

Managing Digital Risk in Micro and Small Businesses: An Assessment of Cybersecurity Awareness and Practices in Gombe State, Nigeria

Usman Aminu; Hassan Ezekiel and Mustapha Aisha Sharif

Department of Cooperative Economics and Management, Federal College of Horticulture Dadinkowa, Gombe State, Nigeria.

Corresponding author: aminuusmanzee@gmail.com

DOI: <https://doi.org/10.62154/ajmbr.2026.023.01025>

Abstract

This study examines cybersecurity awareness and practices among micro and small business owners in Gombe State, Nigeria, highlighting their relevance to effective digital risk management. A descriptive survey design was adopted, and 385 respondents were selected through a multistage sampling technique based on Cochran's sample size formula. Data were collected using a structured questionnaire validated by three experts from Gombe State University, with a Cronbach's alpha reliability coefficient of 0.87. Data were analyzed using mean, standard deviation, and simple linear regression at the 0.05 level of significance. The findings showed a moderate level of cybersecurity awareness ($\bar{x} = 3.35$, $\sigma = 1.35$) and cybersecurity practices ($\bar{x} = 3.01$, $\sigma = 1.32$). Cybersecurity awareness had a positive and statistically significant influence on cybersecurity practices ($\beta = .668$, $p < .001$), explaining 44.6% of the variation in cybersecurity practices. The study concluded that improving cybersecurity awareness is essential for strengthening digital risk management among micro and small business owners. It recommended regular cybersecurity awareness programmes by relevant agencies, including the National Information Technology Development Agency (NITDA), Small and Medium Enterprises Development Agency of Nigeria (SMEDAN), National Orientation Agency (NOA), Nigeria Computer Society (NCS), and other relevant organizations. It also recommended integrating cybersecurity awareness into business support programmes delivered by SMEDAN, Industrial Training Fund (ITF), and educational institutions to strengthen the digital resilience of micro and small business owners in Gombe State.

Keywords: Cybersecurity Awareness, Cybersecurity Practices, Digital Risk Management, Micro and Small Business Owners, Nigeria.

Introduction

Micro and small businesses are essential drivers of economic growth and development of a country. They play an integral role in generating employment, reducing poverty, stimulating innovation, and promoting entrepreneurship. Their flexibility and relatively low entry barriers enable them to respond rapidly to changing market conditions. This places them as essential contributors to local and national economies. In developing countries such as Nigeria, micro and small businesses constitute the majority of business establishments and provide livelihoods for millions of people. Consequently, improving

their competitiveness and long-term sustainability has become a priority for governments and development agencies (Rawindaran et al., 2021; Al-Somali et al., 2024; Dagada & Saar, 2025).

The rapid advancement of digital technologies has transformed the way micro and small businesses operate. These technologies have enhanced operational efficiency, reduced transaction costs, and created new opportunities for business growth, making digital transformation an important driver of business competitiveness. The widespread availability of smartphones, internet services, digital payment platforms, cloud-based applications, and social media has enabled business owners to improve customer engagement, manage inventories, process financial transactions, and expand market access beyond traditional physical boundaries (Moreno et al., 2025; Falch et al., 2022).

However, the increasing reliance on digital technologies has also intensified exposure to cybersecurity threats. Cybercriminals increasingly exploit vulnerabilities through phishing, malware, ransomware, identity theft, social engineering, and online payment fraud. Unlike large organisations with dedicated information technology units and substantial security budgets, most micro and small businesses operate with limited financial resources, inadequate technical expertise, and insufficient investment in cybersecurity infrastructure. Consequently, they are particularly vulnerable to cyberattacks that may disrupt business operations, compromise sensitive information, damage customer trust, and threaten business continuity (Mitrofan et al., 2020; Kariuki et al., 2023; Tiwari et al., 2025).

Addressing these risks requires both cybersecurity awareness and effective cybersecurity practices. Cybersecurity awareness refers to an individual's knowledge and understanding of cyber threats, associated risks, and appropriate protective measures, while cybersecurity practices involve the consistent implementation of security measures such as strong password management, regular software updates, secure data backups, multi-factor authentication, safe internet use, and protection of customer information. Although awareness provides the foundation for secure behaviour, evidence suggests that knowledge alone does not necessarily translate into effective cybersecurity practices. This is because financial constraints, limited technical skills, organisational culture, and inadequate institutional support often hinder the adoption of recommended security measures (Bada & Nurse, 2019; Masselink, 2025).

Recent studies indicate that cybersecurity awareness positively influences risk perception and encourages the adoption of protective practices, yet many small businesses continue to exhibit inadequate cybersecurity preparedness despite increasing digital adoption. Human error remains one of the leading causes of cybersecurity incidents, highlighting the need for greater awareness, continuous training, and improved cybersecurity practices among business owners and employees (Ncubukezi et al., 2020; Fagbule, 2023; Alluhayb et al., 2025).

