

Cybersecurity awareness and business sustainability among small and medium enterprises in Lagos State, Nigeria

Hajarah Aramide Abdulrauf ^{1,*}, Ubadinachi Obum Christopher ², Daniel David Bolorunduro ³, Nguhemem Esther Ugba ⁴, Abdul-Azeez Opeyemi Adeyanju ⁵ and Simon Ugochukwu Awaogu ⁶

¹ The Department of Computer Science, Al-Hikmah University Ilorin, Nigeria.

² The Department of Computing, University of Greater Manchester, United Kingdom.

³ The Department of Agricultural and Resource Economics, Federal University of Technology Akure, Nigeria.

⁴ The Department of Business Management, Benue State University, Nigeria.

⁵ The Department of Accounting, National Open University of Nigeria.

⁶ The School of Computer Science, University of Sunderland, United Kingdom.

World Journal of Advanced Research and Reviews, 2026, 31(01), 422–427

Publication history: Received on 30 May 2026; revised on 06 July 2026; accepted on 08 July 2026

Article DOI: <https://doi.org/10.30574/wjarr.2026.31.1.1860>

Abstract

The current research sought to assess the relationship between cyber security awareness and business sustainability within small and medium-sized enterprises in Lagos State, Nigeria. With the growing use of technology by SMEs, including online banking, mobile payment services, electronic commerce websites, and cloud computing applications, businesses have been faced with numerous cyber security threats including hacking, phishing, malware infections, ransom ware, and identity theft. Although SMEs are essential for job creation, alleviating poverty, and economic growth in Nigeria, there have been numerous cyber security issues facing many firms due to lack of cyber security awareness, poor training of employees, and inadequate digital security measures. The research used the secondary method of data collection whereby data was collected through information sources such as journals, cyber security reports, government publications, online databases, and other relevant publications. The theoretical foundation of the research was based on the Protection Motivation Theory, which outlines the mechanisms through which organizations take protective measures as a means of minimizing risks. According to the results of the research, cyber security awareness plays a vital role in ensuring business sustainability by helping in achieving continuity, protecting organizational data, increasing customer confidence, minimizing financial losses, and boosting organizational resilience to cyber risks. Also, SMEs that conduct cyber security awareness programs always face little cyber risks and have better performance. The study discovered that cyber security awareness contributes to the long-term sustainability of SMEs in Lagos State. It therefore recommends that SME owners should participate in cyber security awareness programs to reduce their exposure to cyber threats.

Keywords: Cyber Security; Business Sustainability; Small and Medium Enterprises; Lagos State

1. Introduction

Adoption of cyber security Awareness can be considered among the strategies to ensure the sustainability of companies, particularly those operating in the developing countries like Nigeria, where an increasing number of small and medium enterprises (SMEs) rely on technological advancements in order to perform their daily business transactions. In Nigeria, SMEs play an important role in the creation of jobs, earning revenues, lowering poverty levels, and ensuring economic growth (Nairametrics, 2026). These companies play a significant role in economic development by creating business opportunities and innovations. Although the SMEs were involved in the entire process, there are still problems for

* Corresponding author: Hajarah Aramide Abdulrauf

digital security risks, cybercrimes, and lack of proper cyber security measures. If any organization uses digital technology in its activities, then the organization becomes vulnerable to cyber-crimes such as hacking, phishing, ransom ware, malware attack, identity theft, and data breach. Hence, it becomes extremely important that the organizations adopt cyber security awareness to avoid any loss.

Cyber security awareness entails protecting computer systems and data from cyber criminals by people and businesses. This includes educating business owners and their employees on cybercrimes and the ways to avoid them through passwords, phishing protection, updating software, encryption, and internet use. As per the latest report, the financial losses from cybercrimes in Nigeria will increase every year due to the growing number of transactions and firms operating online (Nairametrics, 2026). Cyber criminals target small and medium enterprises more because they lack adequate resources and knowledge to counter cybercrimes.

