Journal of People and Worldviews (JPW)

Volume 1, Number 2

Empirical Article https://doi.org/10.5281/zenodo.21133913 Open Access

Cybersecurity Knowledge Deficits, Information Management Failures, and Organizational Moderators Among Small and Medium-Sized Enterprises in Lagos, Nigeria

Abstract

This study evaluated the effect of cybersecurity awareness on the information management practices of small and medium-sized enterprises (SMEs) in Lagos, Nigeria. A quantitative descriptive survey design was adopted, with data collected from 331 valid respondents drawn from SMEs across three major Lagos business districts using a multistage stratified sampling technique. The adapted Human Aspects of Information Security Questionnaire (HAIS-Q) served as the primary data collection instrument. Findings revealed a moderate overall cybersecurity awareness level (M = 3.03) among SME employees, with incident reporting constituting the most acutely deficient focus area. Information management practices were found to be broadly inadequate (M = 2.41), with incident response, backup and recovery recording the most severe deficits. A statistically significant, moderately strong positive relationship was established between cybersecurity awareness and information management practices (r = 0.618, p < .001), with awareness accounting for approximately 38% of the variance in practice scores. Hierarchical moderated regression analysis revealed that training availability, leadership support, and formal cybersecurity policy significantly amplify the behavioral dividend of higher awareness levels, while resource constraints attenuate it. The study concluded that awareness is a pivotal but institutionally conditioned determinant of information management quality in Lagos SMEs.

Keywords: Cybersecurity awareness, information management practices, Protection Motivation Theory, HAIS-Q

Jude Chinonso Njoku
Shorelands British Academy
0009-0004-2264-8235

Ugonna Onyedikachukwu Chukwueke
Ahmadu Bello University Zaria
0009-0005-8601-9857

Date Received: 24th May, 2026

Date Accepted: 06th May, 2026

Introduction

Small and medium-sized enterprises (SMEs) occupy a peculiar and increasingly vulnerable position in the global digital landscape. They are, on the one hand, the backbone of most developing economies, contributing substantially to employment, gross domestic product, and industrial diversification, while on the other hand, they remain disproportionately exposed to cybersecurity risks owing to constrained resources, limited technical expertise, and inadequate institutional frameworks for protecting the information assets that underpin their

operations (Bada & Nurse, 2019; Ngoqo & Flowerday, 2015). As business processes become ever more reliant on digital technologies, the manner in which SMEs manage their information; how it is collected, stored, processed, shared, and protected increasingly determines their operational resilience, competitive viability, and long-term sustainability.

Cybersecurity awareness, broadly defined as the extent to which individuals within an organization understand, appreciate, and act in accordance with the security risks, policies, and protective behaviours relevant to their digital environment, has emerged as a foundational element of effective information management (Parsons *et al.*, 2017; Tran *et al.*, 2021). Information management, in turn, encompasses the systematic governance of an organization's information resources throughout their entire lifecycle, including the acquisition, organization, maintenance, retrieval, dissemination, and disposal of information in ways that support organizational objectives, regulatory compliance, and stakeholder accountability (Choo, 2014; Liao *et al.*, 2021). When employees lack adequate awareness of cybersecurity threats and best practices, information management systems become susceptible to breaches, unauthorized access, data corruption, and a host of other vulnerabilities that can fundamentally undermine an organization's information integrity and operational continuity (Siponen & Vance, 2010; Zwilling *et al.*, 2022).

Ransomware attacks, phishing campaigns, social engineering exploits, insider threats, and sophisticated malware have proliferated at a pace that has consistently outrun the defensive capabilities of most organizations, particularly those operating with limited cybersecurity budgets and expertise (ENISA, 2023; IBM Security, 2023). The consequences of cybersecurity incidents are often disproportionately severe for SMEs. A single significant breach can result in financial losses, reputational damage, loss of customer trust, regulatory penalties, and in some cases, business closure (Bada & Nurse, 2019; Alahmari & Duncan, 2020). The National Bureau of Statistics (2021) estimates that SMEs account for approximately 96% of all businesses and contribute nearly 50% of Nigeria's gross domestic product. Lagos, as Nigeria's commercial capital and the largest city in sub-Saharan Africa, hosts the highest concentration of SMEs across multiple sectors, including fintech, retail, manufacturing, professional services, media, healthcare, and logistics (LCCI, 2022). The rapid digitalization of business operations in Lagos has dramatically increased the volume and sensitivity of digital information that SMEs now manage daily, yet this has not been matched by commensurate growth in cybersecurity awareness or information management sophistication, leaving a

Citation: Njoku, Jude Chinonso & Chukwueke, Ugonna Onyedikachukwu. "Cybersecurity Knowledge Deficits, Information Management Failures, and Organizational Moderators Among Small and Medium-Sized Enterprises in Lagos, Nigeria". *Journal of People and Worldviews (JPW),* 2026: pp158-174.

significant and widening vulnerability gap (Aderibigbe *et al.*, 2022).

