CHALLENGES SMALL AND MEDIUM-SIZED ENTERPRISES (SMES) FACE IN IMPLEMENTING EFFECTIVE CYBERSECURITY MEASURES IN AWKA SOUTH LGA

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

Abstract
Background: Cybersecurity protocol adherence among SMEs appears to be low, with consequences that can negatively affect business operations and profitability. Despite increasing digitalization of business operations, many SMEs still operate without formal cybersecurity policies, leaving them vulnerable to cyberattacks.
Objective: This study examined the consequences of lack of awareness and compliance with cybersecurity protocols among Small and Medium-sized Enterprises (SMEs) in Anambra State, as well as measures to address these challenges.
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 Resource-Based Theory (RBT) was adopted as the theoretical framework.
Findings: Training and awareness programs were identified as the most important solutions, followed closely by government support and subsidized cybersecurity tools.

Keywords: cyber security, small and medium-sized enterprises, protocol, awareness, cyber-attacks.

Introduction

The economic operation of Anambra State Nigeria depends substantially on small and medium-sized enterprises (SMEs). Small and medium-sized enterprises operating in Anambra State must navigate through major cybersecurity challenges related to awareness training and regulatory requirements. Lack of financial as well as human resources represent the primary difficulties faced by these businesses during their cybersecurity awareness implementation (Mishra et al, 2022). Most small to medium enterprises work with limited financial resources thus they must frequently avoid spending on proper cybersecurity security solutions. The financial limitations prevent these organizations from putting into practice strong security protocols or implementing employee training or hiring the specialized professionals needed to handle cybersecurity risks adequately (Adeniran, 2019).

SME owners and their employees demonstrate limited understanding of the cybersecurity dangers that exist in the online world. The awareness level for cyber threats among small business operators is often limited because they do not have a complete understanding of potential risks from phishing attacks, ransomware and data breaches (Hasani et al, 2023). The insufficient knowledge about cybersecurity threats among individuals leads them to show indifference toward implementing proper security measures. Organizational cyber security is at greater risk when employees unknowingly commit risky actions like making simple password choices and missing suspect email notifications (Ilca et al, 2023).

SMEs in many states like Anambra State face substantial barriers when trying to meet regulatory compliance standards (Amirin, 2019). The Nigerian government established new regulations to boost cybersecurity in all sectors yet numerous SMEs encounter problems in meeting these standards because they lack appropriate knowledge or financial capability (Polkowsi & Dysarz, 2017). Small business owners face difficulties in managing operational responsibilities because specific compliance requirements may seem burdensome to implement new policies and procedures (Abdulmajeed & Bob, 2020). Non-compliance with regulations produces negative legal impacts while simultaneously harming a business's professional standing Yeboah-Boateng, 2023).

The requirement to follow regulatory standards creates a major obstacle for business enterprises in Anambra State. Multiple cybersecurity regulations from the Nigerian government now exist for sectors across the country yet smaller businesses in Anambra State find it difficult to comply because they lack understanding or proper resources (Amirin, 2019). The requirement for compliance forces business owners to put in place specific rules and process frameworks that they commonly view as time-consuming given their already demanding parts managing their daily operations. Such non-compliance actions expose SMEs to legal consequences which simultaneously jeopardize their established brand image (Akter et al, 2022). Additionally, there is a notable gap in collaboration between SMEs and larger organizations or governmental bodies that could provide support in enhancing cybersecurity measures. Larger corporations typically have more resources dedicated to cybersecurity initiatives and could potentially share knowledge or tools with smaller enterprises. However, this kind of collaboration is often lacking, leaving many SMEs isolated in their efforts to combat cyber threats (Adeniran, 2019). This paper therefore looked at the Challenges Small and Medium-sized Enterprises (SMEs) face in Implementing Effective Cybersecurity Measures in Awka South LGA

Literature Review

Defining SMEs

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.

