CYBERSECURITY AWARENESS AND COMPLIANCE AMONG SMALL AND MEDIUM-SIZED ENTERPRISES (SMES) IN ANAMBRA STATE

Chikwendu, Stephen Chilaka
Department of Sociology and Anthropology,
Nnamdi Azikiwe University, Awka, Anambra State, Nigeria
Email: sc.chikwendu@unizik.edu.ng

Abstract
Background: Small and medium-sized enterprises (SMEs) in Nigeria face unique cybersecurity challenges due to limited resources, lack of dedicated IT personnel, and inadequate security budgets. Despite increasing digitalization of business operations, many SMEs operate without formal cybersecurity policies or structured training programmes, leaving them vulnerable to cyber threats such as phishing, ransomware, and data breaches.
Objective: This study examined the level of cybersecurity awareness among SMEs in Awka South LGA, Anambra State, and identified the factors influencing compliance with cybersecurity regulations and best practices.
Methods: The study adopted a mixed-methods research design. A sample size of 184 respondents was determined using the Taro Yamane formula, drawn from a population of 1,902 registered SMEs in Awka South LGA. A multi-stage sampling procedure was employed to select respondents across seven towns and fourteen business locations. Quantitative data were collected using structured questionnaires and analyzed using descriptive statistics (frequency distributions and percentages), while qualitative data were gathered through six in-depth interviews (IDIs) with business owners and managers and analyzed using thematic analysis. The Technology Acceptance Model (TAM) served as the theoretical framework.
Results: The findings revealed that while 40.9% of respondents reported high awareness of basic cybersecurity practices and 47.7% perceived cyber threats as high risk, only 33.0% had participated in formal cybersecurity training, and 63.6% lacked formal cybersecurity policies. Regarding compliance, lack of funds (39.8%) was the most frequently cited barrier, followed by lack of technical knowledge (30.7%), weak enforcement (18.2%), and low risk perception (11.3%). Furthermore, 75.0% of respondents indicated that financial capacity influences compliance, 84.1% identified technical expertise as a key factor, and 71.6% highlighted the role of organizational culture.
Objective: This study examined the level of cybersecurity awareness among SMEs in Awka South LGA, Anambra State, and identified the factors influencing compliance with cybersecurity regulations and best practices.
Methods: The study adopted a mixed methods research design. A sample size of 184 respondents was determined using the Taro Yamane formula, drawn from a population of 1,902 registered SMEs in Awka South LGA. A multi-stage sampling procedure was employed to select respondents across seven towns and fourteen business locations. Quantitative data were collected using structured questionnaires and analyzed using descriptive statistics (frequency distributions and percentages). Qualitative data were gathered through six In-Depth Interviews (IDIs) with business owners and managers, analyzed using thematic analysis. The Technology Acceptance Model (TAM) served as the theoretical framework.
Results: The findings revealed that while 40.9% of respondents reported high awareness of basic cybersecurity practices and 47.7% perceived cyber threats as high risk, only 33.0% had ever participated in formal cybersecurity training, and 63.6% lacked formal cybersecurity policies. Regarding compliance, lack of funds (39.8%) was the most frequently cited barrier, followed by lack of technical knowledge (30.7%), weak enforcement (18.2%), and low risk perception (11.3%). Furthermore, 75.0% of respondents affirmed that financial capacity influences compliance, 84.1% affirmed that technical expertise influences compliance, and 71.6% affirmed that organizational culture influences compliance.

Keywords: Cybersecurity awareness, compliance, small and medium-sized enterprises (SMEs), Technology Acceptance Model,

Introduction

Today's digital environment delivers unique security challenges to small and medium-sized enterprises (SMEs) regarding both cybersecurity awareness and corresponding standards. The pitfall of small and medium-sized enterprises involves working with minimal resources because they frequently lack a full-time IT security team and profound cybersecurity budgets (Daengsi et al, 2022). Akter et al (2021) noted that vital weak points exist due to the resource imbalance that cybercriminals exploit eagerly. They further stated that these businesses need urgent development of a comprehensive cybersecurity awareness initiative. An organization should start by comprehending threats while understanding data protection value and establishing effective defense methods to reduce exposure to these risks (Vrhovec & Markelj, 2024).

Risk management enables SMEs to make effective cybersecurity decisions by helping them establish priority order for their security initiatives. Businesses who perform routine risk assessments will understand which assets represent their most value and what vulnerabilities exist. The method helps organizations direct their funds to defend essential data and systems while reducing their commitment to safeguarding unimportant areas (Haney & Lutters, 2020). Using technology solutions that were made specifically for SMEs makes another fundamental contribution to their cybersecurity measures. According to Rohan et al (2023), cloud-based security solutions enable small organizations to obtain sophisticated security programmes at flexible prices without requiring substantial initial capital expenditures. Intrusion detection systems firewalls endpoint protection among other essential features are typically found in these security services which defend sensitive data against cyber-attacks. Small and medium-sized enterprises (SMEs) in Nigeria encounter a complex cybersecurity environment which has grown more intricate during the last years. These organizations experience distinct business obstacles which result from their limited resources alongside inadequate specialized understanding and dynamic threat conditions (Rawindaran et al, 2022). The accelerated digital transformation of different sectors leads SMEs to depend increasingly on technological infrastructure for conducting their operations. The dependency of these systems makes businesses highly susceptible to cybercriminals who attack unprotected network vulnerabilities. These enterprises need proper cybersecurity training alongside regulatory compliance standards to maintain security levels effectively (Ilca et al, 2023).