Statement of the Problem

Despite growing scholarly attention to cybersecurity in organizations, studies specifically evaluating how cybersecurity awareness shapes information management practices within SMEs in Nigeria remain limited. Studies show that while 89.8% of Nigerian SMEs are aware of the term "cybersecurity," only 9.1% have received formal training (Ngoqo & Flowerday, 2015; Aderibigbe *et al.*, 2022). Most available studies either focus on large enterprises or examine cybersecurity practices without adequately examining their downstream effects on information management quality and outcomes. This study addresses the identified gap by systematically evaluating the effect of cybersecurity awareness on information management practices of SMEs in Lagos, Nigeria.

Research Questions

This study is guided by the following research questions:

1. What is the level of cybersecurity awareness among employees of SMEs in Lagos, Nigeria?
2. What are the prevailing information management practices of SMEs in Lagos, Nigeria?
3. What is the effect of cybersecurity awareness on the information management practices of SMEs in Lagos, Nigeria?
4. What organizational factors moderate the relationship between cybersecurity awareness and information management practices in SMEs in Lagos, Nigeria?

Objectives of the Study

The specific objectives of this study are as follows:

1. To assess the level of cybersecurity awareness among employees of SMEs in Lagos, Nigeria.
2. To examine the prevailing information management practices of SMEs in Lagos, Nigeria.
3. To evaluate the effect of cybersecurity awareness on the information management practices of SMEs in Lagos, Nigeria.
4. To identify the organizational factors that moderate the relationship between cybersecurity awareness and information management practices in SMEs in Lagos, Nigeria.

Literature Review

Cybersecurity Awareness

Cybersecurity awareness is not a monolithic construct but a multidimensional one encompassing cognitive, attitudinal, and behavioral dimensions that together determine how effectively individuals contribute to, or

Citation: Njoku, Jude Chinonso & Chukwueke, Ugonna Onyedikachukwu. "Cybersecurity Knowledge Deficits, Information Management Failures, and Organizational Moderators Among Small and Medium-Sized Enterprises in Lagos, Nigeria". *Journal of People and Worldviews (JPW)*, 2026: pp158-174.

undermine, the security of an organization's information systems (Parsons *et al*., 2017; Zwilling *et al*., 2022). At the cognitive level, cybersecurity awareness encompasses an individual's knowledge of the types of cyber threats that exist, their understanding of how these threats are manifested in everyday digital interactions, and their familiarity with organizational policies, procedures, and best practices (Tran *et al*., 2021). This includes awareness of threat categories such as phishing, social engineering, ransomware, malware, and insider threats, as well as an understanding of how individual behaviors such as clicking on unfamiliar links, using weak passwords, or accessing organizational systems through unsecured networks can expose the organization to these threats. Cognitive cybersecurity knowledge is a necessary, though not sufficient, precondition for protective behavior (Bulgurcu *et al*., 2010; Parsons *et al*., 2017).

The attitudinal dimension refers to the beliefs, values, and orientations that individuals hold toward cybersecurity and toward the protective behaviors that security policies prescribe. Employees who hold positive attitudes toward cybersecurity tend to perceive security-compliant behaviors as worthwhile and consistent with their professional responsibilities, whereas those with negative attitudes may view security requirements as burdensome or unnecessary (Siponen & Vance, 2010). The behavioral dimension encompasses the actual security-related actions and habits that employees exhibit in their day-to-day work such as use of strong passwords, proper handling of sensitive data, recognition and reporting of phishing attempts, and observance of access control protocols (Zwilling *et al*., 2022). The gap between stated security intentions and actual behavior, termed the "knowing-doing gap," remains a persistent challenge that underscores the complexity of translating cognitive awareness into reliable security behavior (Beautement *et al*., 2016; Parsons *et al*., 2017). Unlike large corporations, SMEs rarely have dedicated information security departments, making each employee's awareness level proportionally more consequential as fewer institutional defense layers exist to compensate for individual lapses (Bada & Nurse, 2019; Alahmari & Duncan, 2020).

Information Management Practices

Information management practices refer to the systematic organizational processes, procedures, and behaviors through which enterprises acquire, organize, store, protect, retrieve, share, and dispose of information assets throughout their lifecycle in ways that support operational objectives, ensure data integrity and availability, and promote compliance with applicable regulatory requirements (Choo, 2014; Liao *et al*., 2021). Data classification involves the categorization of information according to its sensitivity, value, and

Citation: Njoku, Jude Chinonso & Chukwueke, Ugonna Onyedikachukwu. "Cybersecurity Knowledge Deficits, Information Management Failures, and Organizational Moderators Among Small and Medium-Sized Enterprises in Lagos, Nigeria". *Journal of People and Worldviews (JPW)*, 2026: pp158-174.

regulatory obligations, enabling organizations to apply appropriate levels of protection to different categories of data (Choo, 2014). Access control refers to the policies and technical mechanisms through which an organization regulates who can access specific information assets, under what conditions, and for what purposes (Siponen & Vance, 2010). In SMEs, it is frequently under-implemented, with employees granted broader system access than their roles require (Alahmari & Duncan, 2020).