Small and medium-sized enterprises (SMEs) are critical drivers of economic growth, innovation, and employment in many parts of the world (International Labour Organization, 2021). However, their increasing reliance on digital technologies exposes them to numerous cybersecurity risks. Cyberattacks such as phishing, ransomware, malware infiltration, and data breaches are no longer limited to large corporations; they have become common threats for smaller firms as well (Zwilling et al., 2022). Unfortunately, SMEs are often ill-equipped to deal with these challenges due to resource limitations and structural weaknesses. Implementing robust cybersecurity measures requires more than just awareness; it demands technical expertise, financial investment, regulatory compliance, and organizational commitment (Abdulmajeed & Bob, 2020). Yet, many SMEs struggle in these areas, leaving them vulnerable to attacks that could cripple their operations.

One of the most significant obstacles SMEs face in enhancing cybersecurity is limited financial resources. Unlike large corporations that allocate substantial budgets to cybersecurity infrastructure, SMEs typically operate on tighter margins and prioritize revenue-generating activities over security investments (Beck & Cull, 2021). Advanced security systems such as intrusion detection tools, endpoint protection, and encryption software can be costly to procure and maintain. Moreover, many SMEs cannot afford to hire dedicated cybersecurity specialists or outsource to managed security providers, forcing them to rely on basic or outdated solutions (Baporikar, 2020). This cost constraint often leads to a reactive rather than proactive approach, where SMEs only invest in security after suffering a breach. Unfortunately, by the time a breach occurs, the financial and reputational damage may already be irreparable (Mugwagwa et al., 2024).

Another critical challenge lies in the lack of cybersecurity expertise and awareness within SMEs. Many small business owners and employees have limited knowledge of cybersecurity best practices, making them susceptible to human error, which is one of the leading causes of breaches (Haney & Lutters, 2020). For instance, employees may use weak passwords, fall for phishing scams, or fail to update software regularly, inadvertently creating entry points for attackers (Alhuwail et al., 2021). Unlike larger firms that can afford regular staff training and awareness programs, SMEs rarely implement structured capacity-building initiatives (Shojaifar & Järvinen, 2021). The absence of skilled personnel also means that SMEs often underestimate risks, fail to monitor their networks effectively, or misinterpret regulatory requirements (Uchendu et al., 2021). This knowledge gap significantly undermines the effectiveness of any technical measures they may attempt to implement.

In addition to financial and knowledge-related constraints, SMEs encounter technological and infrastructural limitations. Many rely on legacy systems or inexpensive hardware that is incompatible with modern security solutions (Fatoki, 2020). Outdated operating systems and software may no longer receive security patches, leaving businesses exposed to known vulnerabilities (Polkowsi & Dysarz, 2017). Furthermore, SMEs that are transitioning to cloud-based platforms often struggle to configure and secure their environments properly, increasing the risk of misconfigurations that cybercriminals can exploit (Ilca et al., 2023). The lack of redundancy and backup systems also compounds the problem, as a single ransomware attack can lead to data loss and prolonged downtime without any recovery plan in place (Podrecca et al., 2022). Thus, the technological foundation of many SMEs is inherently fragile, making it difficult to sustain effective security practices.

Compliance with cybersecurity regulations and standards represents another formidable challenge. Many jurisdictions now require businesses of all sizes to comply with data protection laws, such as ensuring proper storage and handling of customer information (International Organization for Standardization, 2022). For SMEs, navigating these regulatory frameworks can be complex and overwhelming (Bokhari, 2023). They often lack the legal or compliance teams needed to interpret evolving rules, leading to unintentional non-compliance (Murphy et al., 2022). The penalties for failing to comply with cybersecurity regulations can be severe, ranging from fines to reputational damage, yet many SMEs continue to struggle with understanding what is required of them (Chikwendu & Oli, 2024). The regulatory burden, therefore, creates additional pressure on small businesses that are already stretched thin in terms of resources and capabilities.