Small and medium enterprise organizations in Nigeria struggle to maintain cybersecurity awareness and compliance because business owners do not recognize the essential value of cybersecurity protection (Irhebhude et al, 2022). Small to medium-sized business leaders often view cybersecurity costs as superfluous commitments because they fail to recognize how essential security measures are for business integrity and public image (Hasani et al, 2023). This misunderstanding causes businesses to implement insufficient security protocols which includes weak passwords and neglected maintenance of software alongside inadequate training of workers to recognize cyber threats. SMEs typically lack enough IT personnel together with funding to put in place robust cybersecurity approaches despite their limited technical expertise. The reliance on basic security practices by these entities results in the inability to protect themselves against contemporary cybercriminal techniques (Kariuki et al, 2023). Based on the foregoing, two objectives were put forward to guide the study namely: to determine the current levels of cybersecurity awareness among small and medium-sized enterprises (SMEs) in Awka South LGA, Anambra State and to determine the factors influencing compliance to cybersecurity regulations among small and medium-sized enterprises (SMEs) in Awka South LGA, Anambra State

Related Literature

Cybersecurity Awareness and Compliance

Haney and Lutters (2020) stated that **cybersecurity awareness and compliance re**fers to the combination of knowledge, attitudes, and practices that individuals and organizations adopt to recognize cyber threats and to act in accordance with established security standards and policies. They noted that awareness entails understanding risks such as phishing, ransomware, data breaches, and identity theft, as well as knowing how to respond effectively to minimize vulnerabilities. Compliance, on the other hand, involves aligning behaviors and organizational processes with legal, regulatory, and institutional requirements designed to safeguard information systems. Cybersecurity awareness and compliance matter because many security breaches happen when people make mistakes or ignore warnings. Training and policies work hand in hand: awareness gives people the knowledge to spot threats like phishing emails, unsafe networks, and weak passwords, while compliance turns that knowledge into daily habits through clear rules and responsibilities. Haney and Lutters (2020) note that awareness provides the foundation for recognizing risks, and compliance ensures those lessons are consistently applied. Uchendu et al. (2021) add that leadership support and consistent messaging are essential for building a strong security culture, since people are more likely to follow practices that leaders reinforce and reward. When awareness is treated as a onetime event and compliance as a box ticking exercise, organizations stay vulnerable. But when education is meaningful and rules are practical, security behaviors become routine and risks are reduced. For awareness programs to actually change behavior, they must be engaging, practical, and continuous. Haney and Lutters (2020) recommend short, varied learning methods such as micro training, real life scenarios, and timely reminders so security stays fresh instead of being just an annual task. Chaudhary et al. (2022) argue that awareness programs should be measured with clear metrics like sustainability, accessibility, and impact so leaders can see what works. Simulated phishing exercises are especially useful when they combine testing with immediate feedback and follow up instruction. Training is most effective when it connects directly to people's daily work. Alotaibi et al. (2023) highlight that in today's hybrid work environment, awareness should cover both home and office risks, helping remote workers make secure choices wherever they are. Compliance frameworks provide the structure that turns good intentions into consistent practices. ISO's information security management standard (ISO, 2022) sets requirements for defining roles, performing risk assessments, and managing controls in a systematic way. Research shows that certification and careful implementation of ISMS can lead to real operational

benefits. Podrecca et al. (2022) note that compliance works best when it aligns with business processes rather than being treated as an extra burden. Well-designed controls such as access management, patching routines, and incident reporting systems reduce the chance of human error, while clear governance ensures accountability and effective auditing.

Knowledge alone is not enough, because under time pressure people often take shortcuts, especially when tools are inconvenient. Closing this knowing doing gap requires both cultural and technical solutions. Haney and Lutters (2020) caution that a box ticking approach has little impact, and stress that training should use advocacy and creativity to keep people engaged. Uchendu et al. (2021) emphasize that leaders must set the example and create a safe environment where employees can report mistakes without fear. Chaudhary et al. (2022) recommend measuring not just fewer risky clicks but also positive actions like reporting suspicious items, since these show that secure habits are becoming routine. Making security easier through tools such as single sign on and multi factor authentication, combined with recognition for good practice, helps turn awareness into lasting habits. Lasting progress requires a combined approach that blends education, compliance, user friendly tools, and continuous evaluation. Chaudhary et al. (2022) suggest that programs should be assessed based on impact and sustainability so resources go to what truly changes behavior. Alotaibi et al. (2023) stress the importance of tailoring materials for different work settings so guidance is practical for everyone. Haney and Lutters (2020) point out that security trainers need strong communication skills to make learning engaging rather than dull. Finally, standards like ISO 27001 provide a governance roadmap, and research shows disciplined adoption improves resilience (ISO, 2022; Podrecca et al., 2022). Together, these elements create a security culture where awareness and compliance reinforce each other, reducing the human risks attackers often exploit.

Small and Medium-sized Enterprises (SMEs) Defined

Small and Medium-sized Enterprises (SMEs) are widely recognized as the foundation of economic activity, contributing to productivity, innovation, and employment across diverse economies. Although definitions vary, SMEs are commonly classified by size, turnover, and assets, with countries applying their own thresholds. The European Commission (2020) identifies SMEs as firms employing fewer than 250 people, while other economies use different cut-offs depending on sector and national policy. The International Labour Organization (2021) emphasizes that SMEs account for a significant share of global businesses, particularly in emerging markets where they dominate the private sector landscape. Baporikar (2020) argues that SMEs embody flexibility and entrepreneurial drive, making them adaptive to rapidly changing markets and consumer needs. Their ability to operate in both formal and informal sectors makes them inclusive actors, bridging economic gaps. By linking small-scale entrepreneurial energy with larger value chains, SMEs serve as a conceptual bridge between microenterprises and large corporations, embodying resilience, innovation, and inclusivity in one framework.

