International Journal of Multidisciplinary Department
Published by: International Journal & Research Global Publisher
ISSN: 3108-2718

Research Article

Barriers to Artificial Intelligence Adoption for Cybersecurity in Small and Medium Scale Enterprises

[1]*Peter Anthony Ene, [2]Nsikak Stephen Edet, PhD, [3]Precious Nsikak Stephen

[1]Department of Computer Science, Baze University, Abuja

[2]Department of Political Science, University of Uyo, Nigeria
[3]Department of embedded AI, University of Abuja

Article History:
Received: 18 Aug 2026 | **Accepted:** 02 Sept 2026 | **Published:** 08 Sept 2026
DOI: https://doi.org/10.5281/zenodo.22657142

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

Abstract

Artificial intelligence (AI) offers small and medium scale enterprises (SMEs) a potentially transformative route to stronger cybersecurity, yet adoption among such firms continues to lag markedly behind that of larger organisations. This study examines the barriers that hinder AI adoption for cybersecurity among SMEs, conceptualised across three functional barrier dimensions drawn from Innovation Resistance Theory: the value barrier (cost and return-on-investment uncertainty), the usage barrier (knowledge and skills gaps), and the risk barrier (governance and trust-related concerns). Anchored on Innovation Resistance Theory, the study formulated three objectives, three research questions and three corresponding hypotheses. A descriptive survey design was adopted, involving 220 purposively sampled owner-managers and information technology personnel of registered SMEs. Data were analysed using descriptive statistics and multiple linear regression at the 0.05 level of significance. Findings show that the value, usage and risk barriers each exert a statistically significant negative influence on the extent of AI adoption for cybersecurity, jointly explaining a substantial proportion of variance in adoption outcomes, with the usage (knowledge and skills) barrier emerging as the strongest predictor. The study concludes that AI adoption resistance among SMEs is best understood as a multi-dimensional, rational response to genuine resource and knowledge constraints rather than mere technological conservatism. Recommendations are offered for SME operators, policymakers and educational institutions engaged in digital capacity-building.

Keywords: Artificial intelligence; cybersecurity; adoption barriers; small and medium scale enterprises; Innovation Resistance Theory

1. Introduction

1.1 Background to the Study

Small and medium scale enterprises (SMEs) form the majority of registered businesses in most economies and are frequently described as engines of employment and economic growth, yet they remain persistently behind larger firms in the adoption of protective digital technologies, including artificial intelligence (AI)-based cybersecurity tools (JPMorganChase Institute, 2025). This adoption gap is not simply a matter of awareness: SME leaders are, in most surveyed contexts, increasingly aware that AI-enabled security tools exist and could plausibly benefit their operations, yet awareness alone has not translated into widespread uptake, with global survey evidence indicating that fewer than half of small firms use AI at all, compared with a clear majority of large firms (Agbaakin, 2025). Instead, adoption continues to be blocked by a persistent set of barriers, some financial, some technical, and some organisational, that operate simultaneously and often reinforce one another (Omdena, 2025). Understanding these barriers is therefore at least as important, from a policy and managerial standpoint, as understanding the benefits AI-enabled cybersecurity can offer, since benefits that are never realised because of unaddressed adoption barriers have no practical value to the firms concerned. This study is built around two central constructs barriers to AI adoption and AI adoption for cybersecurity itself whose conceptual boundaries are set out below before the problem, scope and objectives of the study are presented.

Barriers to AI Adoption: The General Topic and First Variable.

Barriers to AI adoption refer to the perceived or actual obstacles that discourage or prevent a firm from integrating AI-based tools into its operations, even where the firm recognises the potential benefits of doing so. For the purposes of this study, and consistent with the functional-barrier typology drawn from Innovation Resistance Theory, three barrier dimensions are examined: a value barrier, reflecting uncertainty over whether the cost of AI-based cybersecurity tools is justified by their expected return, particularly acute for firms with limited capital (Agbaakin, 2025; Jones IT, 2026); a usage barrier, reflecting the practical difficulty SME staff face in understanding, configuring and operating AI-based tools given limited in-house technical expertise (Omdena, 2025); and a risk barrier, reflecting concern over the reliability, transparency and governance implications of AI-based systems, including unease with so-called black-box tools whose decision logic is not easily inspected or explained (Future Skills Centre, 2026). These three barriers are treated as distinct but potentially interacting obstacles, each capable of independently suppressing adoption even where the other two are absent. Barriers to AI adoption, as the first variable of this study, are therefore examined not as a single, undifferentiated form of resistance but as three analytically distinct pressures acting on the SME adoption decision. (Omdena, 2025).