Backup and recovery procedures directly determine an organization's ability to maintain operational continuity in the face of cybersecurity incidents or data loss events (IBM Security, 2023). Incident response practices encompass the organizational processes through which cybersecurity incidents are detected, reported, contained, investigated, and resolved (ENISA, 2023). In SMEs, incident response is frequently informal and reactive, with many organizations lacking documented incident response plans, defined response roles, or post-incident review processes (Alahmari & Duncan, 2020). Regulatory compliance behaviors relate to adherence to the Nigeria Data Protection Regulation (2019) and the Nigeria Data Protection Act (2023), both of which impose specific obligations on organizations processing personal data, including requirements for consent, data minimization, storage limitation, security safeguards, and breach notification (Abdulrauf, 2021). Compliance among SMEs remains limited, reflecting limited awareness of regulatory requirements, inadequate technical capacity, and limited enforcement action by supervisory authorities (Abdulrauf, 2021; Aderibigbe *et al*., 2022).

Theoretical Framework

This study is primarily anchored on Protection Motivation Theory (PMT), originally formulated by Rogers (1975) and subsequently applied extensively in the information security domain to explain cybersecurity awareness and compliance behavior (Herath & Rao, 2009; Ifinedo, 2012; Liang & Xue, 2010). According to PMT, individuals facing a potential threat engage in two parallel appraisal processes. One is threat appraisal, through which the individual evaluates the severity and probability of harm if no protective action is taken while the other is coping appraisal, through which the individual evaluates the efficacy of the recommended protective response (response efficacy) and their confidence in their own ability to implement that response (self-efficacy). Protection motivation arises from the interaction of these appraisal processes and drives the adoption of protective information security behaviors (Rogers, 1975). PMT is particularly relevant here because it places individual cognitive appraisal at the center of security behavior, explains why awareness alone is insufficient to guarantee security-compliant behavior, and provides a

Citation: Njoku, Jude Chinonso & Chukwueke, Ugonna Onyedikachukwu. "Cybersecurity Knowledge Deficits, Information Management Failures, and Organizational Moderators Among Small and Medium-Sized Enterprises in Lagos, Nigeria". *Journal of People and Worldviews (JPW)*, 2026: pp158-174.

framework for understanding how organizational conditions enable or constrain the path from awareness to action.

The study also draws on General Deterrence Theory (GDT), which posits that individuals are deterred from engaging in harmful or prohibited behaviors when they perceive that such behaviors are likely to be detected (certainty of sanction) and that the consequences of detection are sufficiently severe (severity of sanction) (D'Arcy *et al*., 2009; Siponen & Vance, 2010). In the SME context, formal deterrence mechanisms are often weak or absent. Many SMEs lack security monitoring infrastructure, minimal formal disciplinary frameworks, and operate in institutional cultures where policy enforcement is inconsistent. Under these conditions, individual cybersecurity awareness and internalized security values become even more important as motivational foundations for security-compliant information management behavior.

Effect of Awareness on Information Management and Organizational Moderators

The relationship between cybersecurity awareness and information management practices is well-established empirically. Employees who receive training on data classification principles are more likely to correctly identify the sensitivity of information they handle and apply appropriate storage and handling procedures (Parsons *et al*., 2017; Liao *et al*., 2021). Higher awareness is associated with stronger adherence to access control protocols, higher incident reporting rates, and shorter detection delays (Bulgurcu *et al*., 2010; IBM Security, 2023; ENISA, 2023). Organizations in which employees are aware of ransomware attacks and data loss events are more likely to maintain regular backup routines and verify backup completeness (IBM Security, 2023).

However, the awareness–behavior relationship is moderated by organizational factors. Leadership commitment creates an institutional environment in which employee awareness more readily translates into protective behavior (Bada & Nurse, 2019; Tran *et al*., 2021). Formal cybersecurity policies provide behavioral frameworks that channel awareness-motivated intentions into specific prescribed actions. Without formal policies, even highly aware employees may be uncertain what their organization specifically requires (Bulgurcu *et al*., 2010; Siponen & Vance, 2010). Resource constraints create a ceiling effect. Employees cannot implement technically demanding security measures if the organization has not invested in enabling infrastructure (Alahmari & Duncan, 2020). Organizational security culture, the shared values and norms shaping how employees respond to security requirements, amplifies the translation of awareness into behavior in supportive environments and suppresses it in

Citation: Njoku, Jude Chinonso & Chukwueke, Ugonna Onyedikachukwu. "Cybersecurity Knowledge Deficits, Information Management Failures, and Organizational Moderators Among Small and Medium-Sized Enterprises in Lagos, Nigeria". *Journal of People and Worldviews (JPW)*, 2026: pp158-174.

indifferent ones (Da Veiga & Eloff, 2010). The level of investment in formal, structured security awareness training is also consistently superior to informally acquired awareness in motivating security-compliant information management behavior (Parsons et al., 2017; Tran *et al.,* 2021).