In Nigeria, rapid growth in internet penetration, mobile banking, electronic payment systems, and social media commerce has accelerated the digitalisation of micro and small businesses. While these technologies have improved business efficiency and expanded

market opportunities, they have also increased vulnerability to cyber threats, particularly among businesses with limited cybersecurity capabilities (Fagbule, 2023). Within Gombe State, business owners increasingly rely on digital platforms such as mobile banking applications, point-of-sale terminals, WhatsApp Business, Facebook, and Instagram to support daily operations. Despite this growing dependence on digital technologies, empirical evidence on cybersecurity awareness and cybersecurity practices among micro and small business owners in the State remains limited.

Against this background, this study assesses cybersecurity awareness and cybersecurity practices among micro and small business owners in Gombe State, Nigeria. Specifically, it examines the level of cybersecurity awareness among business owners and the cybersecurity practices they adopt in managing digital risks. The findings from this study contribute to the growing literature on small business cybersecurity while providing evidence to support policy development, entrepreneurship support programmes, cybersecurity awareness initiatives, and capacity-building interventions aimed at strengthening the digital resilience of micro and small businesses.

Statement of the Problem

The increasing adoption of digital technologies has transformed the operations of micro and small businesses in Nigeria. In Gombe State, many business owners now rely on smartphones, mobile banking, electronic payment platforms, point-of-sale terminals, and social media to conduct business dealings, advertise products and communicate with customers. However, this digital transition has been accompanied by growing cybersecurity challenges. Cases of fake payment alerts, phishing messages, fraudulent online transactions, compromised social media accounts, identity theft, and other forms of cyber fraud have become increasingly prevalent. Preliminary field observations and interactions with business owners suggest that some merchants now prefer cash transactions because of fears of cyber fraud while others who engage in digital marketing or online business have experienced various forms of cyber scams. These situations expose businesses to financial losses, disrupt business operations, weaken customer confidence in electronic transactions, discourage the adoption of digital technologies, and ultimately threaten the competitiveness and sustainability of micro and small businesses in an increasingly digital economy.

Empirical evidence from different studies indicates that inadequate cybersecurity awareness and poor cybersecurity practices remain major contributors to cyber incidents among micro and small businesses. Studies have shown that many business owners fail to implement basic security measures such as strong password management, regular software updates, secure data backup, verification of suspicious electronic communications, and other essential cybersecurity controls, thereby increasing their vulnerability to cyberattacks (Cartwright et al., 2023; Khoza & Hoeyi, 2025; Alluhayb et al., 2025). Within Nigeria, available studies have similarly highlighted growing cybersecurity

challenges and the need to strengthen cybersecurity awareness and protective practices among businesses (Adelusi et al., 2022; Fagbule, 2023). However, a review of the available literature to the best of the researchers' knowledge, revealed an absence of empirical studies specifically examining the cybersecurity awareness and cybersecurity practices of micro and small business owners in Gombe State, Nigeria.

The lack of context-specific evidence poses significant challenges for policymakers and institutions responsible for promoting secure digital entrepreneurship. For example, agencies such as the National Information Technology Development Agency (NITDA), the Small and Medium Enterprises Development Agency of Nigeria (SMEDAN), the National Orientation Agency (NOA), the Industrial Training Fund (ITF), the Nigeria Computer Society (NCS), higher educational institutions, financial institutions, and other relevant public and private organisations require empirical evidence to design and implement interventions that effectively address the cybersecurity needs of micro and small businesses. Without a clear understanding of the cybersecurity awareness and cybersecurity practices of business owners, such interventions may not adequately address their actual vulnerabilities. If this situation persists, cyber fraud may continue to discourage the adoption of digital technologies, increase avoidable financial losses, weaken trust in digital transactions, and undermine efforts to promote digital entrepreneurship, financial inclusion, and sustainable business growth in Gombe State. It is against this backdrop that this study assesses cybersecurity awareness and cybersecurity practices among micro and small business owners in Gombe State, Nigeria, with a view to providing empirical evidence that will inform policies and capacity-building initiatives aimed at strengthening the cybersecurity resilience of the sector.

Objectives of the Study

The main objective of this study is to assess cybersecurity awareness and cybersecurity practices among micro and small business owners in Gombe State, Nigeria. The specific objectives are to:

1. assess the level of cybersecurity awareness among micro and small business owners in Gombe State, Nigeria.
2. assess the cybersecurity practices adopted by micro and small business owners in Gombe State, Nigeria.
3. determine the influence of cybersecurity awareness on cybersecurity practices among micro and small business owners in Gombe State, Nigeria.

Research Questions

The following research questions guided the study:

1. What is the level of cybersecurity awareness among micro and small business owners in Gombe State, Nigeria?
2. What cybersecurity practices are adopted by micro and small business owners in Gombe State, Nigeria?

3. To what extent does cybersecurity awareness influence cybersecurity practices among micro and small business owners in Gombe State, Nigeria?

Hypothesis

The following null hypothesis was tested at the 0.05 level of significance:

H₀: Cybersecurity awareness has no statistically significant influence on cybersecurity practices among micro and small business owners in Gombe State, Nigeria.