Finally, SMEs face the challenge of balancing operational efficiency with security. In their drive to remain competitive and agile, many small businesses adopt new digital tools, mobile applications, and online platforms without fully assessing the security implications (Ali & Agyapong, 2021). While such innovations improve efficiency and customer engagement, they also expand the attack surface for cybercriminals (Kariuki et al., 2023). Implementing strict cybersecurity protocols may sometimes slow down operations or inconvenience customers, leading SMEs to compromise on certain measures for the sake of speed and accessibility (Curtin et al., 2024). This trade-off creates a persistent vulnerability, as convenience often comes at the cost of security resilience. The tension between business growth and security discipline remains one of the most difficult challenges for SMEs to resolve (Hasani et al., 2023).

Neyole et al. (2024) examined the impact of cybersecurity threats on SME performance in Kajiado County, Kenya, adopting a mixed-methods case study to capture both organizational practices and contextual challenges. The study employed a structured questionnaire administered to SMEs alongside semi-structured interviews with key informants, including ICT officers and county business representatives. Sampling combined purposive selection of sectors heavily dependent on digital platforms with convenience sampling for SME participants. Quantitative data were analyzed using descriptive statistics and basic inferential tests, while interview transcripts underwent thematic coding. Findings revealed several critical vulnerabilities: poor patch management practices, absence of formal security budgets, minimal use of data backups, and substantial business disruptions linked to phishing and scam incidents. These results highlight how resource constraints, weak institutional planning, and inadequate technical safeguards combine to expose SMEs in Kenya to heightened risks, ultimately undermining their operational resilience and overall performance.

Mugwagwa et al. (2024) addressed the development of future-proof cybersecurity strategies for SMEs in South Africa, integrating both empirical evidence and strategic recommendations. While primarily framed as a strategy paper, the study incorporated empirical components by surveying SME managers across several provinces and conducting practitioner interviews. Quota sampling was employed to ensure representation of micro, small, and medium firms, and the data were analyzed descriptively to identify recurring gaps. The findings pointed to widespread deficiencies, including the absence of formal cybersecurity policies, irregular patching practices, inadequate staff training, and restricted access to affordable managed security services. By combining insights from SME managers with practitioner perspectives, the study underscored the urgent need for scalable, cost-

effective cybersecurity interventions tailored to the resource constraints of South African SMEs, while also emphasizing the role of strategic alignment between business priorities and cybersecurity practices.

2.1.6 Strategies to Improve Cybersecurity Awareness and Compliance among Small and Medium-sized Enterprises (SMEs)

Small and medium-sized enterprises (SMEs) are increasingly dependent on digital platforms for daily operations, customer engagement, and financial transactions. While this dependence enhances efficiency and market competitiveness, it also exposes them to heightened cybersecurity threats (Amrin, 2019). Unfortunately, many SMEs lack the resources, knowledge, or structures to implement robust cybersecurity measures, making awareness and compliance a persistent challenge (Lejaka, 2021). Strengthening these areas is essential, not only for business continuity but also for safeguarding customer trust and meeting regulatory requirements (European Commission, 2020). Several strategies can help SMEs improve cybersecurity awareness and compliance despite their unique limitations.

One effective strategy is the introduction of affordable and scalable training programs tailored to SMEs. Cybersecurity awareness is often hindered by employees' lack of knowledge, which makes them vulnerable to phishing, social engineering, and poor data handling practices (Bada et al., 2019). SMEs can counter this by implementing regular, simplified training sessions that emphasize practical steps such as identifying suspicious emails, creating strong passwords, and safely handling sensitive information (Hijji & Alam, 2022). Online courses, webinars, and interactive simulations can be used to deliver training cost-effectively (Chaudhary et al., 2022). The key is to make cybersecurity a shared responsibility, ensuring that every staff member, regardless of role, understands their part in protecting the organization's digital infrastructure (Stoyanova, 2023).