Methodology

Research Design and Population

A quantitative descriptive survey design was adopted, enabling the systematic collection of data from a representative sample using standardized instruments capable of generating data amenable to statistical analysis and generalization (Creswell & Creswell, 2018). The target population comprised employees of registered SMEs operating within Lagos State, Nigeria, defined in accordance with the SMEDAN classification as organizations employing between 10 and 199 workers and generating annual turnover between ten million and one billion naira. The study focused on SMEs registered with the Lagos Chamber of Commerce and Industry (LCCI) and operating within three major business districts: Lagos Island, Victoria Island/Ikoyi, and Ikeja.

Sample Size, Sampling, and Instrument

A multistage stratified sampling technique was employed, combining stratification by business district for proportional geographic representation with simple random selection of SMEs within each stratum. Table 1 presents the sample allocation.

Table 1
Sample Allocation by Business District

Business District	Sample (n)
Lagos Island	118
Victoria Island/Ikoyi	120
Ikeja	116
Total	354

Source: field (2026).

The primary instrument was a structured questionnaire adapted from the Human Aspects of Information Security Questionnaire (HAIS-Q) validated by Parsons *et al.* (2017). The HAIS-Q is a psychometrically validated instrument designed to measure cybersecurity awareness across knowledge, attitudes, and behavioral intention dimensions across seven focus areas: password management, email use, internet use, social media use, mobile computing, incident reporting, and information handling. The questionnaire comprised five sections: Section A (demographics); Section B (cybersecurity awareness, 35 items across seven focus areas); Section C (information management practices, 25 items across five sub-dimensions); Section D (perceived effect of awareness on practices, 15 items); and Section E (organizational moderating factors, 24 items). All Sections B–E used a five-point

Citation: Njoku, Jude Chinonso & Chukwueke, Ugonna Onyedikachukwu. "Cybersecurity Knowledge Deficits, Information Management Failures, and Organizational Moderators Among Small and Medium-Sized Enterprises in Lagos, Nigeria". *Journal of People and Worldviews (JPW),* 2026: pp158-174.

Likert scale (5 = Strongly Agree; 1 = Strongly Disagree) with a criterion mean of 2.50. Content validity was established through expert review by three Information Science academics. A pilot study with 40 employees in Surulere confirmed internal consistency reliability (Cronbach's $\alpha \geq 0.70$ across all sections; Nunnally, 1978). Data were analyzed using SPSS version 27 with descriptive statistics, Pearson product-moment correlation, simple linear regression, and hierarchical moderated multiple regression (significance threshold: $p < .05$).

Results

Response Rate and Demographic Profile

Of 354 questionnaires distributed, 331 were returned and deemed valid, yielding a response rate of 93.50%, substantially exceeding the 70% benchmark (Creswell & Creswell, 2018). Males constituted 54.68% of the sample; females 45.32%. The dominant age cohort was 26–35 years (36.56%), followed by 36–45 years (31.12%). Bachelor's degree holders dominated the sample at 43.20%; only 2.72% held professional cybersecurity certifications. Administrative staff formed the largest occupational cluster (29.31%), followed by sales and marketing staff (24.77%); technical and IT staff comprised only 12.99%. Fintech and financial services organizations supplied the largest sectoral representation (22.36%). The majority of respondents occupied non-technical roles, precisely the segments of the SME workforce most likely to serve as inadvertent vectors for cybersecurity breaches through everyday behavioral lapses (Verizon, 2023).

Level of Cybersecurity Awareness (Research Question 1)

Table 2 presents the aggregated means and standard deviations for each cybersecurity awareness focus area.

Table 2

Cybersecurity Awareness by Focus Area

Focus Area	No. Items	Mean	SD	Interpretation
Password Management	5	3.41	0.84	Moderate
Email Use	5	3.17	0.91	Moderate
Internet Use	5	3.09	0.87	Moderate
Social Media Use	5	2.86	0.93	Low-Moderate
Mobile Computing	5	2.94	0.89	Low-Moderate
Incident Reporting	5	2.73	0.96	Low
Information Handling	5	3.02	0.88	Moderate
Overall Cybersecurity Awareness	35	3.03	0.61	Moderate

Note. Criterion mean = 2.50. Scores < 2.50 = Low; 2.50–3.49 = Moderate; ≥ 3.50 = High. Source: Field Survey (2026).

The overall cybersecurity awareness mean of 3.03 (SD = 0.61) is above the criterion threshold of 2.50,

Citation: Njoku, Jude Chinonso & Chukwueke, Ugonna Onyedikachukwu. "Cybersecurity Knowledge Deficits, Information Management Failures, and Organizational Moderators Among Small and Medium-Sized Enterprises in Lagos, Nigeria". *Journal of People and Worldviews (JPW)*, 2026: pp158-174.

indicating a moderate but by no means robust awareness level across the study population. Password management returns the highest focus-area mean (M = 3.41, SD = 0.84), reflecting familiarity with password-strength concepts attributable to the ubiquity of password-creation prompts in everyday digital platforms. Email use follows (M = 3.17, SD = 0.91), consistent with relatively broad public discourse around phishing threats. Incident reporting is the weakest focus area (M = 2.73, SD = 0.96). This is a particularly consequential finding given that the capacity to recognize and report security incidents is the organizational last line of defence in many SME environments lacking automated threat detection. Item-level analysis reveals a stark knowing-doing gap within this focus area. Knowing the conceptual importance of prompt reporting (M = 3.41) coexisted with a deeply below-criterion mean of 1.98 for the behavioral item on whether respondents would actually report an uncertain incident immediately. Knowing who to contact also fell below criterion (M = 2.31). These findings align with Zwilling *et al*. (2022) and Parsons *et al*. (2017), who found that incident reporting and information handling consistently recorded the lowest HAIS-Q awareness scores across organizational samples. Siponen and Vance (2010) recognize this pattern as an instance of neutralization-driven non-compliance, in which employees understand the requirement but rationalize inaction through appeals to ambiguity, time pressure, or diffusion of responsibility.