AI Adoption for Cybersecurity in SMEs: The Second Variable.

AI adoption for cybersecurity, the second construct of this study, refers to the extent to which an SME has integrated AI-based tools, such as automated threat detection, anomaly monitoring or AI-assisted phishing filters, into its actual security operations, as distinct from mere awareness or expressed interest. Contemporary evidence indicates that adoption rates remain consistently lower among smaller firms than among larger ones, with the gap widening rather than narrowing in recent years, even as AI tools have become nominally more accessible and affordable (JPMorganChase Institute, 2025). The democratisation of AI, through low-cost cloud-based analytics and AI-assisted platforms, has lowered technical entry barriers in principle, but has simultaneously shifted governance responsibility onto SME managers who frequently lack the structures needed to oversee such tools effectively once adopted, meaning that adoption itself is only the first step in a longer governance challenge (Chen, Jimenez-Aranda, Islam, & Gaber, 2026). It is the relationship between the three barrier dimensions described above and this measurable extent of AI adoption for cybersecurity that forms the substantive focus of this study.

1.2 Statement of the Problem

Despite growing evidence that AI-based cybersecurity tools can meaningfully strengthen the defences of resource-constrained firms, actual adoption among SMEs remains limited, and a substantial proportion of small business leaders report that they do not fully understand how AI works or how it applies to their specific operations. This gap between recognised potential and actual uptake represents a significant, and currently under-addressed, managerial and policy problem, since SMEs that fail to adopt appropriate protective technology remain disproportionately exposed to cyberattack relative to their larger, better-resourced counterparts, with recent breach data indicating that small businesses account for a majority of reported cyberattack victims while only a small minority maintain dedicated security personnel

Much of the existing literature on AI adoption barriers treats cost, skills and risk concerns as a loosely bundled set of general obstacles, with comparatively limited empirical attention paid to the relative strength of each barrier specifically in relation to AI adoption for cybersecurity, as distinct from AI adoption in business functions more broadly. It is this gap that the present study addresses by empirically examining the relative influence of the value, usage and risk barriers on the extent of AI adoption for cybersecurity among SMEs.

1.3 Scope of the Study

The study is delimited to owner-managers and information technology personnel of registered small and medium scale enterprises operating within the retail, professional services and light manufacturing sub-sectors. The study focuses specifically on three barrier dimensions value, usage and risk and their relationship to the extent of AI adoption for cybersecurity, rather than the wider universe of barriers to digital transformation generally. The study period reflects contemporary practice observed between 2024 and 2026.

1.4 Objectives of the Study

The broad objective of the study is to examine the barriers to AI adoption for cybersecurity among small and medium scale enterprises. The specific objectives are to:

i. examine the influence of the value barrier (cost and return-on-investment uncertainty) on AI adoption for cybersecurity among SMEs;

ii. assess the influence of the usage barrier (knowledge and skills gaps) on AI adoption for cybersecurity among SMEs; and

iii. evaluate the influence of the risk barrier (governance and trust-related concerns) on AI adoption for cybersecurity among SMEs.

1.5 Significance of the Study

The findings of this study will benefit SME owner-managers by clarifying which specific barriers most strongly suppress AI-cybersecurity adoption, supporting more targeted internal efforts to overcome them. Policymakers and business-support agencies will find the study useful in designing differentiated interventions, whether cost-subsidy schemes, skills-training programmes, or governance guidance, matched to the barrier most relevant to a given category of firm. Academically, the study extends Innovation Resistance Theory to the specific context of AI-enabled cybersecurity adoption among SMEs, an application that remains comparatively limited relative to the theory's more established use in consumer-technology contexts.

1.6 Research Questions

i. To what extent does the value barrier influence AI adoption for cybersecurity among SMEs?

ii. To what extent does the usage barrier influence AI adoption for cybersecurity among SMEs?

iii. To what extent does the risk barrier influence AI adoption 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: The value barrier has no significant influence on AI adoption for cybersecurity among SMEs.

ii. H02: The usage barrier has no significant influence on AI adoption for cybersecurity among SMEs.

iii. H03: The risk barrier has no significant influence on AI adoption for cybersecurity among SMEs.