Another critical strategy involves leveraging partnerships and external support. SMEs often lack the resources to build in-house cybersecurity departments, but they can partner with managed security service providers (MSSPs), government agencies, or industry associations that offer specialized support (Mishra et al., 2022). Such collaborations can provide SMEs with access to threat intelligence, compliance toolkits, and technical expertise at a fraction of the cost of hiring full-time specialists (Chiekezie & Ikwuka, 2025). Public-private partnerships can also play a significant role, with governments offering subsidies, grants, or free advisory services to help SMEs comply with cybersecurity regulations (Herrington & Kew, 2020). By pooling resources and expertise, SMEs can bridge the gap between their needs and their capabilities (Ngek, 2020).

Bada and Nurse (2019) examined the effectiveness of cybersecurity education and awareness programmes for SMEs, combining literature synthesis with empirical evaluation of a city-level initiative in the UK. Using an action research and programme evaluation approach, the study recruited SME staff and managers through programme participation (convenience sampling) and gathered data via pre- and post-training questionnaires, direct observation, and practitioner logs. Analysis involved descriptive statistics and paired comparisons to measure knowledge gains, complemented by qualitative reflections used to refine programme components. The findings demonstrated that targeted, contextually relevant education significantly improved SME staff's cybersecurity knowledge and behavioral intentions. However, the study emphasized that sustainable change requires continued follow-up support and integration of awareness initiatives with simple, practical technical controls. This highlights the importance of coupling training with ongoing reinforcement and infrastructural measures to strengthen SME cybersecurity resilience.

Lejaka (2021) developed and empirically tested a cybersecurity awareness framework tailored for South African small, medium, and micro enterprises (SMMEs) through an exploratory sequential mixed-methods design. The study began with a qualitative phase involving focus groups and expert interviews, which were recorded and thematically coded to generate the initial framework components. This was followed by a quantitative validation stage, using purposive and snowball sampling to survey SMMEs through online and paper-based questionnaires. Descriptive statistics and factor analysis were applied to assess construct coherence and strengthen the framework's validity. The findings culminated in the proposal of a context-sensitive, low-cost awareness model, with training, clear role definition, and localized messaging identified as essential elements for effective uptake. This research emphasized the importance of designing cybersecurity interventions that align with the unique resource constraints and cultural contexts of SMEs in South Africa.

Theoretical Framework

The research adopted the Resource-Based Theory as its framework. The Resource-Based Theory (RBT), also known as the Resource-Based View (RBV), was introduced by Wernerfelt in 1984 and further advanced by Barney in 1991. The theory posits that an organization's competitive advantage and long-term performance are determined by its possession and effective utilization of valuable, rare, inimitable, and non-substitutable resources.

These resources can be tangible, such as financial and physical assets, or intangible, such as knowledge, skills, organizational culture, and technological capabilities. The theory emphasizes that firms that strategically deploy their unique resources are better positioned to achieve sustainable success than those that rely solely on external market conditions.

Applying RBT to the evaluation of cybersecurity awareness and compliance among SMEs in Anambra State, the theory suggests that cybersecurity capabilities themselves can be treated as strategic resources. For instance, SMEs that invest in cybersecurity training, awareness programmes, and security infrastructure build intangible assets in the form of knowledge, technical skills, and organizational routines that enhance resilience against cyber threats. These capabilities, once developed, can provide a sustained advantage, as they are difficult for competitors to replicate. Additionally, compliance with cybersecurity standards may not only reduce exposure to risks but also enhance business credibility, customer trust, and market competitiveness, turning compliance into a resource that contributes to growth.

However, the theory also highlights disparities in resource availability among SMEs. In Anambra State, many SMEs operate with limited financial capital and inadequate technical expertise, making it difficult for them to acquire and maintain sophisticated cybersecurity tools. From an RBT perspective, such firms are disadvantaged because they lack access to the critical resources needed to develop strong cybersecurity awareness and compliance mechanisms. This limitation suggests that without external support, such as government subsidies, public-private partnerships, or collective industry initiatives, many SMEs may remain vulnerable to cyber risks despite the theoretical potential of cybersecurity as a resource-based advantage.