The role of SMEs in job creation remains one of the most important aspects of their conceptual significance. They are not merely business entities but also employment drivers, absorbing a large share of labor and reducing unemployment pressures. According to the International Trade Centre (2020), SMEs provide around 70 percent of total employment in many developing economies, demonstrating their role in expanding labor markets. Herrington and Kew (2020) note that entrepreneurship through SMEs creates opportunities for youth and women, groups often excluded from formal employment in large corporations. Similarly, Olanrewaju and George (2021) highlight that SMEs in African economies remain the largest employers of the working population, showing their importance in addressing job scarcity. Beyond numbers, SMEs contribute to skills development and human capital growth by providing on-the-job training and fostering entrepreneurship. Their embeddedness in local economies means they generate employment opportunities that are both geographically dispersed and socially inclusive. This employment dimension reveals why SMEs are central not only to business growth but also to broader social and economic transformation.

Another defining aspect of SMEs is their contribution to innovation and competitiveness in markets. SMEs are often agile, capable of experimenting with new technologies, processes, and business models. United Nations Industrial Development Organization (2020) underscores that SMEs act as catalysts for industrial development through incremental and frugal innovation, which adapts products and services to local needs. Ali and Agyapong (2021) show that SMEs in Africa frequently innovate in resource-constrained environments by tailoring solutions to specific community challenges. Similarly, Bhattacharya and Londhe (2021) stress that SMEs enhance competition by preventing monopolistic dominance, thereby ensuring diversity in products and services. In the digital age, SMEs are also drivers of technological adoption, integrating e-commerce, fintech, and green practices into business models. This adaptability makes them central players in competitive markets, keeping larger firms accountable while fueling dynamic growth. Thus, within their conceptual framework, SMEs represent not only scale-based enterprises but also engines of creativity and competitive vibrancy.

Despite their importance, SMEs face constraints that shape how the concept is understood in practical terms. Limited access to finance is often cited as a critical barrier, as banks and investors perceive SMEs as risky due to inadequate collateral and limited credit histories. According to Beck and Cull (2021), financing constraints hinder SMEs' ability to scale and modernize. Fatoki (2020) notes that managerial inefficiencies, lack of strategic planning, and poor access to technology exacerbate the difficulties SMEs face in sustaining growth. Similarly, Lawal and Ijaiya (2020) emphasize that regulatory bottlenecks and inconsistent government support policies discourage expansion, leaving many SMEs trapped in survival mode. These challenges highlight the vulnerability of SMEs to external shocks such as economic downturns or public health crises. The COVID-19 pandemic, as underscored by Shafi, Liu, and Ren (2020), exposed how fragile many SMEs are, with widespread closures due to weak financial buffers. Therefore, the concept of SMEs includes not only their contributions but also the systemic limitations that condition their development.

Conceptually, SMEs are increasingly viewed as instruments of inclusive and sustainable development. Their impact goes beyond business to social empowerment, community resilience, and equitable growth. The United Nations (2021) acknowledges SMEs as vital partners in achieving the Sustainable Development Goals, particularly in reducing poverty, promoting decent work, and fostering innovation. According to Asare, Acquah, and Baah (2021), SMEs help expand economic participation by empowering marginalized groups, thus promoting inclusive development. Similarly, Ngek (2020) argues that supporting SMEs through targeted policies enhances economic diversification and resilience against external shocks. As the global economy becomes more interconnected, SMEs are also playing larger roles in global value chains, integrating local production into international markets. Their conceptual framework now includes sustainability, digitalization, and global integration as defining characteristics. Understanding SMEs in this broader sense emphasizes their role not just as small businesses, but as key drivers of long-term development strategies across diverse economic systems.

Current Levels of Cybersecurity Awareness among Small and Medium-sized Enterprises (SMEs)

Small and medium sized enterprises (SMEs) have become central actors in the global economy, yet their growing reliance on digital platforms exposes them to cybersecurity threats that require awareness beyond technical compliance. For SMEs, cybersecurity awareness means recognizing the range of threats, understanding vulnerabilities, and integrating preventive behaviors into daily operations. Erdogan et al. (2023) note that although SMEs recognize cyber risks, their awareness is often fragmented and limited to surface level practices such as antivirus use or password management. Shojaifar and Järvinen (2021) add that awareness levels vary depending on management orientation, with some SMEs ignoring security entirely while others adopt only minimal defensive measures. This unevenness shows that awareness is not evenly distributed but shaped by competing priorities such as finance, marketing, and business survival. When cybersecurity is framed as an external burden instead of an internal necessity, SMEs remain vulnerable to attacks that exploit organizational inattentiveness. In this sense, cybersecurity awareness is not just a technical issue but a structural capability tied to SME survival.

The environments in which SMEs operate also shape awareness. In Africa, weak institutions and infrastructural challenges make awareness especially fragile. Kergroach and Pedota (2024) explain that SMEs in Kenya struggle with limited capacity to manage risks because of low institutional support and restricted digital literacy, creating awareness gaps that hurt productivity. Similarly, Olanrewaju and George (2021) add that African SMEs often lack structured cybersecurity training, which perpetuates cycles of vulnerability. These findings show that in resource constrained economies, awareness is not only an internal problem but also shaped by poverty, limited infrastructure, and weak regulation. As a result, many SMEs are unable to build the awareness needed to protect themselves, even as they become more dependent on digital markets.

Outside Africa, SMEs in Asia and Europe display somewhat higher awareness levels, though major gaps remain. Zwilling et al. (2022) find that Malaysian SMEs recognize cyber threats in theory but often practice only basic protective behaviors, lacking deeper situational awareness. Stoyanova (2023) observes that many European SMEs acknowledge the need for cybersecurity but underinvest in awareness training and risk management due to financial pressure and competing priorities. This paradox reflects the broader challenge: awareness exists at a surface level, but action is limited because entrepreneurs see security as a cost rather than an investment. Curtin et al. (2024) argue that structured tools can help SMEs bridge this gap by simplifying cyber risks and translating awareness into practical steps. With the right frameworks, SMEs can move from superficial recognition of threats to embedding awareness into everyday practice.