SMEs that are engaged in different sectors such as retail, tourism, manufacturing, transport, education, finance, and information technology are found in Lagos State, known as the economic capital of Nigeria. In Lagos State, there are many small enterprises that depend largely on technologies and Internet-related activities for their survival in the existing competitive environment. Although there is a notable uptake of digital transformation by many firms in Lagos State, it should be mentioned that most SMEs have insufficient awareness regarding cybersecurity and weak digital security measures. As reported by BusinessDay (2025), in 2025 there were thousands of cyberattacks per week experienced by Nigerian businesses.

Furthermore, the increasing use of digital payment methods among small and medium-sized enterprises (SMEs) is posing a serious threat to cyber security, which is essential in ensuring the survival of the business. As stated in a recent report by Mastercard (2025), most SMEs in Nigeria have been adopting digital payment methods and engaging in online business operations in order to improve efficiency and satisfy their customers. However, many business owners and workers do not realize the dangers associated with cyber security threats and the steps needed to protect their business from such threats.

However, despite the involvement of the SMEs throughout the process, there are still some problems associated with the digital security threats, cybercrimes, and lack of cyber security practices. The use of digital technology in the processes of organizations exposes them to cybercrimes like hacking, phishing, ransom ware attack, malware attack, identity theft, and data breach. It is essential for the organization to have cyber security awareness to avoid any losses.

Sustainability within the business environment refers to the ability of the business firm to be able to sustain itself in terms of viability, profitability, competition, and survival in relation to threats such as environmental, technological, and economic challenges. For small and medium-sized firms, the issue of sustainability is greatly influenced by their ability to cope with risks, which include cyber security. Business organizations that are consistently attacked by cyber criminals will end up being unsustainable due to issues such as financial difficulties and low productivity.

Although cyber-attacks have become increasingly important in Nigeria, there is a lack of research done on the correlation between cyber security awareness and business sustainability in small and medium-sized firms operating in Lagos State. Small and medium-sized businesses emphasize earning money more than cyber security awareness when doing business. Therefore, some firms can easily be attacked by cyber attackers, which may impact their sustainability and even survival. The purpose of this paper is to explore the relationship between cybersecurity awareness and business sustainability among small and medium-sized enterprises in Lagos State, Nigeria.

1.1. Statement Of the Problem

The Small and Medium Enterprises (SMEs) are significant players in the Nigerian economy because of their contribution towards job creation, innovations, poverty reduction, and economic development. In Lagos State, the SMEs have contributed immensely to the promotion of business activities in the region due to the high presence of many companies. Various technological advancements such as online banking, mobile money transfer, cloud computing, e-commerce, and social media marketing have helped the SMEs become more competitive in their operations. Nevertheless, the use of these technologies has left the SMEs vulnerable to various cyber security risks.

A number of small and medium-sized businesses in Lagos State have been victims of several cyberattacks like phishing hacking malware attacks ransom ware identity theft, and other types of cyber fraud mainly due to the poor cyber security awareness among the organizations. BusinessDay (2025) reported that there were over 4,000 cyberattacks weekly against Nigerian businesses in the first quarter of 2025 alone...

Although there is a rise in cases of cybercrimes, there is low awareness among the SME owners and employees about cyber security practices such as password security, phishing, data security, software updating, and internet security. Some SMEs have never organized any cyber security training sessions for their employees while others consider it to be expensive.

In addition, the sustainability of several SMEs is threatened due to their inability to cope with cyber-attacks. The effects of such attacks may hinder the activities of the business entity, reduce customer trust, and affect its profitability. In spite of several cyber awareness campaigns and security initiatives having been proposed by government bodies and institutions, the importance of cyber awareness with regard to business sustainability among Small and Medium Scale Enterprises (SMEs) in Lagos State has yet to be realized. Further research is needed on this matter, hence the study.

Objectives Of the Study

This research work aims at investigating cyber security Awareness and Business Sustainability of Small and Medium Enterprises in Lagos State, Nigeria. The specific objectives of this study are:

- Investigating the relationship between cyber security Awareness and Business Sustainability of SMEs in Lagos State.
- Identifying the benefits associated with cyber security Awareness for business sustainability of SMEs in Lagos State, Nigeria.