Critically, while RBT provides valuable insights into how internal resources shape cybersecurity outcomes, it has limitations in this context. The theory largely assumes that firms operate in relatively stable environments where internal resources are the main determinants of success. In cybersecurity, however, external threats evolve rapidly, and compliance is often driven by external regulations and industry standards rather than solely by internal resource optimization. Moreover, the theory does not adequately account for institutional weaknesses, regulatory enforcement gaps, or the collaborative nature of cybersecurity, where networks of firms may need to share knowledge and resources.

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.

Findings 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

Objective 1: What are the consequences of poor cybersecurity practices among SMEs? Findings are presented in Tables 2 and 3.

Table 2: Reported consequences of cybersecurity breaches among SMESs in Awka South LGA

Responses	Frequency	Percentage
Financial loss	44	25.0
Data theft	36	20.5
Business disruption	48	27.3
All of the above	48	27.3
Total	176	100.0

Field Survey, 2026

Table 2 shows that a large proportion of respondents (27.3%) reported business disruption as the consequence of cyber security breaches they experience. This shows that breaches carry significant consequences that disrupt businesses while affecting finances. Data from the interviews supports this finding. Data from the interviews supports this finding

An interviewee stated:

When our system was hacked, we could not process customer orders for three days. We lost money and customers went to our competitors. It was a disaster for our small business. The disruption almost put us out of operation completely" (Male, 42, Business Owner).

Another respondent added:

We lost all our customer records and payment details. Some customers started receiving fraudulent messages from people pretending to be us. The data theft damaged our reputation badly. Even after we resolved the issue, some customers never came back because they lost trust in us (Female, 38, SME Manager).

A third interviewee stated:

The financial loss was huge. We had to pay professionals to clean our systems and restore our data. On top of that, we lost sales during the downtime. For a small business like ours, that kind of loss is very difficult to recover from (Male, 45, Retail

Table 3: Experience of previous cyber attack

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

Field Survey, 2026

Table 3 shows that majority of the respondents (67.0%) have experienced a cyberattack. This indicates that SMEs are predisposed to cyber attacks.

Objective 2: What measures can improve cybersecurity compliance among SMEs? Findings are presented in Tables 4 and 5.

Table 4: measures to improve compliance to cyber security protocols by SMEs in Awka South LGA

Responses	Frequency	Percentage
Training and education	62	35.2
Government support	54	30.7
Subsidized cybersecurity tools	38	21.6
Stronger regulation	22	12.5
Total	176	100.0

Field Survey, 2026

Table 4 shows that majority of the respondents (35.2%) identified training and education as the most important way to improve compliance to cyber security protocols by SMEs in Awka South LGA. Other measures includes government support (30.7%), subsidized cyber security tools (21.6%) and stronger regulation (12.5%). This aligns with data from the IDI.

One interviewee explained:

We need someone to teach us simple things like how to create strong passwords, how to spot fake emails, and how to backup our data. Most of us do not know these basic things. If we receive proper training, many of these attacks can be avoided" (Male, 40, Shop Owner).

Another interviewee added:

Government should subsidize antivirus software for small businesses. The good ones are too expensive for us. If they can make it affordable, many of us will buy and use them. Even a fifty percent subsidy would help a lot" (Female, 45, Trader).

Table 5: Support for public-private partnership to improve compliance to cyber security protocols by SMEs in Awka South LGA

Responses	Frequency	Percentage
Yes	150	85.2
No	26	14.8
Total	176	100.0

Field Survey, 2026

Discussions

The study also explored the consequences of poor cybersecurity practices. A significant number of respondents reported experiencing cyber attacks, and many identified financial loss, business disruption, and data theft as major consequences. The fact that a majority had direct experience with cyber incidents demonstrates that cybersecurity threats are not hypothetical. They are already affecting SMEs in tangible ways. This widespread exposure to cyber risk suggests that SMEs operate in a highly vulnerable digital environment. Yet, despite this exposure, preventive structures remain weak. This contradiction underscores a critical vulnerability: businesses are aware of threats and have experienced their impact, but systemic responses remain insufficient. In terms of improvement measures, respondents strongly supported education, government intervention, and collaborative efforts. Training and awareness programs were identified as the most important solution, followed closely by government support and subsidized cybersecurity tools. There was also overwhelming support for partnerships between public institutions and private organizations, as well as the involvement of professional cybersecurity agencies. These findings suggest that SMEs do not view cybersecurity as an individual responsibility alone but as a shared societal and institutional obligation. The respondents' emphasis on collaboration reflects a recognition that small businesses cannot independently shoulder the technical and financial burden of cybersecurity.