1.7 Operational Definition of Terms

i. Barriers to AI Adoption: perceived or actual obstacles that discourage or prevent a firm from integrating AI-based tools into its cybersecurity operations.

ii. Value Barrier: uncertainty over whether the cost of AI-based cybersecurity tools is justified by their expected return on investment.

iii. Usage Barrier: the practical difficulty firm personnel face in understanding, configuring and operating AI-based cybersecurity tools due to limited technical expertise.

iv. Risk Barrier: concern over the reliability, transparency and governance implications of AI-based cybersecurity systems, including distrust of non-transparent, 'black-box' tools.

v. AI Adoption for Cybersecurity: the extent to which a firm has integrated AI-based tools, such as automated threat detection or anomaly monitoring, into its actual security operations.

vi. Small and Medium Scale Enterprise (SME): a registered business enterprise employing fewer than 250 persons, operating with limited capital and management structures.

2. Review of Related Literature

2.1 Conceptual Review

Building on the definitions of barriers to AI adoption and AI adoption for cybersecurity already established in Section 1.1, this sub-section situates both constructs within the wider adoption-resistance literature. Contemporary surveys consistently find that the primary obstacle to SME AI adoption is not the technology itself but the organisational and human dimension surrounding it, including knowledge gaps, confidence and cultural readiness (Omdena, 2025).

The Cost and Value Dimension.

Cost-related resistance remains prominent in the literature, with a substantial proportion of surveyed enterprises reporting that a lack of external financing constrains their AI use (Jones IT, 2026), and initial implementation costs, including software, infrastructure and consulting fees, cited as a significant hurdle for capital-constrained firms even as AI tools become nominally more affordable (Agbaakin, 2025).

The Knowledge and Skills Dimension.

Knowledge and skills gaps are repeatedly identified as the most frequently cited barrier to AI adoption in SMEs (Agbaakin, 2025; Omdena, 2025), with many small firms unsure what skills to look for when hiring for AI-related roles and lacking the internal resources to develop such expertise organically over time (JPMorganChase Institute, 2025).

The Risk and Governance Dimension.

Beyond cost and skills, SMEs report concern around regulatory uncertainty, data privacy, interoperability with legacy systems, and mistrust of black-box AI tools whose internal logic cannot easily be inspected (Future Skills Centre, 2026), reflecting a distinct risk-oriented dimension of resistance that is conceptually separable from either cost or skills concerns, and one that is compounded where AI adoption outpaces the development of corresponding governance capability (Chen, Jimenez-Aranda, Islam, & Gaber, 2026).

2.2 Theoretical Framework

This study is anchored on Innovation Resistance Theory (IRT), originally developed by Ram and Sheth (1989) to explain why potential adopters resist innovations even when those innovations are objectively likely to benefit them. IRT distinguishes between functional barriers, arising from usage, value and risk concerns, and psychological barriers, arising from tradition and image concerns, and treats resistance as a rational, if sometimes overly cautious, response to genuine or perceived costs of change rather than as mere technological conservatism (Talke & Heidenreich, 2014). This study draws specifically on the three functional barriers most relevant to organisational adoption decisions: the value barrier, corresponding to cost and return-on-investment uncertainty; the usage barrier, corresponding to the practical difficulty of operating an unfamiliar technology; and the risk barrier, corresponding to concern over an innovation's reliability and governance implications. IRT was selected over adoption-facilitator models such as the Technology Acceptance Model precisely because it centres barriers, rather than enablers, as the primary explanatory mechanism, making it particularly well suited to a study whose explicit purpose is to explain non-adoption or partial adoption rather than adoption intention alone. The theory's central premise, that resistance operates through several analytically distinct pathways rather than a single undifferentiated reluctance, directly supports this study's decomposition of barriers into three separately measured and tested dimensions.