1.2. Significance Of the Study

This study will be helpful for the business operators of SMEs in Lagos State as it will give them information on how cybersecurity awareness affects the sustainability, efficiency, and security of businesses from cyberattacks. The study will help business operators learn about the importance of cybersecurity awareness and how it helps to sustain their businesses in the future. The study, will also be useful for cybersecurity experts and IT professionals as it will help them learn about the cyber threats faced by SMEs.

Findings from this study will be valuable for government institutions and policymakers as they will help in providing information concerning the role of cybersecurity awareness in fostering business sustainability and cyber security among SMEs in Nigeria. The results from this study will also be useful in formulating policies to enhance cybersecurity awareness campaigns and support SMEs.

The financial institutions, fintech firms, and digital payment providers will find the research valuable because it will bring to their attention the need for cybersecurity awareness to ensure that their digital transactions are secure from cybercrimes.

The study will contribute to the body of knowledge and be used as reference material by future researchers who may want to conduct further research on cybersecurity awareness in Nigeria.

2. Literature review

2.1. Theoretical framework

2.1.1. Protection motivation theory

The protection motivation theory is adopted as the conceptual framework for this study. The theory was introduced by Rogers in 1975. The protection motivation theory enables one to understand why people and organizations respond to a threat by engaging in behavior aimed at minimizing potential risks associated with the threat. The protection motivation theory posits that an individual will be motivated to protect himself against a specific threat if he views the threat as being serious and controllable.

In relation to cyber security, the theory of protection motivation can assist in analyzing the reasons why businesses choose to adopt cyber security awareness programs and other cyber security techniques to protect their IT infrastructure from any cyber-attacks. The small businesses that understand the severity of cyber-attacks and their consequences will be involved in cyber security awareness training, password protection, and data encryption.

Moreover, according to this theory, it is anticipated that organizations will implement cyber security practices if they feel that these practices will increase their operational continuity, client trust, and organizational sustainability. cyber security awareness affects the behavior of employees and business owners in terms of taking proactive steps towards safeguarding digital information and reducing vulnerability to cyber-attacks. Hence, Protection Motivation Theory offers an appropriate framework for investigating the topic of cyber security awareness and business sustainability of SMEs in Lagos State, Nigeria.

2.2. Empirical review

The research on cybersecurity awareness and organizational performance of Small and Medium Enterprises in Nigeria was conducted by Adewale and Ibrahim (2025). Questionnaires were conducted among the owners and staff of SMEs in Lagos and Abuja. The regression method was used to study the relationship between cybersecurity awareness and firm performance. It was found out that cyber security awareness positively impacts operational effectiveness, customer satisfaction, and resistance to cyberattacks. The authors suggested carrying out cyber security awareness training for SMEs employees on a regular basis.

Okeke & Nnadi (2025) investigated the impact of cyber security awareness on business continuity within small businesses in Lagos State. This research was done using the descriptive survey research design whereby the data were collected from SMEs through the use of structured questionnaires. Data analysis was done using correlation and regression analysis. It was found out that SMEs that had a high degree of cyber security awareness were less likely to face cyberattacks and were more sustainable.

According to the results obtained from the TechEconomy (2025) report, there has been a rise in cyberattacks in Nigeria for the year 2025. These include spyware attacks, password attacks, and malware infections. It should be noted that organizations, particularly small and medium-sized organizations, will still remain vulnerable to such attacks due to lack of cyber security policies in most organizations.

An analysis was carried out by Ogunleye (2026) on the subject of digital security and sustainability of business among SMEs in Lagos State. The research methodology employed in the study consisted of the use of questionnaires and interviews. It was established that digital security is vital for the sustainability of SMEs due to factors such as higher client trust and reduced cyber-attacks.