Theoretical/Conceptual Framework

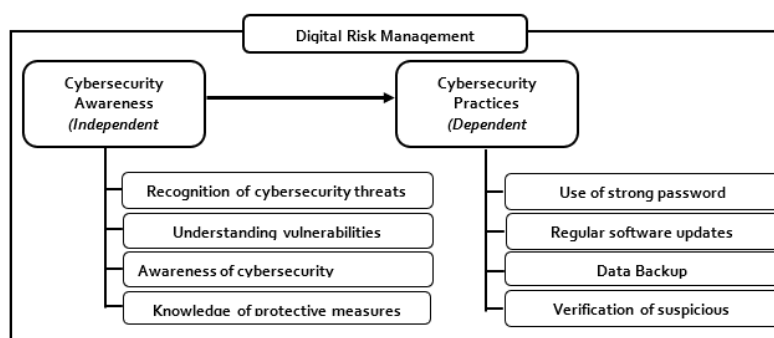
Theoretical Framework

This study is anchored on Protection Motivation Theory (PMT) developed by Rogers (1975, 1983), which explains how individuals respond to perceived threats and become motivated to adopt protective behaviours. The theory emphasises threat appraisal, which involves recognising the seriousness and likelihood of a threat, and coping appraisal, which concerns understanding the effectiveness and feasibility of protective responses. In this study, PMT provides the basis for understanding how cybersecurity awareness of threats, vulnerabilities, consequences, and protective measures may encourage business owners to adopt appropriate cybersecurity practices.

Conceptual Framework

Conceptually, the study positions cybersecurity awareness as the independent variable and cybersecurity practices as the dependent variable. Cybersecurity awareness covers respondents' understanding of cyber threats, password vulnerabilities, unsecured networks, phishing, data protection, software updates, and the consequences of cyberattacks, while cybersecurity practices cover the actual implementation of measures such as strong passwords, software updates, data backup, and verification of suspicious messages. The framework therefore proposes that higher cybersecurity awareness is likely to result in greater adoption of cybersecurity practices, with digital risk management serving as the broader context.

Figure 1: Conceptual Framework of the Study



Source: Researchers' Conceptualisation, 2026

Literature Review

Existing empirical evidence consistently demonstrates that cybersecurity awareness is fundamental to protecting micro and small businesses from increasing cyber threats associated with digital transformation. As businesses adopt electronic payment systems, cloud computing, mobile applications, and social media for daily operations, cybersecurity awareness enables business owners to recognise cyber risks, appreciate their potential consequences, and make informed security decisions. However, studies across both developed and developing economies indicate that cybersecurity awareness among micro and small businesses remains inadequate. Limited cybersecurity knowledge, inadequate training, weak organisational support, and financial constraints continue to hinder business owners from effectively identifying and responding to cyber threats (Bada & Nurse, 2019; Mitrofan et al., 2020; Lejaka et al., 2019; Kariuki et al., 2023; Dagada & Saar, 2025). The literature further suggests that cybersecurity awareness extends beyond knowledge acquisition to include attitudes and behaviours that encourage secure use of digital technologies. Nevertheless, awareness alone does not always translate into secure behaviour, as organisational culture, continuous training, and institutional support significantly influence whether business owners consistently apply cybersecurity knowledge in practice (Fagbule, 2023; Alluhayb et al., 2025).

Similarly, empirical studies consistently report that cybersecurity practices among micro and small businesses remain relatively weak despite increasing digital adoption. Although many businesses implement basic protective measures such as password management, antivirus software, and data backup, more comprehensive practices including regular software updates, multi-factor authentication, incident response planning, cybersecurity policies, employee training, routine security audits, and continuous risk assessment are less frequently adopted (Kabanda et al., 2018; Ncubekezi et al., 2020; Cartwright et al., 2023; Khoza & Hoeyi, 2025). Previous studies attribute these deficiencies to limited financial resources, inadequate technical expertise, insufficient access to cybersecurity information, and weak institutional support, particularly among businesses operating in resource-constrained environments (Falch et al., 2022; Adelusi et al., 2022; Tiwari et al., 2025). Consequently, many micro and small businesses remain vulnerable to phishing attacks, malware, online payment fraud, identity theft, ransomware, and other cyber threats capable of disrupting business operations, reducing customer confidence, and undermining long-term business sustainability.

The relationship between cybersecurity awareness and cybersecurity practices has also attracted considerable scholarly attention. Available evidence generally indicates that business owners with higher levels of cybersecurity awareness are more likely to adopt appropriate cybersecurity practices and invest in measures that protect digital assets and business operations (Udofot & Topchyan, 2020; Masselink, 2025). However, several studies argue that awareness alone is insufficient to guarantee secure behaviour because practical implementation is also influenced by financial capacity, organisational commitment, digital skills, and access to technical support (Alluhayb et al., 2025; Al-Somali et al., 2024; Moreno

et al., 2025). Overall, the literature suggests a positive relationship between cybersecurity awareness and cybersecurity practices, although the strength of this relationship varies across business contexts.