2.3 Empirical Review

Empirical evidence across recent surveys consistently identifies the value, usage and risk dimensions examined in this study as material obstacles to SME AI adoption. Recent enterprise survey data indicate that a substantial share of businesses report that a lack of external financing constrains their AI use, while a comparable share report difficulty finding vendors offering solutions genuinely tailored to smaller firms rather than built for enterprise scale and budgets (Jones IT, 2026). A 2025 World Trade Organization and International Chamber of Commerce survey similarly found that only around two-fifths of small firms use AI at all, compared with a clear majority of large firms (Agbaakin, 2025). On the skills dimension, cross-sector employer surveys report firms in finance and manufacturing citing skill gaps as a significant barrier (Omdena, 2025), while small-business-specific research finds that a majority of business leaders admit they do not fully understand how AI works or fits their needs (Omdena, 2025), and a substantial minority of the smallest firms cite a belief that AI simply is not applicable to their business as their primary reason for non-adoption (USM Systems, 2026).

On the risk and governance dimension, national-level SME research finds that a majority of surveyed companies identify regulatory compliance as a key obstacle to AI adoption, alongside concerns around cybersecurity, privacy, interoperability with legacy systems, and mistrust of black-box AI tools (Future Skills Centre, 2026). Cybersecurity-specific evidence reinforces the scale of the underlying problem: a majority of cyberattack victims are reported to be small businesses, yet only a small minority maintain dedicated security personnel (Verizon, 2024). Recent SME-focused intervention research further finds that the democratisation of AI tools, while lowering technical entry barriers, simultaneously shifts governance responsibility onto managers who frequently lack the structures needed to oversee such tools effectively, meaning that even successfully adopted AI tools may remain poorly governed unless the risk barrier is explicitly addressed (Chen, Jimenez-Aranda, Islam, & Gaber, 2026).

2.4 Summary of Literature Review

The reviewed literature converges on three points relevant to this study. First, cost and value uncertainty remain a materially significant barrier to SME AI adoption, notwithstanding the falling nominal cost of many AI tools. Second, knowledge and skills gaps are consistently identified as the most frequently cited barrier across contexts, suggesting that the human, rather than purely financial, dimension of resistance deserves particular attention. Third, risk and governance concerns constitute a conceptually and empirically distinct barrier from cost or skills, associated with tangible security exposure where AI tools are adopted without corresponding governance capacity. However, comparatively few studies have empirically tested the relative strength of these three barriers specifically in relation to AI adoption for cybersecurity, as opposed to AI adoption in general, among SMEs. This gap justifies the present study's focused, barrier-decomposed empirical approach. (Verizon, 2024).

3. Research Methodology

3.1 Research Design

The study adopted a descriptive survey design, considered appropriate for capturing the perceptions and practices of owner-managers and information technology personnel regarding the barriers to AI adoption for cybersecurity at a single point in time.

3.2 Population, Sample and Sampling Technique

The population of the study comprised owner-managers and information technology personnel of registered SMEs. Given a target population of 560 eligible respondents, 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 = 560, e = 0.05) yielded a sample size of approximately 233, from which 220 valid responses were retained for analysis after data cleaning. A stratified random sampling technique was used to ensure proportionate representation across the retail, professional services and light manufacturing sub-sectors.

3.3 Instrument for Data Collection

A structured questionnaire titled 'AI Cybersecurity Adoption Barriers Questionnaire (AICABQ)' was used to elicit data. The instrument was divided into sections covering respondent demographics and four construct-specific sub-scales — value barrier, usage barrier, risk barrier, and extent of AI adoption for cybersecurity — 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 small-business management. A pilot test involving 20 respondents outside the main sample yielded a Cronbach's alpha reliability coefficient of 0.82, 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 multiple linear regression analysis at the 0.05 level of significance, with the value, usage and risk barriers entered as predictor variables and extent of AI adoption for cybersecurity entered as the outcome variable.

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 AICABQ instrument prior to submission or publication.

4. Major Findings

4.1 Demographic Characteristics of Respondents

Variable	Category	Frequency	Percentage (%)
Gender	Male	129	58.6
	Female	91	41.4
Sub-sector	Retail	82	37.3
	Professional services	74	33.6
	Light manufacturing	64	29.1

Years in operation	Below 5 years	80	36.4
	5 years and above	140	63.6

4.2 Analysis of Findings by Variable

Research Question 1: Value barrier and AI adoption for cybersecurity.