Prevailing Information Management Practices (Research Question 2)

Table 3 presents the sub-dimension means for information management practices.

Table 3

Information Management Practices by Sub-Dimension

Sub-Dimension	No. Items	Mean	SD	Interpretation
Data Classification and Storage	5	2.47	0.94	Low
Access Control	5	2.63	0.88	Moderate
Backup and Recovery	5	2.31	0.97	Low
Incident Response	5	2.19	0.99	Low
Regulatory Compliance	5	2.44	0.91	Low
Overall Information Management	25	2.41	0.73	Low

Note. Criterion mean = 2.50. Source: Field Survey (2026).

The overall information management mean of 2.41 (SD = 0.73) falls below the criterion threshold, indicating that prevailing information management practices are, in aggregate, inadequate. Four of five sub-dimensions' record below-criterion means. Access control is the sole exception (M = 2.63, SD = 0.88), partially explained by everyday digital platform design reinforcing access control norms (Siponen & Vance, 2010). Incident response returns the weakest sub-dimension mean (M = 2.19, SD = 0.99); every item falls below criterion, with the

Citation: Njoku, Jude Chinonso & Chukwueke, Ugonna Onyedikachukwu. "Cybersecurity Knowledge Deficits, Information Management Failures, and Organizational Moderators Among Small and Medium-Sized Enterprises in Lagos, Nigeria". *Journal of People and Worldviews (JPW)*, 2026: pp158-174.

lowest being 2.07 for the item that documented incident response plans are largely absent. For backup and recovery, only the existence of regular backup schedules (M = 2.58) exceeds criterion. Periodic testing of backups (M = 2.09) is acutely deficient. The ENISA (2023) threat landscape report specifically identifies this gap. Organizations that maintain backups without testing maintain a false sense of security, as untested backups frequently fail at the moment of greatest need. These findings are consistent with Alahmari and Duncan (2020), who found that backup and recovery preparedness and incident response capability were consistently the most underdeveloped information management dimensions across small organizations globally, and with Aderibigbe *et al.* (2022), who documented comparable deficits across Nigerian SME populations.

Effect of Cybersecurity Awareness on Information Management Practices (Research Question 3)

Respondents' perceptions of the directional relationship between cybersecurity awareness and information management yielded an overall mean of 3.31 (SD = 0.71), above the criterion threshold. The effect was most strongly perceived in the domain of access control (M = 3.47, SD = 0.87), where awareness of credential-sharing risks most directly influences protective behaviors. Table 4 presents the Pearson product-moment correlation and simple linear regression results.

Table 4

Pearson Correlation and Simple Linear Regression: Cybersecurity Awareness Predicting Information Management Practices

	B	Std. Error	β	t	p
(Constant)	0.627	0.188	—	3.336	< .001
Cybersecurity Awareness	0.589	0.061	0.618	9.656	< .001

Note. Pearson r = 0.618, p < .001; R^2 = .382; Adjusted R^2 = .380; F(1, 329) = 93.24, p < .001. N = 331. Source: Field Survey (2026).

The Pearson correlation of r = 0.618 is statistically significant at p < .001, indicating a moderately strong positive linear relationship. Respondents with higher aggregate awareness scores consistently report more robust information management practice across all five sub-dimensions. The regression model is statistically significant (F(1, 329) = 93.24, p < .001), and the R^2 value of .382 indicates that cybersecurity awareness accounts for approximately 38.2% of the variance in information management practice scores. The unstandardized coefficient B = 0.589 means that for each one-unit increase in the cybersecurity awareness scale, information management practice scores increase by 0.589 units. This is a practically meaningful effect. This finding is directly consistent with Protection Motivation Theory (Rogers, 1975), which posits that higher threat appraisal and coping appraisal motivate more protective organizational behaviors. Tran *et al.* (2021)

Citation: Njoku, Jude Chinonso & Chukwueke, Ugonna Onyedikachukwu. "Cybersecurity Knowledge Deficits, Information Management Failures, and Organizational Moderators Among Small and Medium-Sized Enterprises in Lagos, Nigeria". *Journal of People and Worldviews (JPW)*, 2026: pp158-174.

reported a comparably strong awareness-behavior correlation (r = 0.59) in Vietnamese organizational samples, and Bulgurcu *et al.* (2010) found that awareness of security policy requirements was among the strongest predictors of information security compliance intention. The 61.8% of unexplained variance points clearly to the role of the organizational moderating factors.