Despite these valuable contributions, important empirical gaps remain. Existing evidence is concentrated largely in Europe, Asia, and selected African countries, with relatively limited studies focusing on Nigerian micro and small businesses. Furthermore, much of the available literature has employed systematic reviews, or broad investigations of small and medium-sized enterprises without specifically examining micro and small business owners who personally manage day-to-day business operations. A review of the available literature also revealed lack of empirical studies examining both cybersecurity awareness and cybersecurity practices among micro and small business owners in Gombe State, Nigeria. Consequently, there is limited context-specific evidence on the level of cybersecurity awareness, the cybersecurity practices adopted by business owners, and the extent to which awareness influences cybersecurity practices within this setting. This study addresses these gaps by providing quantitative evidence to inform policy, entrepreneurship support programmes, and cybersecurity capacity-building initiatives aimed at strengthening the digital resilience of micro and small businesses.

Methodology

This study adopted a descriptive survey research design. The design was considered appropriate because it enabled the collection of quantitative data from business owners and facilitated the assessment of existing levels of cybersecurity awareness and cybersecurity practices, as well as the influence of cybersecurity awareness on cybersecurity practices. The study was conducted in Gombe State, North-Eastern Nigeria. The target population comprised micro and small business owners operating across the State. A sample size of 385 respondents was determined using Cochran's sample size formula for large populations. A multistage sampling technique was employed to select the respondents. To ensure adequate geographical representation, Gombe State was stratified into three geographical zones representing the northern, central, and southern parts of the State. One major commercial town was purposively selected from each geographical zone, namely Gombe from the northern zone, Kumo from the central zone, and Kaltungo from the southern zone. The selected towns were chosen because they constitute the major commercial centres within their respective geographical zones and host a high concentration of micro and small business activities. The sample was proportionately allocated based on the relative commercial size of the selected towns, with Gombe allocated 193 respondents (50%) because it is the State's largest commercial centre, while Kumo and Kaltungo were each allocated 96 respondents (25%). In the final stage, simple random sampling was used to select the required number of micro and small business owners from each town.

Data were collected using a developed structured questionnaire. The instrument consisted of two sections corresponding to the study variables. The development of the items was guided by the study's conceptualisation of cybersecurity awareness and cybersecurity practices. The cybersecurity awareness section focused on respondents' recognition and understanding of cybersecurity threats, vulnerabilities, consequences, and protective requirements, while the cybersecurity practices section focused on the implementation of protective cybersecurity behaviours. The instrument utilises a five-point rating scale of Very High Level (VHL) = 5, High Level (HL) = 4, Moderate Level (ML) = 3, Low Level (LL) = 2, and Very Low Level (VLL) = 1. The questionnaire was subjected to face validation by two experts from the Department of Business Administration and one expert from the Department of Computer Science, Gombe State University. The internal consistency of the instrument was established using Cronbach's alpha, which yielded a reliability coefficient of 0.87, indicating satisfactory reliability for the study. The questionnaires were administered directly to the selected business owners with the assistance of trained research assistants.

To ensure that appropriate ethical standards were maintained throughout the research process, respondents were provided with clear information about the purpose and nature of the study, the voluntary nature of their participation, and the measures adopted to protect the confidentiality of the information they provided. Informed consent was obtained from each respondent before data collection commenced. Respondents were also informed of their right to decline participation or withdraw from the study at any time without penalty or adverse consequences. No personally identifiable information was collected. All information obtained was treated as confidential, used solely for academic purposes, and securely managed by the researchers. Access to the completed questionnaires and research data was restricted to the research team. The findings were presented in aggregate form to prevent the identification of individual respondents or their businesses.

Data collected were analysed using mean and standard deviation with the aid of the Statistical Package for the Social Sciences (SPSS) version 25.0. Mean and standard deviation were used to answer the research questions, while simple linear regression was employed to test the null hypothesis at the 0.05 level of significance.

Results

Research Question One: What is the level of cybersecurity awareness among micro and small business owners in Gombe State, Nigeria?

Table 1: Summary of Mean and Standard Deviation of Responses on the Level of Cybersecurity Awareness among Micro and Small Business Owners in Gombe State

S/N	Item (n = 385)	$\bar{x}_1$	σ_1	Remark
1	I am aware that businesses are increasingly targeted by cybercriminals.	3.37	1.30	ML

S/N	Item (n = 385)	$\bar{x}_1$	σ_1	Remark
2	I understand the characteristics of a strong password and why weak passwords increase cybersecurity risks.	3.32	1.36	ML
3	I know that internet-connected devices such as smartphones and computers can be exploited to gain unauthorized access to business information.	3.33	1.40	ML
4	I understand the security risks associated with using public or unsecured Wi-Fi networks.	3.38	1.38	ML
5	I understand the importance of protecting customers' personal and financial information from unauthorized access.	3.36	1.32	ML
6	I am aware of the financial and reputational consequences of cyberattacks on businesses.	3.34	1.37	ML
7	I can recognize common cyber threats such as phishing emails, fake websites, and fraudulent text messages.	3.32	1.34	ML
8	I understand why software and security updates are necessary for protecting digital devices.	3.35	1.39	ML
9	I understand that cybersecurity is essential for business continuity and customer trust.	3.43	1.34	ML
10	I understand that human errors by employees or business assistants can create cybersecurity vulnerabilities.	3.33	1.32	ML
	Cluster Mean	3.35	1.35	ML