Organizational culture also plays a crucial role in shaping awareness. Erdogan et al. (2023) stress that awareness improves when managers treat cybersecurity as part of strategic decision making rather than leaving it to technical staff. Shojaifar and Järvinen (2021) note that SMEs with engaged leadership are more likely to spread awareness across employees, creating cultures where secure behaviors become routine. In contrast, firms that treat

cybersecurity as a one off compliance task rarely achieve sustainable awareness. Stoyanova (2023) highlights that collective initiatives, where SMEs collaborate and share best practices, further strengthen awareness and resilience. These cultural and behavioral factors show that awareness is not just about knowledge but about mindset, daily routines, and shared responsibility. When cybersecurity is seen as everyone's concern, SMEs are more likely to integrate it into their operations.

Al-Kayed et al. (2024) explored the influence of cybersecurity on strategic decision-making among small and medium-sized enterprises (SMEs) in Balqa Governorate, Jordan, emphasizing the role of technological infrastructure. The quantitative study surveyed 360 SME managers using structured questionnaires, with data analyzed through SPSS. Findings indicated that strong cybersecurity measures positively impacted SMEs' strategic choices, particularly in safeguarding customer data and enhancing organizational reputation. Nevertheless, the study highlighted a critical limitation: many SMEs lacked sufficient technological infrastructure to effectively implement these cybersecurity practices. This underscores the interplay between cybersecurity readiness and technological capacity, suggesting that strategic benefits can only be realized when firms possess both awareness and the necessary infrastructure to operationalize protective measures.

Erdogan et al. (2023) assessed the cybersecurity awareness and capacities of SMEs in the UK, drawing attention to the gap between basic practices and advanced preparedness. Using a cross-sectional design, the study surveyed 141 SMEs through an online questionnaire and applied descriptive statistical analysis to evaluate awareness and practices. The results showed that although many SMEs had adopted fundamental cybersecurity measures, such as antivirus software and password protections, there was limited awareness of sophisticated cyber threats and emerging risks. Furthermore, most firms lacked formal cybersecurity policies and structured training programs, leaving them vulnerable to evolving threats. The study highlights the need for greater emphasis on capacity building, policy development, and continuous training to strengthen SME resilience in a rapidly changing cybersecurity landscape.

Factors influencing Compliance to Cybersecurity Regulations among Small and Medium-sized Enterprises (SMEs)

Compliance with cybersecurity regulations among small and medium sized enterprises (SMEs) is increasingly important in today's interconnected economy, where digital risks continue to grow. Yet compliance is rarely simple, as it depends on both internal and external factors that shape how SMEs interpret and respond to regulations. Rombaldo Junior et al. (2023) note that many SMEs lack the literacy to fully understand complex regulatory texts, which leads to partial or inconsistent compliance. Erdogan et al. (2023) add that entrepreneurs often prioritize day to day survival over regulatory obligations, making cybersecurity a secondary concern. This tension between business pragmatism and regulatory requirements is particularly challenging for smaller firms with limited technical expertise. As a result, compliance is not only about willingness but also about having the cognitive and resource capacity to understand and implement what regulations demand without disrupting business continuity.

Employee behavior and organizational culture also play a central role in compliance. Shojaifar and Järvinen (2021) describe SMEs along a spectrum, ranging from firms that neglect basic security to those that integrate secure practices into their routines. Curtin et al. (2024) emphasize that leadership is critical, since managers influence whether employees see compliance as meaningful or as a burden. When leaders frame cybersecurity as part of organizational identity, employees are more likely to adopt secure practices willingly. But if regulations are presented as external impositions, staff often treat compliance as irrelevant bureaucracy. Stoyanova (2023) highlights that collective initiatives, such as collaboration and shared learning across SMEs, help normalize compliance behaviors. Culture therefore matters as much as technical knowledge, because it determines whether compliance becomes part of everyday practice or remains a one off enforcement exercise.

The regulatory environment itself also affects SME compliance. Kergroach and Pedota (2024) show that in Kenya, SMEs face overlapping regulatory requirements that are often unclear and poorly adapted to smaller businesses. This complexity discourages compliance by overwhelming firms with obligations that exceed their capacity. In Nigeria, Osifeko (2025) points out challenges arising from overlapping frameworks like the Nigeria Data Protection Act and the Cybercrimes Amendment Act, which smaller enterprises struggle to interpret. Without simplification, SMEs often resort to partial compliance, fulfilling only what they understand or can afford. Clearer, streamlined rules designed with SMEs in mind encourage stronger compliance, while fragmented and overly technical frameworks create confusion and resistance.

Financial and technical capacities are another reason compliance is uneven. Zwilling et al. (2022) show that SMEs often lack the budget for dedicated staff, cybersecurity tools, or third party audits, leaving them poorly equipped

to meet standards. Fatoki (2020) adds that this problem is even more severe in developing economies, where SMEs rely on outdated systems and cannot afford expensive compliance programs. Many SMEs also believe they are unlikely to be targeted, which fosters complacency and discourages investment in security. Yet breaches can have devastating consequences, from financial penalties and reputational damage to disrupted operations. This shows that compliance depends heavily on resources, which most SMEs struggle to secure. Without addressing these gaps, regulations will remain aspirational rather than achievable.

Bokhari (2023) examined the determinants of cybersecurity law implementation in Pakistan, focusing on the challenges faced by managers in banking and IT firms within a developing country context. Employing a quantitative survey approach, the study collected data from 172 managers through a structured questionnaire administered using non-probability sampling. The analysis, conducted with descriptive statistics and multivariate techniques such as regression and hypothesis testing, assessed the influence of factors including corruption, expertise, ambiguity, trust, and related constructs. Results indicated that corruption, discrimination, and other forms of illicit conduct significantly hindered the effective implementation of cybersecurity laws, while managerial expertise and public confidence facilitated compliance and enforcement. Notably, corruption emerged as the strongest negative predictor, underscoring its pervasive role in weakening regulatory frameworks. The study highlights the dual necessity of curbing institutional corruption and enhancing managerial expertise to strengthen cybersecurity governance in developing economies.