Organizational Moderating Factors (Research Question 4)

Table 5 presents the hierarchical moderated multiple regression results. Descriptive statistics for the six organizational factors show that cybersecurity training availability (M = 2.17, SD = 0.98) and formal cybersecurity policies (M = 2.39, SD = 1.01) both fall below criterion, indicating that the two most foundational institutional enablers of awareness-to-behavior translation are absent or severely underdeveloped. The resource constraint factor (M = 3.61, SD = 0.89) is the single factor to return a high mean, indicating near-consensus that financial and staffing limitations impede adequate cybersecurity implementation regardless of individual intent.

Table 5

Hierarchical Moderated Regression: Organizational Moderators of the Awareness–IM Relationship

Predictor	Step 1 B (β)	Step 2 B (β)	Step 3 B (β)
Cybersecurity Awareness	0.589 (.618)**	0.411 (.432)**	0.397 (.417)**
Leadership Support	—	0.214 (.196)**	0.187 (.171)*
Formal Cybersecurity Policies	—	0.186 (.172)*	0.163 (.151)*
Training Availability	—	0.241 (.213)**	0.228 (.202)**
Security Culture	—	0.173 (.161)*	0.149 (.139)*
Technical Infrastructure	—	0.138 (.128)	0.119 (.110)
Resource Constraints (inverse)	—	−0.197 (−.182)**	−0.181 (−.167)*
Awareness × Leadership (E1)	—	—	0.143 (.129)*
Awareness × Policies (E2)	—	—	0.137 (.124)*
Awareness × Training (E3)	—	—	0.189 (.172)**
Awareness × Security Culture (E4)	—	—	0.121 (.109)
Awareness × Infrastructure (E5)	—	—	0.097 (.088)
Awareness × Resources (E6)	—	—	−0.114 (−.103)
R^2	.382	.541	.572
ΔR^2	.382**	.159**	.031*

*Note. *p < .05; **p < .01. Standardized coefficients (β) in parentheses. N = 331. Source: Field Survey (2026).*

Citation: Njoku, Jude Chinonso & Chukwueke, Ugonna Onyedikachukwu. "Cybersecurity Knowledge Deficits, Information Management Failures, and Organizational Moderators Among Small and Medium-Sized Enterprises in Lagos, Nigeria". *Journal of People and Worldviews (JPW)*, 2026: pp158-174.

The introduction of organizational moderators in Step 2 substantially improves model fit ($\Delta R^2 = .159$, $p < .01$), with the model now accounting for 54.1% of the variance in information management practices. Leadership support ($B = 0.214$, $p < .01$), training availability ($B = 0.241$, $p < .01$), formal policies ($B = 0.186$, $p < .05$), and security culture ($B = 0.173$, $p < .05$) all contribute positively and significantly. Resource constraints exert a negative and significant effect ($B = -0.197$, $p < .01$), confirming that organizational resource limitations directly attenuate information management quality. Technical infrastructure does not achieve significance, suggesting its effect is largely mediated through the other organizational variables. The introduction of interaction terms in Step 3 adds a further 3.1% of explained variance ($\Delta R^2 = .031$, $p < .05$), confirming that organizational factors genuinely moderate, not merely add to, the translation of individual awareness into organizational practice. The strongest significant interaction is between awareness and training availability ($B = 0.189$, $p < .01$): the behavioral dividend of awareness is considerably larger in organizations that provide formal training than in those that do not. Awareness interactions with leadership support ($B = 0.143$, $p < .05$) and formal policies ($B = 0.137$, $p < .05$) also produce significant amplification effects.

Discussion

The aggregate cybersecurity awareness mean of 3.03 is above the criterion threshold, yet several of the most operationally consequential awareness dimensions particularly knowing who to contact when a breach is suspected ($M = 2.31$) and the behavioral willingness to report an uncertain incident immediately ($M = 1.98$) fall well below criterion at the item level. The data describe a population that knows, in the abstract, that cyber threats exist and that passwords should be strong, but that has not been equipped with the specific, procedural, and behaviorally embedded knowledge needed to translate that general orientation into reliable protective action under real operational conditions. This distinction between declarative and procedural awareness is analytically vital. Parsons *et al*. (2017) demonstrated that declarative knowledge scores consistently outperformed behavioral intention and practice scores across all seven HAIS-Q focus areas, and Zwilling *et al*. (2022) found this knowing-doing gap to be the most persistent and cross-culturally consistent feature of organizational cybersecurity awareness profiles across six national contexts. The particular weakness of incident reporting awareness reflects not only a motivational gap but also a structural one. An employee cannot report a suspected incident through a channel that has not been established, contact a security officer who has not been appointed, or follow a procedure

Citation: Njoku, Jude Chinonso & Chukwueke, Ugonna Onyedikachukwu. "Cybersecurity Knowledge Deficits, Information Management Failures, and Organizational Moderators Among Small and Medium-Sized Enterprises in Lagos, Nigeria". *Journal of People and Worldviews (JPW)*, 2026: pp158-174.

that has not been documented (Ngoqo & Flowerday, 2015).