Source: Field survey, 2026

The result in Table 1 above shows that the mean scores for cybersecurity awareness among micro and small business owners range from 3.32 to 3.43, while the corresponding standard deviations ranged from 1.30 to 1.40, indicating moderate variability in the respondents' opinions. The highest mean score was obtained for the Statement that cybersecurity measures are important for survival of small and micro businesses ($\bar{x} = 3.43$, $\sigma = 1.34$), suggesting that respondents were relatively more aware of the importance of cybersecurity for sustaining business operations and maintaining customer trust. This was followed by respondents' awareness that using public or unsecured Wi-Fi can expose business data to risk ($\bar{x} = 3.38$, $\sigma = 1.38$) and that small businesses are targets of cyber fraud and online attacks ($\bar{x} = 3.37$, $\sigma = 1.30$). Conversely, the lowest mean scores were recorded for understanding that weak passwords can expose business accounts to cyber risks ($\bar{x} = 3.32$, $\sigma = 1.36$) and awareness that phishing messages can be used to steal business information ($\bar{x} = 3.32$, $\sigma = 1.34$), although these values still fall within the moderate level category.

This shows that micro and small business owners in Gombe State have a moderate level of cybersecurity awareness ($\bar{x} = 3.35$, $\sigma = 1.35$). It therefore suggests that while respondents demonstrate a reasonable understanding of major cybersecurity issues, further awareness-building is needed to strengthen preparedness and response to cyber threats.

Research Question Two: What is the level of cybersecurity practices among micro and small business owners in Gombe State, Nigeria?

Table 2: Summary of Mean and Standard Deviation of Responses on the Level of Cybersecurity Practices among Micro and Small Business Owners in Gombe State, Nigeria

S/N	Item/Statement (n = 385)	$\bar{x}_1$	σ_1	Remark
1	I use strong and difficult-to-guess passwords for my business accounts.	3.00	1.32	ML
2	I regularly change passwords used for business-related platforms.	2.91	1.31	ML
3	I avoid accessing business accounts using public Wi-Fi networks.	3.05	1.34	ML
4	I use security measures such as antivirus or phone protection tools.	3.07	1.34	ML
5	I regularly update my mobile phone and/or computer applications.	3.02	1.33	ML
6	I verify messages or emails before responding to requests involving business information.	3.10	1.34	ML
7	I back up important business information regularly.	2.95	1.31	ML
8	I restrict access to business devices to trusted persons only.	3.03	1.33	ML
9	I take precautions when using mobile money or online banking services to make sure no external party is watching.	3.09	1.34	ML
10	I report or seek help when a cyber-related issue is suspected	2.93	1.31	ML
	Cluster Mean	3.01	1.32	ML

Source: Field survey, 2026

The result in Table 2 indicates that the mean scores for cybersecurity practices among micro and small business owners in Gombe State ranged from 2.91 to 3.10, with corresponding standard deviations ranging from 1.31 to 1.34, indicating moderate variability in respondents' responses. The highest mean score was recorded for the statement that respondents verify messages or emails before responding to requests involving business information ($\bar{x} = 3.10$, $\sigma = 1.34$). This was followed by taking precautions when using mobile money or online banking services ($\bar{x} = 3.09$, $\sigma = 1.34$) and using security measures such as antivirus or phone protection tools ($\bar{x} = 3.07$, $\sigma = 1.34$). These findings suggest that respondents demonstrate moderate adoption of cybersecurity practices aimed at protecting business information and digital transactions. On the other hand, the lowest mean score was obtained for regularly changing passwords used for business-related platforms ($\bar{x} = 2.91$, $\sigma = 1.31$), followed by reporting or seeking help when a cyber-related issue affecting the business is suspected ($\bar{x} = 2.93$, $\sigma = 1.31$) and regularly backing up important business information ($\bar{x} = 2.95$, $\sigma = 1.31$). These findings indicate that although business owners engage in some cybersecurity practices, several important protective behaviours are not consistently implemented.

This indicates that micro and small business owners in Gombe State exhibit a moderate level of cybersecurity practices ($\bar{x} = 3.01$, $\sigma = 1.32$). By implication, it means that although some protective behaviours are in place, the consistent implementation of key cybersecurity practices remains limited.

H₀: Cybersecurity awareness has no statistically significant influence on cybersecurity practices among micro and small business owners in Gombe State, Nigeria.