Murphy et al. (2022) explored the barriers that small, medium, and micro enterprises (SMMEs) in South Africa face in complying with national cybersecurity policy, highlighting organizational and perceptual challenges. The study adopted a qualitative design, conducting semi-structured interviews with 20 purposively selected SMMEs to capture a diverse range of experiences. Data from interview transcripts were analyzed thematically, with findings presented through major themes supported by illustrative quotations. The results revealed three critical impediments: limited awareness and understanding of the national cybersecurity policy, resource constraints in terms of time, finances, and technical expertise, and a low perceived benefit of compliance among SMMEs. These findings underscore the disconnect between policy formulation and practical uptake, suggesting that without tailored awareness campaigns, financial support, and incentives, national cybersecurity frameworks risk limited effectiveness among resource-constrained enterprises.

In sum, compliance with cybersecurity regulations among SMEs is a multidimensional challenge shaped by literacy, culture, regulatory design, and resource capacity. Awareness provides the foundation, but it must be reinforced by leadership that integrates cybersecurity into organizational culture. Regulations need to be clear and proportionate, aligned with SME realities rather than copied from standards meant for large corporations. Financial support and accessible tools are also essential to close the gap between intention and practice. As Kergroach and Pedota (2024) argue, compliance cannot be achieved through obligation alone; it requires enabling conditions that make it practical and realistic for SMEs. Understanding these factors is key to designing interventions that not only impose rules but also empower SMEs to participate in securing the digital economy.

Theoretical Framework

The Technology Acceptance Model (TAM) was first proposed by Fred Davis in 1986 and further developed by Davis, Bagozzi, and Warshaw in 1989. As one of the most influential models in information systems research, TAM is grounded in the theory of reasoned action (TRA) and focuses on explaining user acceptance of technology. Its main tenets are perceived usefulness (the degree to which a person believes that using a system will enhance their job performance) and perceived ease of use (the degree to which a person believes that using the system will be free of effort). These constructs influence users' attitudes toward technology, their behavioral intentions, and ultimately their actual system usage.

In the context of evaluating cybersecurity awareness and compliance among SMEs in Anambra State, TAM provides a relevant lens. SMEs' adoption of cybersecurity practices depends largely on whether managers and employees perceive cybersecurity tools and awareness programs as useful in protecting business operations and whether they consider such tools easy to understand and apply. For instance, if SME owners perceive cybersecurity training as beneficial in reducing risks of fraud or data breaches, they are more likely to comply with recommended security protocols. Similarly, if the implementation of security software is perceived as straightforward and non-disruptive to daily business activities, compliance and awareness levels are likely to be higher. Thus, TAM helps explain the behavioral factors influencing SMEs' willingness to embrace cybersecurity measures beyond mere regulatory compulsion.

The Technology Acceptance Model (TAM) has been adopted as the theoretical framework for this study because it provides a clear and practical framework for understanding the factors influencing cybersecurity awareness and

compliance among SMEs in Anambra State. Cybersecurity practices and tools, like any other form of technology, require acceptance and adoption by users before they can be effective. TAM's core constructs, perceived usefulness and perceived ease of use are directly relevant to SMEs' decisions to engage with cybersecurity initiatives. If SME owners and employees believe that cybersecurity measures will significantly enhance business protection and are easy to implement, they are more likely to embrace and comply with them. By focusing on user perceptions and behavioral intentions, TAM helps explain not just whether SMEs comply, but why they choose to adopt or neglect cybersecurity practices, thereby aligning closely with the objectives of evaluating awareness and compliance in this context.

Methods

Sample and Sampling Procedure

The study was carried out in Awka South LGA, Anambra State. The study sample includes all registered small and medium enterprises (SMEs) in Awka South, Anambra State. According to Chiekezie, and Ikwuka, (2025), there are 1,902 registered SMEs in Awka South LGA, Anambra State. The sample size of184 respondents was statistically determined using the Taro Yamane (1967) formula. The formula is given as: $n = N/1+N (e)^2$. This study will adopt both probability and non-probability sampling methods, each serving a specific purpose in the research design. Probability sampling will enable the researcher to select a sample that accurately represents the characteristics of small and medium businesses in Awka South, ensuring a level of objectivity and representativeness. Non-probability sampling, on the other hand, provides flexibility in selecting businesses that meet particular criteria relevant to the study, such as type of business or length of operation, allowing the researcher to target respondents who can provide relevant information for the study objectives. A multi-stage sampling procedure will be adopted to manage the large and diverse population of businesses in Awka South. Awka South is made up of nine towns: Awka, Amawbia, Nibo, Mbaukwu, Nise, Umudioka, Isiagu, Ezinato, and Okpuno.

In the first stage, the nine towns will serve as the primary sampling units. To ensure geographical spread and representation of businesses across the LGA, two towns will be randomly excluded, leaving seven towns for the study. In the second stage, from each selected town, two major commercial areas will be listed and selected through simple random sampling. This will produce fourteen business locations across the seven towns. In the third stage, a list of registered small and medium businesses on each selected area will be compiled. Using systematic sampling with a random start, a predetermined number of businesses will be drawn. Specifically, 13 businesses will be selected from each of the fourteen business locations, yielding a total of 182 businesses ($14 \times 13 = 182$). To reach the exact sample size of 184, two additional businesses will be randomly selected from the town with the highest concentration of enterprises, typically Awka town, bringing the total to 184.

