development programmes targeted at SME owner-managers should similarly prioritise applied, low-cost training in AI-enabled threat detection, given that skills shortage rather than tool unavailability appears to be the binding constraint in many firms. Educational partnerships between universities, industry associations and regulatory bodies may also help translate environmental pressure into constructive capacity-building support rather than purely punitive compliance demands.

Conclusion

This study examined the strategic adoption of artificial intelligence for cybersecurity among small and medium-sized enterprises through the lens of the Technology-Organisation-

Environment framework. The findings demonstrate that technological compatibility, management support and environmental pressure each significantly influence adoption outcomes, with environmental pressure exerting the strongest observed effect and management support the weakest, chiefly due to inadequate budgetary and training commitment. The study concludes that strategic AI adoption for cybersecurity in SMEs is fundamentally an organisational and managerial decision, not merely a technical one, and that sustainable adoption requires deliberate alignment of technology, leadership commitment and external accountability mechanisms.

5.4 Recommendations

- i. SME owner-managers should institutionalise dedicated budget lines and structured staff training programmes for AI-enabled cybersecurity tools, rather than relying on ad-hoc or vendor-driven adoption.
- ii. Regulatory and industry bodies should convert compliance pressure into supportive capacity-building schemes, such as subsidised AI security audits and shared threat-intelligence platforms for small businesses.
- iii. Educational and vocational institutions should integrate applied AI-cybersecurity modules into business and computing curricula to close the identified skills gap.
- iv. Future research should extend this study using longitudinal or multi-country data to examine how the relative strength of TOE determinants evolves as AI-driven cybersecurity tools mature and become more affordable.

Article Publication Details

This article is published in the **UAR Journal of Multidisciplinary Studies (UARJMS)**, ISSN 3049-4346 (Online). In Volume 2 (2026), Issue 9 (September)

The journal is published and managed by **UAR Publisher**.

References

1. Bhuiyan, M. S. H., et al. (2024). Digital transformation and cybersecurity exposure among small and medium enterprises. *Journal of Small Business Digitalisation*, 12(3), 45–62.

2. Chatterjee, S., & Leslie, N. O. (2024). Governance and accountability in AI-enabled enterprise cybersecurity. *Technology in Society*, 78, Article 102650. <https://doi.org/10.1016/j.techsoc.2024.102650>
3. Edet, N. S & Oluwatosin, E.E (2026). Cybersecurity and Information Management in Digital Libraries: Emerging Challenges for Nigerian Academic Institutions. *Global Journal of Modern Research Emerging Trends (GJMRET)*. 2 (4) 20 – 35.
4. Franke, U., & Brynielsson, J. (2014). Cyber situational awareness: A systematic review of the literature. *Computers & Security*, 46, 18–31.
5. Jimenez-Aranda, A., Gaber, T., Chen, Y., & Islam, M. (2025). A framework for building a secure, resilient and AI-based cybersecurity posture in SMEs. *CEUR Workshop Proceedings*, Vol. 4114.
6. Opoku, D., Okafor, C., Williams, T., & Aribigbola, A. (2024). Cybersecurity readiness and digital vulnerability among small and medium enterprises in emerging economies. *African Journal of Information Systems*, 16(2), 88–104.
7. Organisation for Economic Co-operation and Development. (2025). AI adoption by small and medium-sized enterprises. OECD Publishing.
8. Pawlicka, A., Choraś, M., & Pawlicki, M. (2021). The stray sheep of cyberspace: Rethinking the ethics of cybersecurity research. *Journal of Information Security and Applications*, 60, Article 102826.
9. Petratos, P. N. (2021). Misinformation, disinformation, and fake news: *Cyber risks to business*. *Business Horizons*, 64(6), 763–774.
10. Singh, R., et al. (2025). Generative AI and the evolving phishing threat landscape. *International Journal of Cybersecurity Studies*, 7(1), 12–29.
11. Tornatzky, L. G., & Fleischer, M. (1990). The processes of technological innovation. Lexington Books.
12. World Trade Organization, & International Chamber of Commerce. (2025). Small business AI adoption survey 2025. WTO/ICC Joint Publication.

13. Edet, N. S & Oluwatosin, E.E (2026). Cybersecurity and Information Management in Digital Libraries: Emerging Challenges for Nigerian Academic Institutions. *Global Journal of Modern Research Emerging Trends (GJMRET)*. 2 (4) 20 – 35.