Table 3a: ANOVA from Regression Analysis of the Influence of Cybersecurity Awareness on Cybersecurity Practices

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	91.882	1	91.882	308.961	.001
	Residual	114.131	383	0.298		
	Total	206.013	384			

Source: Field survey, 2026

The result presented in Table 3a indicates that cybersecurity awareness has a statistically significant influence on cybersecurity practices among micro and small business owners in Gombe State. The regression model produced an F-value of 308.961 with a significance value of $p = .001$, which is less than the 0.05 level of significance. This indicates that the regression model is statistically significant and suitable for explaining the influence of cybersecurity awareness on cybersecurity practices among micro and small business owners in Gombe State.

Table 3b: Model Summary from Regression Analysis of the Influence of Cybersecurity Awareness on Cybersecurity Practices

Model	R	R Square	Adjusted R Square	Std. Error
1	.668 ^a	.446	.444	.546

Source: Field survey, 2026

The results presented in Table 3b show a correlation coefficient ($R = 0.668$), indicating a moderately strong positive relationship between cybersecurity awareness and cybersecurity practices among micro and small business owners. The coefficient of determination ($R^2 = 0.446$) indicates that 44.6% of the variation in cybersecurity practices is explained by cybersecurity awareness, while the remaining 55.4% may be attributed to other factors not included in the regression model. The adjusted R^2 value of 0.444 is very close to the R^2 value, indicating that the regression model is stable and provides a good fit to the data. These findings suggest that cybersecurity awareness makes an important contribution to explaining the cybersecurity practices adopted by micro and small business owners in Gombe State.

Table 3c: Coefficients of Regression Analysis of the Influence of Cybersecurity Awareness on Cybersecurity Practices

Model	B	Std. Error	Beta	t	Sig.
Constant	1.612	0.089	–	18.112	.001
Cybersecurity Awareness	0.502	0.029	0.668	17.577	.001

Source: Field survey, 2026

The results presented in Table 3c reveal that cybersecurity awareness has a positive and statistically significant influence on cybersecurity practices among micro and small business owners in Gombe State. The standardized regression coefficient ($\beta = 0.668$) indicates that cybersecurity awareness is a moderately strong predictor of cybersecurity practices. The corresponding t-value of 17.577 and significance value of $p = .001$ confirm that the influence is statistically significant. The unstandardized regression coefficient ($B = 0.502$) implies that a one-unit increase in cybersecurity awareness is associated with an estimated 0.502-unit increase in cybersecurity practices among the respondents. Since the probability value ($p = .001$) is less than the 0.05 level of significance, the null hypothesis is rejected. Hence, it could be concluded that cybersecurity awareness has a statistically significant positive influence on cybersecurity practices among micro and small business owners in Gombe State, Nigeria.

Discussion of Findings

The findings of the study revealed that micro and small business owners in Gombe State possessed a moderate level of cybersecurity awareness. Although the respondents demonstrated knowledge of common cyber threats such as phishing attacks, weak passwords, unsecured public Wi-Fi, and unauthorized access to business information, their overall awareness was not sufficiently high to reflect comprehensive cybersecurity knowledge. This suggests that business owners require continuous cybersecurity education and awareness programmes to improve their ability to recognise emerging threats and implement appropriate protective measures.

The finding is in agreement with the Protection Motivation Theory (PMT), which provides the theoretical foundation for this study. PMT proposes that individuals are more likely to adopt protective actions when they recognise the seriousness of a threat, perceive themselves to be vulnerable, and believe that they possess the ability to implement effective protective measures (Rogers, 1975; 1983). The moderate level of cybersecurity awareness obtained in this study suggests that many business owners have not yet developed sufficient awareness to fully motivate the adoption of effective cybersecurity behaviours.

The findings agree with that of Bada and Nurse (2019); Lejaka et al. (2019), who reported that cybersecurity awareness is essential for improving the security posture of small businesses but observed that many SMEs still lack adequate cybersecurity education and awareness. Similarly, Mitrofan et al. (2020) reported that inadequate cybersecurity knowledge among entrepreneurs remains one of the major causes of cybersecurity vulnerability in small businesses. Lejaka et al. (2019) were also of the view that cybersecurity awareness among small businesses remains underdeveloped and requires context-specific interventions to improve business resilience. Similarly, Kariuki et al. (2023) found that many small-scale entrepreneurs possessed limited cybersecurity knowledge despite increasing use of digital technologies. The finding is also consistent with Dagada and Saar (2025), who

concluded that inadequate cybersecurity awareness continues to hinder effective cybersecurity implementation among SMEs.

The finding further agrees with Kabanda et al. (2018), who reported that SMEs in developing countries generally implement only basic cybersecurity measures because of financial constraints and limited organisational capacity. Similarly, Ncubukezi et al. (2020) found that many small businesses lacked structured cybersecurity procedures and demonstrated weak cybersecurity hygiene due to inadequate knowledge and inconsistent implementation of security measures. Cartwright et al. (2023) also reported that although micro and small businesses increasingly seek cybersecurity guidance, access to reliable cybersecurity information remains inadequate, thereby limiting effective cybersecurity practices. The finding is further supported by Khoza and Hoeyi (2025), who observed that cybersecurity preparedness among small businesses remains inadequate because of low awareness, financial limitations, and weak regulatory support. Similarly, Falch et al. (2022), Adelusi et al. (2022), and Tiwari et al. (2025) attributed poor cybersecurity practices among SMEs to inadequate technical expertise, limited cybersecurity training, and insufficient financial resources.