From each selected business, one eligible respondent, typically the owner, manager, or staff, will be administered a questionnaire. If no eligible respondent is available at the time of the visit, the next business on the sampling list was approached using the same systematic interval. For the qualitative component, purposive sampling was used to identify participants based on their knowledge of the study themes. Six participants were selected for In-Depth Interviews (IDIs), comprising 6 business owners/managers. The instruments for data collection for this study include sa questionnaire schedule, which was used to collect the quantitative data, and an In-Depth Interview (IDI) guide, which was used to collect the qualitative data. The questionnaire was divided into sections. Section A contained items designed to obtain data on the socio-demographic characteristics of the respondents, such as age, gender, marital status, educational qualification, religious affiliation, and occupation, while other sections contained items designed to collect information about the substantive issues of the study. The IDI guide was also being designed in simple English language, in line with the specific objectives of the study, and contains probes associated with each question. The IDI was used to obtain more detailed information on the theme of the study.

Data Analysis

The quantitative data that was collected from the field was processed using the Statistical Package for the Social Sciences (SPSS) software. The data was presented, analyzed, and interpreted using descriptive statistics such as frequency distribution, simple percentages, and graphic illustrations including pie charts, histograms, and bar charts. Furthermore, the hypotheses were tested using the chi-square (X^2) inferential statistics. This was done to test the relationship between the independent and dependent variables. On the other hand, the qualitative data that was collected through IDI was analyzed using thematic analysis. This involves first transcribing the interviews and thereafter reading the interview notes and transcripts to gain an overview of the body and context of the data collected. Subsequently, the variables and ideas in the data were coded and organized under distinct themes. Each theme was then discussed, and necessary illustrative quotes extracted to support and elucidate the quantitative data.

Results and Discussion

Personal Data of Respondents

This section deals with personal data of the respondents such as gender, age, educational qualification, and business category. The personal data of the respondents are presented in the table below.

Table 1: Personal Data of Respondents

Variable	Frequency	Percentage
Sex		
Male	102	58.0
Female	74	42.0
Total	176	100.0
Age		
18—29	48	27.3
30—39	66	37.5
40—49	42	23.9
50 and above	20	11.3
Total	176	100.0
Educational Qualification		
Secondary	46	26.1
OND/NCE	52	29.5
HND/Bachelor's Degree	58	33.0
Postgraduate	20	11.4
Total	176	100.0
Business Category		
Retail/Trading	68	38.6
Services	54	30.7
Hospitality	32	18.2
ICT-related	22	12.5
Total	176	100.0

Field Survey, 2026.

Table 1 shows that the majority of respondents (58.0%) were male. Table 1 also shows that the majority of the respondents (37.5%) are between the ages of 30—39. A further look at Table 1 shows that the majority of respondents (33.0%) possess HND/Bachelor's degrees. Finally, Table 1 shows that most respondents (38.6%) operate retail or trading businesses.

Analysis of Research Objectives

Research Objective One: What is the level of cybersecurity awareness among SMEs in Awka South LGA? Findings are presented in Tables 2, 3, 4, and 5.

Table 2: Awareness of basic cybersecurity practices among SMEs in Awka South LGA

Responses	Frequency	Percentage
High awareness	72	40.9
Moderate awareness	68	38.6
Low awareness	36	20.5
Total	176	100.0

Field Survey, 2026

Table 2 shows that the majority of respondents (40.9%) reported high awareness of basic cybersecurity practices. This shows that businesses and SMEs in Awka South LGA are aware of the cybersecurity practices prevalent in the study area.

Table 3: Participation in cybersecurity training

Responses	Frequency	Percentage
Yes	58	33.0
No	118	67.0
Total	176	100.0

Field Survey, 2026

Table 3 shows that most respondents (67.0%) have never participated in any formal cybersecurity training. This shows limited exposure to traninings that could impact on cybersecurity knowledge.

Table 4: Perception of cybersecurity risk among SMEs in Awka South LGA

Responses	Frequency	Percentage
High risk	84	47.7
Moderate risk	66	37.5

Low risk	26	14.8
Total	176	100.0

Field Survey, 2026

Table 4 shows that a large proportion of respondents (47.7%) perceive cybersecurity threats as high risk.

Table 5: Presence of cybersecurity policies in SMEs in Awka South LGA

Responses	Frequency	Percentage
Yes	64	36.4
No	112	63.6
Total	176	100.0

Field Survey, 2026

Table 5 shows that the majority of SMEs (63.6%) do not have formal cybersecurity policies.

This finding is supported by data from the IDI.

One of the interviewees stated:

We only react when something happens. There is no written policy. We just try to fix problems as they come. *(Male, 34, Business Owner)*

Another interviewee added:

Most small businesses don't think about cybersecurity until they are attacked. *(Female, 29, Manager)*

Objective Two: What factors influence cybersecurity compliance among SMEs? Questionnaire items 10, 11, 12, and 13 were designed to answer research question 2. Findings are presented in Tables 6, 7, 8, and 9.

Table 6: Major barriers to cybersecurity compliance among SMEs in Awka South LGA

Responses	Frequency	Percentage
Lack of funds	70	39.8
Lack of technical knowledge	54	30.7
Weak enforcement	32	18.2
Low risk perception	20	11.3
Total	176	100.0

Field Survey, 2026

Table 6 shows that lack of funds (39.8%) is the major barrier to cybersecurity compliance.

Table 7: Influence of financial capacity on compliance

Responses	Frequency	Percentage
Yes	132	75.0
No	44	25.0
Total	176	100.0

Field Survey, 2026

Table 8: Influence of technical expertise on compliance

Responses	Frequency	Percentage
Yes	148	84.1
No	28	15.9
Total	176	100.0

Field Survey, 2026

Table 9: Role of organizational culture in compliance

Responses	Frequency	Percentage
Yes	126	71.6
No	50	28.4
Total	176	100.0

Field Survey, 2026

Tables 7, 8, and 9 show that financial capacity, technical expertise, and organizational culture significantly influence cybersecurity compliance. This finding is supported by the IDI responses.