The finding that overall information management practices fall below criterion is concerning but unsurprising given the structural characteristics of the SME operating environment. SMEs lack dedicated IT security staff, their information governance arrangements are informal, and they have rarely invested in the documented frameworks such as incident response plans, recovery procedures, backup testing protocols that transform individual awareness-motivated intentions into institutionalized organizational behaviors (Alahmari & Duncan, 2020; Bada & Nurse, 2019). The sub-threshold mean for data classification and storage (M = 2.47) is particularly consequential in view of the Nigeria Data Protection Regulation (2019) and the Nigeria Data Protection Act (2023), since data classification is the foundational prerequisite for implementing most regulatory compliance obligations. An organization that cannot systematically identify which of its data assets are personal, sensitive, or subject to special handling requirements cannot meaningfully implement data minimization, storage limitation, or security safeguard obligations (Abdulrauf, 2021).

The Pearson correlation of r = 0.618 and the regression coefficient B = 0.589 jointly confirm that cybersecurity awareness is a substantively significant predictor of information management quality and not merely statistically significant. A unit increase in the awareness scale produces a nearly 0.6-unit improvement in the information management practice score. The PMT framework explains the mechanism. As threat appraisal increases and employees genuinely understand the severity and probability of cyber threats, coping appraisal increases as they develop confidence in their ability to implement protective responses. Protection motivation rises and translates into more consistent information management behavior (Rogers, 1975; Herath & Rao, 2009). Nonetheless, the 38.2% of explained variance is both practically significant and theoretically honest. Hence, awareness is not the only thing that matters. IBM Security (2023) found that the most impactful security interventions are those that combine awareness enhancement with organizational structural enablers like training, policy, leadership, and infrastructure rather than treating them as alternatives. The regression data are a statistical instantiation of that finding.

The moderating analysis shows that training availability produces the strongest significant interaction with cybersecurity awareness (B = 0.189, p < .01). In organizations where formal cybersecurity training is provided, the behavioral dividend of awareness is substantially larger than in organizations where training is absent. Bada and Nurse

Citation: Njoku, Jude Chinonso & Chukwueke, Ugonna Onyedikachukwu. "Cybersecurity Knowledge Deficits, Information Management Failures, and Organizational Moderators Among Small and Medium-Sized Enterprises in Lagos, Nigeria". *Journal of People and Worldviews (JPW)*, 2026: pp158-174.

(2019) specifically identified this amplification effect, arguing that training converts latent awareness into operationalized practice by providing the procedural scaffolding, role-specific guidance, and organizational context that raw knowledge cannot supply. Leadership support ($B = 0.143$, $p < .05$) is equally resonant. Da Veiga and Eloff (2010) found that leadership commitment was the single most powerful organizational antecedent of employee security behavior across all governance dimensions they examined. The significantly negative effect of resource constraints ($B = -0.197$, $p < .01$) represents what Alahmari and Duncan (2020) described as the "infrastructure ceiling effect". This is the point at which individual awareness motivation collides with an organizational environment that cannot support the behaviors it motivates. The absence of formal cybersecurity policies ($M = 2.39$) is analytically significant for the GDT framework. Without formal policies, even highly aware employees may be uncertain about what their organization specifically requires, leading to inconsistent and improvised security practice (D'Arcy *et al*., 2009; Siponen & Vance, 2010). This policy vacuum, the norm rather than the exception across sampled SMEs, may explain why aggregate information management practice scores remain below threshold despite an above-criterion aggregate awareness level.

Conclusion and Recommendations

This study demonstrates that cybersecurity awareness among Lagos SME employees is moderate in aggregate but uneven in distribution, and that information management practices are broadly inadequate, with the most consequential deficits concentrated in incident response and backup and recovery. The effect of awareness on practice is real, statistically robust, and practically consequential. Cybersecurity awareness accounts for approximately 38% of the variance in information management practice scores, a meaningful effect that directly justifies investment in awareness enhancement as an organizational strategy. But awareness alone is not sufficient. The organizational conditions that amplify or suppress the behavioral yield of awareness like training, policy, leadership, and resource capacity are the decisive variables that explain why SMEs with comparable awareness levels can exhibit dramatically different information management outcomes. The SME employees captured in this study are not passive or indifferent. They hold moderate awareness, acknowledge the relevance of cybersecurity to their work, and perceive a positive relationship between what they know and how they manage information. What they lack is the institutional partnership such as training programs, documented policies, leadership modeling, and adequate resources that would convert individual motivation into

Citation: Njoku, Jude Chinonso & Chukwueke, Ugonna Onyedikachukwu. "Cybersecurity Knowledge Deficits, Information Management Failures, and Organizational Moderators Among Small and Medium-Sized Enterprises in Lagos, Nigeria". *Journal of People and Worldviews (JPW)*, 2026: pp158-174.

sustained, organization-wide protective practice.