Cyber Security Awareness Training and Behavior of Employees in Nigerian SMEs was the topic of research carried out by Eze & Chukwu (2025). The findings of the research showed that businesses which conduct regular cyber security awareness training experience fewer cases of phishing attacks, unauthorized access to their system, and data theft.

3. Methodology

For this research, systematic qualitative content analysis was the methodology used. This means that secondary data were obtained from published sources like newspapers, books, peer-reviewed journal articles, and any other documentation related to Cyber Security Awareness and Business Sustainability Among Small and Medium Enterprises in Lagos State, Nigeria.

Relevant literature was identified through a systematic search using keywords such as cybersecurity awareness, business sustainability, SMEs, cyber risk, and Lagos State, Nigeria. Only credible and relevant publications that addressed the study objectives were included, while duplicated and unrelated materials were not included.

In this research, the researcher employed analytical induction analysis of secondary data collected in an attempt to make sense of the data. The process of explaining study phenomenon through causation is termed analytical induction analysis. This process involves searching for similarities that could lead to the identification of common factors.

4. Data presentation and analysis

4.1. What is the Relationship between cyber security awareness and business sustainability among SMEs in Lagos State

Cybersecurity awareness and business sustainability have become issues of major concern to businesses operating within Lagos State due to the high level of technological adoption in the region and the common occurrence of business

transactions that occur through online mediums. Cybersecurity awareness assists business entities to be aware of cyber threats and protect themselves from cyber-attacks.

Many SMEs operating in Lagos State depend on online banking processes, digital payments, social media marketing, and cloud computing. As much as the technologies improve the processes of doing business, they make the companies more vulnerable to cyber threats like hacking, phishing, ransom ware, and data breach. Various research studies have shown that there have been thousands of cyberattacks in Nigeria in the year 2025, resulting in huge losses to businesses (BusinessDay, 2025).

The importance of cyber security awareness plays an important role in business sustainability since companies that are highly knowledgeable in cyber security will be able to detect and counter any cyber threats. Small and medium-sized enterprises that conduct cyber security awareness training for their employees will not only be subjected to less numbers of cyber-attacks but also achieve sustainable business development.

Cyber security awareness allows employees to detect malicious emails, phishing attacks, computer viruses, and fake websites that can jeopardize company operations. In addition, research studies have proven that cyber security awareness will lead to higher customer trust and reputation of the organization. This is because customers will find it more comfortable to deal with businesses that protect their privacy and financial security.

4.2. What are the Benefits associated with cybersecurity awareness on business sustainability among SMEs in Lagos State

There are some benefits that arise from being aware of cyber security that are beneficial to sustaining the operations of SMEs within Lagos State. Some of these benefits include the security of sensitive information. This comprises of customers' information, financial transactions, and any other information of the business. Cyber security awareness ensures that people learn how to protect themselves against any form of cyber-attack.

Continuity of operation is another benefit of cyber security awareness. In most cases, cyber-attacks interrupt the operations of the businesses through damaging the computer systems in use. Firms that have knowledge of cyber security can protect themselves from any kind of attacks. The second point is that cyber security awareness is important since it creates trust between customers and improves reputation. Companies that use cyber security services will attract many clients because customers like to deal with firms that can protect their personal data. Trustworthiness of companies is very important for their existence.

Also, cyber security awareness is essential in lowering financial losses due to cybercrimes. From various studies, it has been estimated that cybercrime leads to huge financial losses annually amounting to millions of naira in Nigeria (Nairametrics, 2026). This will prevent loss of finances from identity frauds, ransomware, and financial frauds.

Fourthly, there must be cyber security awareness to ensure that the data protection acts are followed. This is due to the fact that companies that practice cyber security do not incur any damages and penalties.