One interviewee stated:

We know security is important but money is always the problem. *(Male, 41, Trader)*

Another interviewee added:

Even if you have money, without technical knowledge you cannot protect your system. *(Female, 35, ICT Staff)*

Discussion

This study examined the level of cybersecurity awareness, compliance behavior, perceived consequences of poor cybersecurity practices, and possible improvement measures among SMEs in Awka South LGA. The findings reveal important patterns about the preparedness of SMEs to manage cybersecurity risks and the structural factors that influence their behavior. First, the study assessed the level of cybersecurity awareness among SMEs. The

findings show that awareness is relatively high, as a plurality of respondents reported high awareness of basic cybersecurity practices. Additionally, most respondents perceived cybersecurity threats as high risk. This suggests that cybersecurity is no longer viewed as a distant or abstract issue but as a real and present danger to business operations. However, despite this awareness, the majority of SMEs had not participated in any formal cybersecurity training and did not have written cybersecurity policies. This gap between awareness and structured action indicates that while SMEs recognize the importance of cybersecurity, they lack the institutional framework and technical capacity needed to translate awareness into consistent practice. The qualitative responses reinforce this conclusion, as interviewees admitted that many businesses operate reactively rather than proactively. Regarding the factors influencing cybersecurity compliance, financial constraint emerged as the most significant barrier. A large proportion of respondents identified lack of funds as the main obstacle to implementing proper cybersecurity measures. This is consistent with the broader economic reality of SMEs, which often operate with limited capital and prioritize immediate operational needs over long-term security investments. Respondents also strongly acknowledged the importance of technical expertise and organizational culture. The data suggest that compliance is not determined by finances alone; knowledge, internal management practices, and workplace attitudes toward security also play crucial roles. Interview responses further illustrate that even when funds are available, lack of technical knowledge can undermine effective protection. This highlights the multidimensional nature of cybersecurity compliance, which requires financial, educational, and organizational support.

Conclusion

The study concludes that the cybersecurity challenges facing SMEs in Awka South LGA are driven less by lack of awareness and more by constraints related to capacity and affordability. Although business owners recognize the seriousness of cyber threats, limited financial resources and inadequate technical expertise hinder the consistent implementation of effective security measures. The findings indicate that cybersecurity vulnerability among SMEs is primarily rooted in structural and economic limitations rather than ignorance. Even where awareness exists, many enterprises lack the institutional support required for proactive engagement. Consequently, the problem is systemic: SMEs operate in a digital environment that demands sustained investment in security, yet the cost and complexity of adequate protection exceed their individual capacities. Without external support, SMEs are likely to remain reactive, addressing cyber incidents only after damage has occurred.

References

Ali, M., & Agyapong, F. O. (2021). Innovation practices and the performance of SMEs in Africa. *Journal of Entrepreneurship in Emerging Economies, 13*(5), 857--873. https://doi.org/10.1108/JEEE-02-2020-0035

Al-Kayed, W. J., Alghizzawi, M., & Alkloub, R. S. A. (2024). The impact of cybersecurity on SMEs strategies through technological infrastructure in Balqa governorate. *Journal of Innovation and Development*, 8(15), 8194. https://doi.org/10.36959/8194

Alotaibi, F., Furnell, S., & He, Y. (2023). Cyber security awareness and education support for home and hybrid workers. In N. Clarke & S. Furnell (Eds.), *Human aspects of information security and assurance* (pp. 64--75). Springer. https://doi.org/10.1007/978-3-031-38530-8_6

Asare, R., Acquah, I. S. K., & Baah, C. (2021). Promoting inclusive development through SMEs. *International Journal of Business and Globalisation, 27*(4), 478--495. https://doi.org/10.1504/IJBG.2021.116278

Baporikar, N. (2020). SMEs and global challenges. *International Journal of Entrepreneurship and Small Business, 40*(3), 291--306. https://doi.org/10.1504/IJESB.2020.105530

Beck, T., & Cull, R. (2021). SME finance in Africa. *Journal of African Economies, 30*(1), i13--i54. https://doi.org/10.1093/jae/ejaa018

Bhattacharya, S., & Londhe, B. R. (2021). Competitiveness of SMEs in emerging markets. *Global Business Review, 22*(6), 1387--1402. https://doi.org/10.1177/0972150919837075

Bokhari, S. A. A. (2023). A quantitative study on the factors influencing implementation of cybersecurity laws and regulations in Pakistan. *Social Sciences, 12*, 629. https://doi.org/10.3390/socsci12110629

Chaudhary, S., Gkioulos, V., & Katsikas, S. (2022). Developing metrics to assess the effectiveness of cybersecurity awareness programs. *Journal of Cybersecurity, 8*(1), tyac006. https://doi.org/10.1093/cybsec/tyac006

Chiekezie, O. M., & Ikwuka, P. C. (2025). Entrepreneurial skills development and performance of small and medium enterprises in Awka-South Local Government Area, Anambra State. *International Journal of Business and Management Review, 6*(2).

Curtin, S., Sheehan, B., Gruben, K., Smith, J., & O'Donnell, M. (2024). Development of a cyber risk assessment tool for Irish small business owners. *Journal of Cybersecurity Practice and Research, 3*(1), 45--62.

Daengsi, T., Pornpongtechavanich, P., & Wuttidittachotti, P. (2022). Cybersecurity awareness enhancement: A study of the effects of age and gender of Thai employees associated with phishing attacks. *Education and Information Technologies, 27*(4), 4729--4752. https://doi.org/10.1007/s10639-021-10806-7

Erdogan, A., Halvorsrud, R., Pickering, J. B., Boletsis, C., & Tverdal, E. (2023). Cybersecurity awareness and capacities of SMEs. In *Proceedings of the 9th International Conference on Information Systems Security and Privacy* (pp. 128--139). SCITEPRESS.