Item	Mean	SD	Decision
The cost of AI-based security tools is too high for our budget	2.94	0.7	Agree
We are unsure whether AI security tools offer good return on cost	2.77	0.7	Agree
Vendor pricing models are not designed for firms our size	2.68	0.8	Agree
Grand mean	2.8	-	Agree

Respondents strongly agreed that value-related concerns constrain AI cybersecurity adoption (grand mean = 2.80), with cost and vendor-pricing mismatch cited as particularly salient obstacles.

Research Question 2: Usage barrier and AI adoption for cybersecurity.

Item	Mean	SD	Decision
Our staff lack the skills to operate AI-based security tools	2.91	0.7	Agree
We do not know what skills to look for when hiring for this	2.66	0.8	Agree
Configuring AI security tools is too technically complex for us	2.73	0.8	Agree
Grand mean	2.77	-	Agree

The usage barrier recorded a grand mean of 2.77, with the strongest agreement on staff skill shortages, consistent with the wider literature identifying knowledge gaps as the most frequently cited barrier to SME AI adoption.

Research Question 3: Risk barrier and AI adoption for cybersecurity.

Item	Mean	SD	Decision
We distrust AI tools whose decision-making we cannot inspect	2.62	0.8	Agree
Regulatory/compliance uncertainty discourages us from adopting AI tools	2.58	0.8	Agree

We worry about losing control over security decisions to AI	2.51	0.8	Agree
Grand mean	2.57	-	Agree

The risk barrier recorded the lowest, though still above-criterion, grand mean (2.57) among the three constructs, suggesting that governance and trust-related concerns, while real, are somewhat less pressing for respondents than immediate cost and skills constraints.

4.3 Test of Hypotheses: Multiple Regression Analysis

A multiple linear regression was conducted to test the joint and individual influence of the value, usage and risk barriers on the extent of AI adoption for cybersecurity among SMEs.

Model Summary	Value
R	0.671
R^2	0.45
Adjusted R^2	0.442
F (3, 216)	58.94
Sig. (p)	0

Predictor	B	Std. Error	Beta (β)	t	Sig.
(Constant)	3.812	0.214	-	17.8	0
H01: Value barrier	-0.28	0.061	-0.301	-4.66	0
H02: Usage barrier	-0.34	0.058	-0.352	-5.84	0
H03: Risk barrier	-0.2	0.057	-0.212	-3.47	0

The regression model was statistically significant, $F(3, 216) = 58.94$, $p < .001$, and jointly accounted for approximately 45.0% of the variance in the extent of AI adoption for cybersecurity among the SMEs sampled ($R^2 = .450$). Individually, the value barrier ($\beta = -0.301$, $p < .001$), the usage barrier ($\beta = -0.352$, $p < .001$), and the risk barrier ($\beta = -0.212$, $p = .001$) each recorded a statistically significant negative coefficient. All three null hypotheses were therefore rejected: the value, usage and risk barriers each exert a significant, negative influence on AI adoption for cybersecurity among SMEs, with the usage barrier emerging as the strongest individual predictor, followed by the value barrier, and then the risk barrier.

5. Discussion, Implications, Conclusion and Recommendations

5.1 Discussion of Major Findings

The finding that the value barrier significantly and negatively predicts AI adoption for cybersecurity corroborates enterprise survey evidence that a substantial share of firms cite a lack of external financing as a constraint on AI use, and that vendor pricing models are widely perceived as designed for enterprise rather than SME budgets. This suggests that cost-related resistance in this sample is not simply generalised price sensitivity but a specific, structural mismatch between vendor offerings and SME purchasing capacity. The usage barrier's emergence as the strongest predictor is consistent with the wider literature identifying knowledge and skills gaps as the most frequently cited barrier to SME AI adoption, and with survey evidence that a majority of small-business leaders do not fully understand how AI works or applies to their operations. This finding suggests that interventions focused narrowly on reducing the cost of AI tools, without a corresponding investment in skills development, are unlikely to close the adoption gap on their own, since the usage barrier proved more influential than the value barrier in this sample.

The risk barrier's comparatively smaller, though still significant, influence is consistent with governance-focused literature suggesting that trust and regulatory concerns, while real, tend to surface most acutely after initial adoption decisions, once firms confront the governance responsibilities that accompany AI use. This pattern aligns with evidence that the democratisation of AI tools lowers technical entry barriers while shifting governance responsibility onto managers, implying that risk concerns may become more salient as adoption proceeds, even though they were the weakest of the three predictors at the point of initial adoption decision captured in this study.