Four recommendations follow directly from the findings. First, SME owners and managers should institutionalize structured cybersecurity awareness training, given that training availability produces the strongest moderating amplification of awareness. Secondly, SMEs should develop and formally promulgate documented cybersecurity policies. The absence of formal policies creates a behavioral vacuum that weakens the deterrence value of even high individual awareness. Thirdly, SME leadership should visibly champion cybersecurity as an organizational priority by allocating resources for awareness investment, enforcing security policies consistently, and modeling security-compliant behavior. Lastly, incident response plans and backup testing protocols should be prioritized as immediate operational investments given the acute deficits recorded across these sub-dimensions.

References

Abdulrauf, L. A. (2021). Data protection law and regulation in Nigeria: Early implementation experiences and lessons. *International Data Privacy Law, 11*(4), 322–339.

Aderibigbe, A. A., Ojo, A. I., & Odunaike, S. A. (2022). Cybersecurity challenges facing SMEs in Nigeria: An empirical assessment. *Journal of Information Technology and Development Studies, 11*(2), 45–61.

Alahmari, A., & Duncan, B. (2020). Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence. *Proceedings of the 2020 International Conference on Information Systems and Management Science,* 1–9.

Bada, M., & Nurse, J. R. C. (2019). Developing cybersecurity education and awareness programmes for small and medium-sized enterprises (SMEs). *Information and Computer Security, 27*(3), 393–410.

Beautement, A., Sasse, M. A., & Wonham, M. (2016). The compliance budget: Managing security behaviour in organisations. *Proceedings of the 2008 Workshop on New Security Paradigms,* 47–58.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523–548.

Choo, C. W. (2014). Information culture and organizational effectiveness. *International Journal of Information Management, 33*(5), 775–779.

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). SAGE Publications.

Citation: Njoku, Jude Chinonso & Chukwueke, Ugonna Onyedikachukwu. "Cybersecurity Knowledge Deficits, Information Management Failures, and Organizational Moderators Among Small and Medium-Sized Enterprises in Lagos, Nigeria". *Journal of People and Worldviews (JPW),* 2026: pp158-174.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research, 20*(1), 79–98.

Da Veiga, A., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. *Computers and Security, 29*(2), 196–207.

ENISA (European Union Agency for Cybersecurity). (2023). *ENISA threat landscape 2023.* European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*(2), 154–165.

IBM Security. (2023). *Cost of a data breach report 2023.* IBM Corporation. https://www.ibm.com/reports/data-breach

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers and Security, 31*(1), 83–95.

Lagos Chamber of Commerce and Industry (LCCI). (2022). *Lagos business environment report 2022.* LCCI Publications.

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems, 11*(7), 394–413.

Liao, Q., Luo, X. R., Gurung, A., & Li, L. (2021). Information security behaviors in the workplace: Determinants and mechanisms. *Journal of Information Management, 41*(1), 100–118.

National Bureau of Statistics. (2021). *MSME national survey report 2021.* Federal Government of Nigeria.

Ngoqo, B., & Flowerday, S. V. (2015). Student mobile phone security awareness and behaviour: NMMU students as a case study. *South African Journal of Information Management, 17*(1), 1–7.

Nigeria Data Protection Act. (2023). *Nigeria Data Protection Act 2023.* Federal Republic of Nigeria Official Gazette.

Nigeria Data Protection Regulation. (2019). *Nigeria Data Protection Regulation 2019.* National Information Technology Development Agency.

Nunnally, J. C. (1978). *Psychometric theory* (2nd ed.). McGraw-Hill.

Ogunyemi, A. A., & Johnston, K. A. (2020). Examining ICT adoption and use by SMEs in Lagos, Nigeria. *The*

Citation: Njoku, Jude Chinonso & Chukwueke, Ugonna Onyedikachukwu. "Cybersecurity Knowledge Deficits, Information Management Failures, and Organizational Moderators Among Small and Medium-Sized Enterprises in Lagos, Nigeria". *Journal of People and Worldviews (JPW),* 2026: pp158-174.

African Journal of Information Systems, 12(1), 1–27.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The human aspects of information security questionnaire (HAIS-Q): Two further validation studies. *Computers and Security, 66*, 40–51.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology, 91*(1), 93–114.

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly, 34*(3), 487–502.

Small and Medium Enterprises Development Agency of Nigeria (SMEDAN). (2021). *SMEDAN and NBS survey report on micro, small and medium enterprises in Nigeria 2021*. SMEDAN.

Tran, H. L., Luong, D. A., & Le, T. T. M. (2021). The impact of cybersecurity awareness on the information security behavior of employees: Empirical evidence from Vietnam. *Sustainability, 13*(15), Article 8208.

Verizon. (2023). *2023 data breach investigations report.* Verizon Business. https://www.verizon.com/business/resources/reports/dbir/

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, L., Cetin, F., & Bassyiouny, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems, 62*(1), 82–97.

Citation: Njoku, Jude Chinonso & Chukwueke, Ugonna Onyedikachukwu. "Cybersecurity Knowledge Deficits, Information Management Failures, and Organizational Moderators Among Small and Medium-Sized Enterprises in Lagos, Nigeria". *Journal of People and Worldviews (JPW),* 2026: pp158-174.