European Commission. (2020). *User guide to the SME definition*. Publications Office of the European Union. https://doi.org/10.2873/87310

Fatoki, O. (2020). Challenges facing small and medium enterprises in South Africa. *Journal of Economics and Behavioral Studies, 12*(1), 48--56.

Haney, J., & Lutters, W. (2020). Security awareness training for the workforce: Moving beyond "check-the-box" compliance. *Computer, 53*(10), 10.1109/mc.2020.3001959. https://doi.org/10.1109/mc.2020.3001959

Hasani, T., O'Reilly, N., Dehghantanha, A., Rezania, D., & Levallet, N. (2023). Evaluating the adoption of cybersecurity and its influence on organizational performance. *SN Business & Economics, 3*(5), 97. https://doi.org/10.1007/s43546-023-00477-6

Herrington, M., & Kew, P. (2020). *Global Entrepreneurship Monitor 2020/2021 global report*. Global Entrepreneurship Research Association.

Ilca, L. F., Lucian, O. P., & Balan, T. C. (2023). Enhancing cyber-resilience for small and medium-sized organizations with prescriptive malware analysis, detection and response. *Sensors (Basel, Switzerland), 23*(15), 6757. https://doi.org/10.3390/s23156757

International Labour Organization (ILO). (2021). *SMEs and employment creation: Key statistics and trends*. ILO Publishing.

International Organization for Standardization. (2022). *ISO/IEC 27001:2022 information security, cybersecurity and privacy protection — information security management systems — requirements*. ISO. https://www.iso.org/standard/27001.html

International Trade Centre. (2020). *SMEs: Drivers of sustainable development*. ITC Publishing.

Irhebhude, M.E., Kolawole, A.O., Yashim, M.S., & Agwi, C.U. (2022). Cybersecurity awareness among public sector employees of Kaduna State E-Government system. *NDA Journal of Military Science and Interdisciplinary Studies, 1*(2), 69-82.

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*, 1--30. https://doi.org/10.1057/s41284-023-00378-1

Kergroach, A., & Pedota, P. (2024). Cyberattack, cyber risk mitigation capabilities, and firm productivity in Kenya. *Small Business Economics, 62*(3), 1123--1142. https://doi.org/10.1007/s11187-024-00946-8

Lawal, F., & Ijaiya, T. (2020). Government policies and SME growth in Nigeria. *Ilorin Journal of Economic Policy, 7*(2), 45--58.

Murphy, C., Mtegha, C. Q., Chigona, W., & Tuyeni, T. T. (2022). *Factors affecting compliance with the national cybersecurity policy by SMMEs in South Africa.* Conference / ACIST proceedings.

Ngek, N. (2020). SME development and inclusive growth in sub-Saharan Africa. *African Journal of Economic and Management Studies, 11*(2), 317--331. https://doi.org/10.1108/AJEMS-08-2019-0311

Olanrewaju, A., & George, O. J. (2021). SMEs and employment generation in African economies. *Journal of African Business, 22*(3), 327--345. https://doi.org/10.1080/15228916.2020.1775644

Osifeko, A. (2025, March 5). Why cybersecurity is important to Nigeria's startups, SMEs. *Vanguard Nigeria*.

Podrecca, M., Culot, G., Nassimbeni, G., & Sartor, M. (2022). Information security and value creation: The performance implications of ISO/IEC 27001. *Computers in Industry, 142*, 103744. https://doi.org/10.1016/j.compind.2022.103744

Rawindaran, N., Jayal, A., & Prakash, E. (2022). Exploration of the impact of cybersecurity awareness on small and medium enterprises (SMEs) in Wales using intelligent software to combat cybercrime. *Computers, 11*(12), 174. https://doi.org/10.3390/computers11120174

Rohan, R., Pal, D., Hautamäki, J., Funilkul, S., Chutimaskul, W., & Thapliyal, H. (2023). A systematic literature review of cybersecurity scales assessing information security awareness. *Heliyon, 9*(3), e14234. https://doi.org/10.1016/j.heliyon.2023.e14234

Rombaldo Junior, C., Becker, I., & Johnson, S. (2023). *Unaware, unfunded and uneducated: A systematic review of SME cybersecurity*. *Preprint*.

Shafi, M., Liu, J., & Ren, W. (2020). Impact of COVID-19 pandemic on SMEs in Pakistan. *International Journal of Environmental Research and Public Health, 17*(21), 8082. https://doi.org/10.3390/ijerph17218082

Shojaifar, A., & Järvinen, H. (2021). Classifying SMEs for approaching cybersecurity competence and awareness. *Journal of Information Security and Applications, 59*, 102837. https://doi.org/10.1016/j.jisa.2021.102837

Stoyanova, M. (2023). IT security awareness among SMEs in Europe. *Cybersecurity: Theory and Practice, 4*(2), 53--66.

Taro Yamane (1967). *Statistics: An Introductory Analysis* (2nd ed.). Harper and Row.

Uchendu, B., Nurse, J. R. C., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. *Computers & Security, 109*, 102387. https://doi.org/10.1016/j.cose.2021.102387

United Nations. (2021). *Micro-, small and medium-sized enterprises day: Statement by the Secretary-General*. United Nations.

United Nations Industrial Development Organization (UNIDO). (2020). *The role of SMEs in industrial development*. UNIDO Publishing.

Vrhovec, S., & Markelj, B. (2024). We need to aim at the top: Factors associated with cybersecurity awareness of cyber and information security decision-makers. *PloS One, 19*(10), e0312266. https://doi.org/10.1371/journal.pone.0312266

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, L., Cetin, F., & Basim, H. N. (2022). Cyber situational awareness of small and medium-sized enterprises in Malaysia. *Journal of Informatics and Web Engineering, 5*(1), 130--144.