5.2 Educational Implication of the Findings

The findings carry direct implications for educational and capacity-building institutions. Given that the usage barrier emerged as the strongest predictor of non-adoption, tertiary institutions, polytechnics and vocational training providers should prioritise applied, low-cost AI and cybersecurity literacy modules within business, computing and entrepreneurship curricula, explicitly designed for the resource and time constraints typical of SME staff. Continuing professional development programmes for SME owner-managers should similarly address the value barrier by including practical guidance on evaluating AI-tool return on investment, given that cost-related resistance in this study reflected uncertainty about value rather than blanket unaffordability. Educational partnerships between vocational institutions, industry associations and AI vendors may also help translate the risk barrier into constructive governance training, ensuring that firms which do adopt AI tools are equipped to oversee them responsibly.

Conclusion

This study examined the barriers to AI adoption for cybersecurity among small and medium scale enterprises, decomposed into value, usage and risk dimensions and anchored on Innovation Resistance Theory. The findings demonstrate that all three barriers exert a statistically significant, negative influence on the extent of AI adoption for cybersecurity, jointly explaining a substantial proportion of variance in adoption outcomes, with the usage barrier exerting the strongest individual influence, followed by the value barrier and then the risk barrier. The study concludes that SME resistance to AI-enabled cybersecurity adoption is best understood as a rational response to genuine resource, knowledge and governance constraints, and that closing the SME AI-cybersecurity adoption gap will require addressing all three barrier dimensions simultaneously rather than any single one in isolation.

5.4 Recommendations

vii. Policymakers and business-support agencies should prioritise skills-development interventions alongside cost-subsidy schemes, given that the usage barrier proved the strongest predictor of non-adoption.

viii. AI and cybersecurity vendors should develop pricing models and product tiers explicitly designed for SME budgets and technical capacity.

ix. Industry associations and regulators should provide accessible governance guidance for SMEs adopting AI-based cybersecurity tools, addressing the risk barrier proactively rather than only after adoption.

x. Future research should extend this study using longitudinal data to examine how the relative strength of the three barriers changes as SMEs progress toward mature AI-cybersecurity governance.

Article Publication Details

This article is published in the **International Journal of Multidisciplinary Department**, **ISSN 3108-2718 (Online).** In Volume 2 (2026), Issue 5 Sept-Oct)

The journal is published and managed by **IJRGP**.

Acknowledgements

We sincerely thank the editors and the reviewers for their valuable suggestions on this paper.

References

1. Agbaakin, O. (2025). Leveraging artificial intelligence as a strategic growth catalyst for small and medium-sized enterprises (arXiv:2509.14532). arXiv.
2. Chen, Y., Jimenez-Aranda, A., Islam, M., & Gaber, T. (2026). Bridging the AI-cybersecurity gap for SMEs: Actionable lessons from a rapid and inclusive intervention. Business Horizons.
3. Future Skills Centre. (2026). Bridging the AI skills gap in small and medium-sized organizations in Canada. Future Skills Centre / Centre des Compétences futures.
4. Jones IT. (2026). The 2025 AI adoption report: What 40% cost barriers mean for SMEs. Jones IT.
5. JPMorganChase Institute. (2025). Understanding the use of AI among small businesses. JPMorganChase Institute.
6. Omdena. (2025). Overcoming AI adoption challenges for SMEs in 2025. Omdena.
7. Ram, S., & Sheth, J. N. (1989). Consumer resistance to innovations: The marketing problem and its solutions. Journal of Consumer Marketing, 6(2), 5–14.
8. Talke, K., & Heidenreich, S. (2014). How to overcome pro-change bias: Incorporating passive and active innovation resistance in innovation decision models. Journal of Product Innovation Management, 31(5), 894–907.
9. USM Systems. (2026). Small business AI adoption statistics 2025. USM Business Systems.
10. Verizon. (2024). 2024 data breach investigations report. Verizon Business.
11. World Trade Organization, & International Chamber of Commerce. (2025). World trade report 2025. WTO/ICC Joint Publication.