International Journal of Science and Research Archive
eISSN: 2582-8185
Cross Ref DOI: 10.30574/ijsra
Journal homepage: https://ijsra.net/

(RESEARCH ARTICLE)

Check for updates

The impact of cybersecurity on SMES in Edo State, Nigeria

Edirin Pereye [1], Dirisu Osagie Aziegbe [2], Muhammed Aminu Ali [3,*] and Engr Clement Agbeboaye [3]

[1] *Global Maritime Academy, Agbowhiame, Delta State.*
[2] *N-power, Olinlin Secondary School, Uzea, Edo State.*
[3] *Department of Electrical/Electronic Engineering Technology, National Institute of Construction Technology and Management, Uromi, Edo State.*

International Journal of Science and Research Archive, 2025, 16(02), 1511-1518

Publication history: Received on 19 July 2025; revised on 25 August 2025; accepted on 29 August 2025

Article DOI: https://doi.org/10.30574/ijsra.2025.16.2.2481

Abstract

In an era of escalating cyber threats, the vulnerability of Small and Medium-sized Enterprises (SMEs) to cybersecurity risks is alarming. This research x-rayed the impact of cybersecurity on SMEs in Edo State, Nigeria. The study unveiled the prevailing state of cybersecurity awareness, practices and incidents among SMEs in Edo State. The study used stratified sampling to select one hundred (100) SMEs in Edo State and structured questionnaire was designed and distributed to them. The focal areas were adoption of cybersecurity technologies, risk assessment practices, vulnerabilities faced by these enterprises, the implications of cybersecurity incidents on financial stability, reputation and business continuity. The findings revealed that over a quarter of the sampled SMEs were victims of cybercrimes. SMEs remain unaware of IT security incidents as victimized SMEs avoid spreading the news to prevent further damage to their reputation. Recommendations were made to strengthen cybersecurity resilience within Edo State SMEs, as well as policy considerations in order to empower enterprises to safeguard their operations against evolving cyber risks.

Keywords: Cybersecurity; SMES; Edo State; Cyber Risks

1. Introduction

According to World Trade Organization, Small and Medium-sized Enterprises (SMEs) are representing not only more than 90% population of business, 60% to 70% of employment but also 55% of the GDP of developed economies [1, 2, 3]. SMEs as vital components of the economic terrain are increasingly reliant on digital infrastructure for their day-to-day operations. Due to the rapid digitization of business operations and the increasing connectivity of global networks, cybersecurity has emerged as a paramount concern for enterprises of all scales. However, this reliance also exposes them to a growing array of cyber threats, ranging from sophisticated malware to targeted phishing attacks. Hence, protecting SMEs from cybercrimes and cyber security treats should be a major concern for SMEs themselves [4, 5].

Cyber-attacks are on the increase because it is cheaper, convenient and less risky than physical attacks. According to Symantec statistics, 14 adults become the victim of a cyber-attack every second, or more than one million attack everyday [6, 7]. A survey conducted on 234 organizations from different countries affirmed that, the organizations have experienced 20 percent more successful cyber-attack in 2013 than the previous year [5, 8]. Without deliberate measures taken to address the issue of cybercrime, particularly among SMEs, there is a significant risk of the economy facing potential collapse.

This research aimed to x-ray the impact of cybersecurity on SMEs within the dynamic business environment of Edo State, Nigeria. As the engine of economic growth and job creation in the region, the resilience of SMEs to cyber risks holds profound implications for the economic stability and prosperity of the local community. The insights garnered

* Corresponding author: Muhammed Aminu Ali

herein were anticipated to serve as a foundation for collaborative efforts between SMEs, government entities, and cybersecurity experts, ultimately fostering a more secure and prosperous economic ecosystem.