5. Discussion of findings

i) The findings from this study indicate that there exists a very strong degree of positive correlation between cybersecurity awareness and business sustainability among SMEs operating in Lagos State. Organizations practicing cybersecurity awareness practices are efficient in operations, less likely to be victims of attacks, increase the level of customer confidence and enjoy business sustainability. This observation is corroborated by the findings from research carried out by Okeke and Nnadi (2025) on the impact of cybersecurity awareness practices on business sustainability among SMEs.

ii) Furthermore, the findings from this study indicate that there exist several benefits to SMEs from cybersecurity awareness practices. These include data security, continuity, financial security, customer confidence, and protection against cyber-attacks. This observation supports the findings from research conducted by Adewale and Ibrahim (2025) indicating that cybersecurity awareness enhances organizational performance and sustainability.

6. Conclusion

Cybersecurity awareness is one of the key determinants of sustainability in business among the Small and Medium-sized Enterprises in Lagos State, Nigeria. With more companies depending on digital technologies and online services

in their operations, there are many challenges posed by cyberattacks that threaten the existence and growth of firms. This is especially so for the SMEs since many companies lack awareness about cybersecurity.

The research finds out that cybersecurity awareness has a positive effect on sustainability in businesses since it ensures reduction in cyber threats, customer confidence, safety of organization's data, and business continuity. SMEs that embrace cybersecurity awareness and adopt digital security measures will be sustainable in the future.

But, even with all the benefits tied to cybersecurity awareness, a lot of SMEs in Lagos State for example are still facing issues like inadequate cybersecurity infrastructure, limited funds, and lack of cybersecurity awareness. Because of this, raising cybersecurity awareness is a big part for improving sustainable business operations and economic development in Nigeria.

Recommendations

- In order for SMEs to protect themselves in the most effective manner, it is of the utmost significance for them to schedule cybersecurity awareness training sessions. Such awareness sessions will equip them with the necessary knowledge to protect themselves from cyber threats.
- Apart from being familiar with the various cyber threats, it is also very important for SMEs to implement countermeasures like antivirus software firewall encryption software and secure payment systems.
- Through government-led awareness programs and the provision of grants and equipment, SMEs can be better guided and resourced in the area of cybersecurity.
- Banks and fintech companies can be key in the fight against cybercrime by partnering with SMEs to provide them with safe digital transaction environments.
- Besides being a very apt aspect of a business, cybersecurity plans and measures become a necessity for SMEs that wish to be capable of defending themselves against cyber threats.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

- [1] Adewale, T., & Ibrahim, S. (2025). Cybersecurity awareness and organizational performance among SMEs in Nigeria. *Journal of Information Security and Digital Management*, 8*(2), 45–59.
- [2] BusinessDay. (2025). *Nigeria records 4,388 weekly cyberattacks on businesses in Q1 2025*. Retrieved from (<https://businessday.ng>)
- [3] Eze, P., & Chukwu, A. (2025). Cybersecurity awareness training and employee behavior among Nigerian SMEs. *African Journal of Cyber Studies*, 6 (1), 22–38.
- [4] Guardian Nigeria. (2025). *LASG promises sustained digital protection at cybersecurity awareness campaign*. Retrieved from (<https://guardian.ng>)
- [5] Kaspersky. (2025). *Kaspersky and SMEDAN support SMEs in Nigeria with cybersecurity knowledge*. Retrieved from (<https://kaspersky.com>)
- [6] Mastercard. (2025). *Nigerian SMEs embrace digital payments and innovation to drive business growth*. Retrieved from (<https://mastercard.com>)
- [7] Nairametrics. (2026). *Lagos unveils cybersecurity guidelines as cybercrime losses hit \$500 million*. Retrieved from (<https://nairametrics.com>)
- [8] Ogunleye, A. (2026). Digital security and business sustainability among SMEs in Lagos State, Nigeria. *International Journal of Entrepreneurship and Digital Innovation*, 7 (1), 80–96.
- [9] Okeke, C., & Nnadi, U. (2025). Cybersecurity awareness and business continuity among SMEs in Lagos State. *Nigerian Journal of Business and Information Technology*, 10 (3), 61–75.
- [10] Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology*, 91(1), 93–114.
- [11] TechEconomy. (2025). *Cyber threats in Nigeria increase significantly in 2025*. Retrieved from (<https://techeconomy.ng>)