The finding from regression analysis reveals that cybersecurity awareness has a positive and statistically significant influence on cybersecurity protective practices among micro and small business owners in Gombe State. This indicates that improvement in cybersecurity awareness is associated with increased adoption of cybersecurity protective practices among business owners. Hence, business owners who possess greater awareness of cyber threats are more likely to implement security measures capable of protecting their businesses from cyber-attacks.

The finding agrees with Udofot and Topchyan (2020), who reported that cyber-attack knowledge was the strongest predictor of cybersecurity protection among small businesses in the United States. Similarly, Masselink (2025) found that cybersecurity awareness significantly influenced SME owners' willingness to invest in cybersecurity protection measures. Moreno et al. (2025) also reported that cybersecurity perceptions significantly influenced business owners' willingness to adopt secure online payment systems, indicating that awareness shapes digital security decisions. Likewise, Al-Somali et al. (2024) concluded that stronger cybersecurity capabilities contribute significantly to organisational resilience and sustainable business performance.

However, the finding differs slightly from that of Alluhayb et al. (2025), who reported that cybersecurity awareness does not always translate into consistent cybersecurity behaviour because practical implementation is influenced by behavioural habits, organisational commitment, and continuous training. Fagbule (2023) similarly argued that cybersecurity knowledge alone is insufficient unless supported by organisational culture and practical cybersecurity education. The slight variation between these findings and the present study may be attributed to differences in research focus and methodology. While the present study examined the influence of cybersecurity awareness on general cybersecurity

protective practices among micro and small business owners in Gombe State, using a descriptive survey and regression analysis, the previous studies focused on behavioural patterns and organisational factors affecting cybersecurity implementation in different socio-economic environments. Differences in digital maturity, access to cybersecurity infrastructure, regulatory support, and business environments may also explain the observed variations.

Therefore, the findings of this study reinforce the view that cybersecurity awareness is an important foundation for improving cybersecurity protective practices among micro and small business owners. The study provides empirical evidence that strengthening cybersecurity awareness through continuous education, practical training, and institutional support can enhance the adoption of cybersecurity practices and improve the digital resilience of micro and small businesses in Gombe State, Nigeria.

However, the findings of this study should be interpreted in light of certain methodological and contextual limitations arising from the study design, geographical scope, and reliance on self-reported data. Because the data were collected within a single study period, the study provides evidence of the relationship between cybersecurity awareness and cybersecurity practices but does not establish temporal precedence or causality. Although the regression analysis estimates the magnitude and direction of the relationship between the two variables, it does not provide a sufficient basis for concluding that cybersecurity awareness causes changes in cybersecurity practices. The study covered selected commercial centres across Gombe State, and the findings should therefore not be generalised to micro and small business owners across Nigeria without evidence from other states or regions. In addition, reliance on self-reported questionnaire responses may introduce response bias, as respondents' reported cybersecurity practices may not always correspond fully with their actual practices. These considerations define the appropriate boundaries within which the findings should be interpreted and applied.

Conclusion

Based on the findings of this study, it is concluded that micro and small business owners in Gombe State possess a moderate level of cybersecurity awareness and demonstrate a moderate level of cybersecurity practices. Although respondents generally understand common cyber threats and appreciate the importance of cybersecurity, this awareness has not fully translated into the consistent adoption of recommended cybersecurity practices. Given the increasing digitalisation of business operations and the rising sophistication of cyber threats, strengthening cybersecurity awareness among micro and small business owners remains essential for improving business resilience, protecting customer confidence, and ensuring sustainable participation in the digital economy.

Recommendations

1. The National Information Technology Development Agency (NITDA), Small and Medium Enterprises Development Agency of Nigeria (SMEDAN), National

Orientation Agency (NOA), Nigeria Computer Society (NCS), and other relevant organizations should strengthen and expand cybersecurity awareness campaigns for micro and small business owners through community sensitization, digital literacy, and practical training.

2. The Small and Medium Enterprises Development Agency of Nigeria (SMEDAN), Industrial Training Fund (ITF), and educational institutions should integrate practical cybersecurity education into entrepreneurship and business support programmes so that cybersecurity becomes a regular part of business capacity-building.
3. Micro and small business owners should make cybersecurity part of their daily business operations by employing protective measures such as using strong passwords, updating devices and applications, backing up data, avoiding unsecured public Wi-Fi for transactions, and verifying suspicious emails and messages.