Conclusion

The study concludes that the cybersecurity challenge facing SMEs in Awka South LGA is not primarily due to lack of awareness, but rather 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 driven more by structural and economic limitations than by ignorance. Even where awareness exists, many businesses lack the institutional support required for proactive action. Consequently, the problem is systemic: SMEs operate in a digital environment that requires 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

Abdulmajeed, A. & Bob, A. (2020). Cybersecurity challenges and compliance among small and medium enterprises in Nigeria. *Journal of Business and Information Security, 12*(3), 45-58.

Adeniran, T. O. (2019). Cybersecurity threats and vulnerabilities among SMEs in developing economies. *African Journal of Information Systems, 11*(2), 88-102.

Akter, S., Hossain, M. A., & Sultana, S. (2022). Digital transformation and cybersecurity risks in small businesses. *International Journal of Business and Management, 17*(4), 112-128.

Alhuwail, D., Alazmi, A., & Al-Sharhan, S. (2021). Human factors in cybersecurity: Awareness and training needs for SMEs. *Journal of Cybersecurity Research, 8*(1), 33-47.

Ali, A., & Agyapong, D. (2021). Innovation and digital adoption among SMEs in Africa: Opportunities and challenges. *African Journal of Business and Economic Research, 16*(3), 201-220.

Amirin, S. (2019). Regulatory compliance and cybersecurity governance in Nigerian SMEs. *Nigerian Journal of Business Administration, 14*(2), 67-82.

Bada, M., & Nurse, J. R. C. (2019). The effectiveness of cybersecurity education and awareness programmes for SMEs. *Journal of Cybersecurity, 5*(1), 1-15.

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *International Conference on Cyber Security for Sustainable Society*, 118-132.

Baporikar, N. (2020). SMEs and cybersecurity: Strategies for resource-constrained enterprises. *International Journal of Innovation and Economic Development, 6*(2), 23-36.

Barney, J. (1991). Firm resources and sustained competitive advantage. *Journal of Management, 17*(1), 99-120.

Beck, T., & Cull, R. (2021). Financing constraints and SME growth in emerging economies. *World Bank Economic Review, 35*(2), 321-345.

Bokhari, S. M. (2023). Determinants of cybersecurity law implementation in developing countries. *Journal of Cyber Policy and Governance, 7*(1), 44-62.

Chaudhary, S., Gaur, S., & Sharma, R. (2022). Measuring the impact of cybersecurity awareness programs in SMEs. *International Journal of Information Security, 21*(4), 567-582.

Chiekezie, O. M., & Ikwuka, C. P. (2025). Registered small and medium enterprises in Awka South LGA: A directory. *Anambra Business Research Journal, 9*(1), 45-58.

Chikwendu, S. C., & Oli, N. P. (2024). Regulatory compliance and cybersecurity practices in Nigerian public universities. *International Journal of Cybersecurity and Digital Forensics, 8*(2), 112-128.

Curtin, M., O'Donovan, D., & Golden, W. (2024). Bridging the cybersecurity gap for SMEs: A framework for action. *Journal of Small Business Management, 62*(1), 88-106.

European Commission. (2020). *User guide to the SME definition*. Publications Office of the European Union.

Fatoki, O. (2020). Managerial challenges and technology adoption in South African SMEs. *Journal of Entrepreneurship and Business Innovation, 7*(1), 33-48.

Haney, J. M., & Lutters, W. G. (2020). Cybersecurity awareness and compliance in small organizations. *Journal of Cybersecurity Research, 15*(3), 201-218.