2. Materials and methods

2.1. MATERIALS: The study utilized a structured questionnaire to collect data from 100 SMEs in Edo State

2.1.1. Methods

Stratified sampling was employed to ensure a representative selection of Small and Medium-sized Enterprises (SMEs) in Edo State. This technique involves dividing the population into distinct subgroups, or strata, based on specific characteristics relevant to the study. In this case, the strata were determined based on industry sector. The first step was to categorize SMEs in Edo State into industry sectors such as Retail, Manufacturing, Services, etc. This division allowed for a more refined analysis of the impact of cybersecurity within different sectors. After the strata were defined, the next step was to determine the proportion of SMEs to be selected from each sector. This allocation was based on the relative size of each industry sector in Edo State. Within each industry sector, SMEs were randomly selected to participate in the study. This was done to ensure that the sample within each stratum was represented and not biased towards specific businesses. The sample size for each stratum was determined based on factors such as the total number of SMEs in that sector and the desired level of statistical precision. Among the 100 questionnaires distributed to SMEs, 88 SMEs provided responses, resulting in a response rate of 88%. However, 12 SMEs did not participate in the survey. After data collection, the results from each stratum were combined to form a comprehensive dataset representing SMEs across various industry sectors in Edo State.

2.1.2. Questionnaire design

The questionnaire designed for this research study was carefully structured to gather comprehensive and insightful data from Small and Medium-sized Enterprises (SMEs) in Edo State. It comprises several key sections, each strategically crafted to address specific aspects of cybersecurity awareness, practices, and incidents within the SME community. The questionnaire begins with a clear introduction, setting the context and purpose of the study, fostering transparency and participant understanding.

The subsequent sections were thoughtfully organized, commencing with a gathering of general information about the SMEs, such as industry sector, number of employees, and years in operation. The questionnaire then assesses SMEs' awareness of cybersecurity, whether they have received formal training, and whether they have established written policies or guidelines. Additionally, its inquiries about the frequency of cybersecurity training provided to employees. This structured approach allows for a systematic evaluation of the SMEs' knowledge and preparedness in the area of cybersecurity.

Furthermore, the questionnaire addresses the adoption of specific cybersecurity technologies, which includes a checklist of essential tools and systems like antivirus software, firewalls, encryption tools, and others. This section enables a clear understanding of the technological safeguards implemented by SMEs in Edo State. The questionnaire also ventures into risk assessment and vulnerabilities, probing whether SMEs conduct regular assessments and identifying the types of vulnerabilities they consider most critical.

A critical facet of the questionnaire lies in its exploration of actual cybersecurity incidents. It seeks to determine whether SMEs have experienced any incidents. This provides invaluable qualitative insights into the real-world impact of cyber threats on SMEs' operations and stability.

The implications of cybersecurity incidents are not overlooked. The questionnaire employs a 4-point scale to gauge the impact on financial stability, reputation, and business continuity, shedding light on the multifaceted repercussions of such incidents. Additionally, the questionnaire addresses the reporting and communication aspect of cybersecurity incidents, probing SMEs on whether they would report such incidents to external entities and the factors influencing their decision.

The anticipated respondent for the questionnaire was a designated individual within the SMEs responsible for overseeing IT and other core operations, ideally holding a key position such as CEO, CTO, COO, or CFO of the SME.

3. Results

3.1. Sample description

After a period of gathering information from respondents, a total of 88 SMEs filled in the questionnaires while 12 SMEs did not participate in the survey. Table 1 is a representation of the industry sectors of the SMEs while table 2 is a representation of the number of employees by the SMEs. The largest representation comes from the retail sector, comprising nearly 30% of respondents, followed closely by services and manufacturing at around 27% and 24% respectively. This indicates a well-rounded sample, capturing a cross-section of the local economy. In terms of workforce size, the majority of respondents fall within the range of 5 to 9 employees, accounting for about 31% of the sample. This is followed by SMEs with 20 to 49 employees (25%) and those with 2 to 4 employees (21.6%). This diversity in employment size suggests a mix of micro, small, and medium-sized enterprises, reflecting the typical composition of SMEs. Regarding the longevity of these SMEs, the majority have been in operation for a span of 3 to 20 years.