References

- Adelusi, B. S., Ojika, F. U., & Uzoka, A. C. (2022). Advances in cybersecurity strategy and cloud infrastructure protection for SMEs in emerging markets. *Journal of Frontiers in Multidisciplinary Research*, 3(1), 467–482. <https://doi.org/10.54660/JFMR.2022.3.1.467-482>
- Alluhayb, A. I. M., Rehman, S. U., & Janjua, N. (2025). Cyber hygiene awareness and practices among Saudi micro and small enterprises. In *2025 IEEE International Conference on E-Business Engineering (ICEBE)* (pp. 292–297). IEEE. <https://doi.org/10.1109/ICEBE68123.2025.00053>
- Al-Somali, S. A., Saqr, R. R., Asiri, A. M., & Al-Somali, N. A. (2024). Organizational cybersecurity systems and sustainable business performance of small and medium enterprises (SMEs): The mediating and moderating role of cybersecurity resilience and organizational culture. *Sustainability*, 16(5), Article 1880. <https://doi.org/10.3390/su16051880>
- Bada, M., & Nurse, J. R. C. (2019). Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). *Information & Computer Security*, 27(3), 393–410. <https://doi.org/10.1108/ICS-07-2018-0080>
- Cartwright, A., Cartwright, E., & Edun, S. (2023). Cascading information on best practice: Cyber security risk management in UK micro and small businesses and the role of IT companies. *Computers & Security*, 131, Article 103288. <https://doi.org/10.1016/j.cose.2023.103288>
- Dagada, R., & Saar, G. (2025). Bridging the cybersecurity gap: Tailored strategies for Zambia's SMEs. *Southern African Journal of Security*, 3, Article 15713. <https://doi.org/10.25159/3005-4222/15713>
- Fagbule, O. (2023). *Cyber security training in small to medium-sized enterprises (SMEs): Exploring organisation culture and employee training needs* (Doctoral thesis). Bournemouth University.
- Falch, M., Olesen, H., Skouby, K. E., Tadayoni, R., & Williams, I. (2022). Cybersecurity strategies for SMEs in the Nordic Baltic region. *Journal of Cyber Security and Mobility*, 11(6), 727–753. <https://doi.org/10.13052/jcsm2245-1439.1161>
- Kabanda, S., Tanner, M., & Kent, C. (2018). Exploring SME cybersecurity practices in developing countries. *Journal of Organizational Computing and Electronic Commerce*, 28(3), 269–282. <https://doi.org/10.1080/10919392.2018.1484598>
- Kariuki, P., Ofusori, L. O., & Subramaniam, P. R. (2023). Cybersecurity threats and vulnerabilities experienced by small-scale African migrant traders in Southern Africa. *Security Journal*. <https://doi.org/10.1057/s41284-023-00378-1>

- Khoza, N. G., & Hoeyi, P. (2025). Cyber security preparedness among SMMEs in the digital economy. *African Journal of Innovation and Entrepreneurship*, 4(3), 71–96. <https://doi.org/10.31920/2753-314X/2025/v4n3a4>
- Lejaka, T. K., Da Veiga, A., & Looock, M. (2019). Cyber security awareness for small, medium and micro enterprises (SMMEs) in South Africa. In *2019 Conference on Information Communications Technology and Society (ICTAS)* (pp. 1–6). IEEE. <https://doi.org/10.1109/ICTAS.2019.8703609>
- Masselink, M. (2025). *From awareness to action: The role of cybersecurity awareness in investment behaviour among SME retailers* [Master's thesis, Radboud University]. Radboud University Repository. <https://theses.ubn.nl/handle/123456789/19180>
- Mitrofan, A. L., Cruceru, E. V., & Barbu, A. (2020). Determining the main causes that lead to cybersecurity risks in SMEs. *Business Excellence and Management*, 10(4), 38–48.
- Moreno, D. E., Torres, R., Red, E., Hipolito, K. A., Maristela, M. N., & Ramos, B. J. (2025). Cybersecurity perception and online payment adoption among micro and small enterprises using the Theory of Planned Behavior. In *Proceedings of the 16th International Conference on E-Business, Management and Economics* (pp. 62–68). <https://doi.org/10.1145/3760557.3760568>
- Ncubukezi, T., Mwansa, L., & Rocaries, F. (2020). A review of the current cyber hygiene in small and medium-sized businesses. In *2020 15th International Conference for Internet Technology and Secured Transactions (ICITST)* (pp. 1–6). IEEE. <https://doi.org/10.23919/ICITST51030.2020.9351339>
- Rawindaran, N., Jayal, A., & Prakash, E. (2021). Machine learning cybersecurity adoption in small and medium enterprises in developed countries. *Computers*, 10(11), Article 150. <https://doi.org/10.3390/computers10110150>
- Rogers, R. W. (1975). *A protection motivation theory of fear appeals and attitude change*. *The Journal of Psychology*, 91(1), 93–114.
- Rogers, R. W. (1983). *Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation*. In *Social Psychophysiology* (pp. 153–176).
- Tiwari, A., Biswas, B., Islam, A., Sarkar, I., Saha, S., Alam, M. Z., & Farabi, S. F. (2025). Implementing robust cybersecurity strategies to protect small businesses from potential threats in the USA. *Journal of Ecohumanism*, 4(3), 322–333.
- Udofot, M., & Topchyan, R. (2020). Factors related to small business cyber-attack protection in the United States. *International Journal of Cyber-Security and Digital Forensics*, 9(1), 12–25.