Hasani, T., Kotowicz, J., & Lee, S. (2023). Perceived cybersecurity risks and investment decisions in SMEs. *Computers and Security, 124*, 102-118.

Herrington, M., & Kew, P. (2020). *Global entrepreneurship monitor: South African report*. University of Cape Town.

Hijji, M., & Alam, G. (2022). A practical cybersecurity training framework for SMEs. *IEEE Access, 10*, 45678-45692.

Ilca, V., Popa, I., & Dobrin, C. (2023). Digital transformation and cybersecurity readiness in European SMEs. *Journal of Business Research, 156*, 113-128.

International Labour Organization. (2021). *Small matters: Global evidence on the contribution of SMEs to employment and productivity*. ILO Publications.

International Organization for Standardization. (2022). *ISO/IEC 27001: Information security management systems - Requirements*. ISO.

International Trade Centre. (2020). *SME competitiveness outlook 2020: The SME journey*. ITC Publications.

Kariuki, P., Mbuvi, J., & Ndungu, S. (2023). Technical expertise and cybersecurity preparedness among SMEs in East Africa. *East African Journal of Information Technology, 6*(2), 77-92.

Lejaka, M. (2021). *A cybersecurity awareness framework for South African small, medium and micro enterprises (SMMEs)*. Doctoral dissertation, University of South Africa.

Mishra, A., Alzoubi, Y. I., & Anjum, M. (2022). Resource constraints and cybersecurity challenges in SMEs: A systematic review. *Journal of Cyber Security Technology, 6*(3), 145-168.

Mugwagwa, I., van Niekerk, J., & Thomson, K. L. (2024). Developing future-proof cybersecurity strategies for SMEs in South Africa. *South African Journal of Information Management, 26*(1), a1456.

Murphy, T., Katurura, M., & Twum-Darko, M. (2022). Barriers to cybersecurity policy compliance among SMMEs in South Africa. *African Journal of Business Ethics, 16*(1), 55-72.

Neyole, M., Okello, G., & Wanyama, S. (2024). Impact of cybersecurity threats on SME performance in Kajiado County, Kenya. *Journal of Business and Technology, 11*(2), 88-104.

Ngek, N. B. (2020). Policy support and SME resilience in developing economies. *Journal of Entrepreneurship and Public Policy, 9*(4), 445-462.

Olanrewaju, A. S., & George, O. J. (2021). SMEs and employment generation in African economies. *African Economic Review, 13*(2), 112-128.

Podrecca, M., Sartor, M., & Orzes, G. (2022). ISO 27001 certification and operational benefits: Evidence from European SMEs. *International Journal of Production Research, 60*(15), 4689-4706.

Polkowski, Z., & Dysarz, T. (2017). Cybersecurity threats and vulnerabilities in small and medium enterprises. *Scientific Journal of the Polish Economic Society, 5*(2), 45-58.

Shojaifar, A., & Järvinen, J. (2021). Cybersecurity awareness spectrum in SMEs: From neglect to integration. *Journal of Information Systems Security, 17*(3), 89-106.

Stoyanova, T. (2023). Collective initiatives and shared learning for SME cybersecurity. *European Journal of Information Systems, 32*(4), 567-582.

Uchendu, B., Nurse, J. R. C., & Bada, M. (2021). Leadership and security culture in small and medium enterprises. *Computers and Security, 108*, 102-118.

Wernerfelt, B. (1984). A resource-based view of the firm. *Strategic Management Journal, 5*(2), 171-180.

Yamane, T. (1967). *Elementary sampling theory*. Prentice-Hall.

Yeboah-Boateng, E. O. (2023). Regulatory non-compliance and reputational risks among SMEs in developing countries. *Journal of Cybersecurity Law and Policy, 8*(1), 33-48.

Zwilling, M., Klien, G., & Lesjak, D. (2022). Cybersecurity awareness and practices among SMEs in Malaysia. *Journal of Small Business and Enterprise Development, 29*(3), 456-472.