Table 1 Industry Sectors of the SMES

SME Types	Respondent Percentage
Retail	29.55%
Manufacturing	23.86%
Services	27.27%
IT and Software Development	7.95%
Construction and Engineering	11.36%

Table 2 Number of Employees by the SMES

Number of Employees	Number of Respondents	Cumulative Sample
2 to 4	19	19
5 to 9	27	46
10 to 19	15	61
20 to 49	22	83
50 to 249	5	N = 88

3.2. Survey results

3.2.1. Cybersecurity awareness and practices

- **Awareness of Cybersecurity:** SMEs were asked about their awareness of cybersecurity. A substantial majority of respondents (89.8%) demonstrated awareness of the term "cybersecurity," while a smaller proportion (10.2%) indicated a lack of familiarity with the term.
- **Received formal Training:** SMEs were asked if they have received any formal training on cybersecurity. Only a limited percentage (9.1%) of respondents reported receiving formal training on cybersecurity for themselves or their employees, with the majority (90.9%) indicating a lack of such training.
- **Written Cybersecurity Policy:** SMEs were asked if they have any written cybersecurity policy or guidelines in place. A relatively small percentage (7.95%) of SMEs reported having a written cybersecurity policy or guidelines in place, while the majority (92.05%) indicated the absence of such formalized policies.
- **Frequency of Training:** SMEs were asked how often cybersecurity training is provided for their employees. The data reveals that a significant proportion of SMEs indicated that cybersecurity training is provided infrequently or not at all. Specifically, 90.9% reported that they never provide cybersecurity training, while 4.55% and 4.55% mentioned providing it rarely and occasionally, respectively. However, none of the respondents reported providing cybersecurity training frequently for their employees.

Figure 1 is a representation of the cybersecurity awareness and practices by the SMEs.

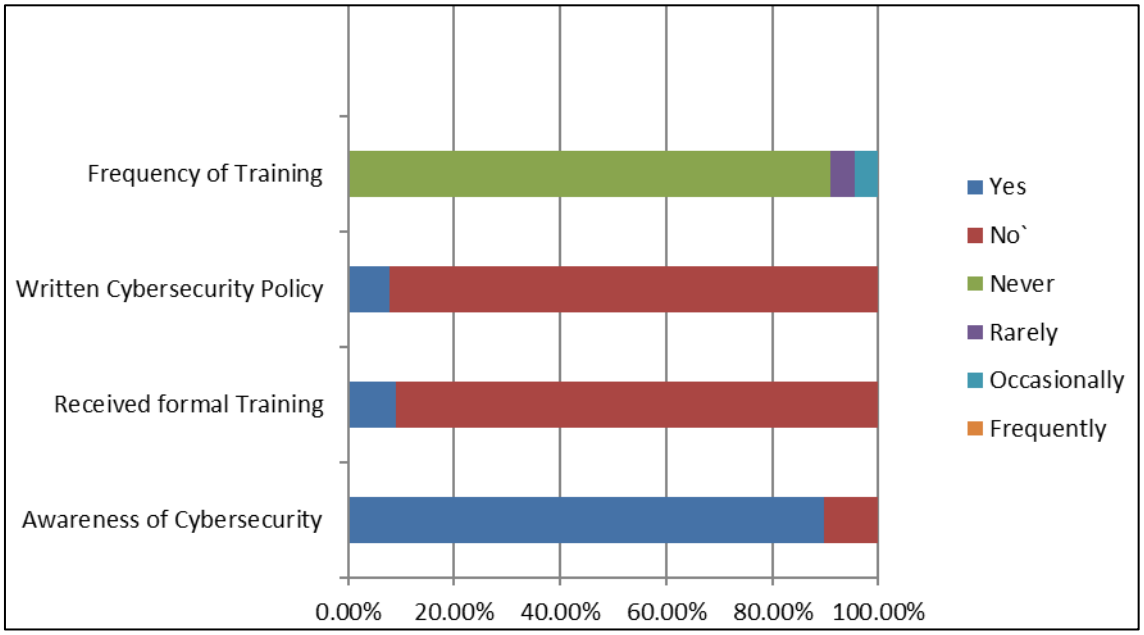

Figure 1 Cybersecurity Awareness and Practices by SMES

3.2.2. Adoption of cybersecurity technologies

SMEs where asked what type of cybersecurity technologies they utilized. 89.8% of respondents reported using antivirus software, 50% of respondents reported using firewalls, 6.8% reported using intrusion detection system (IDS), 11.4% of respondents reported using intrusion prevention system (IPS), 6.8% of respondents reported using virtual private network (VPN), 10.2% of respondents reported using encryption tools, 27.3% respondents reported using multi-factor authentication, and 12.5% respondents reported using other cybersecurity technologies.

Figure 2 is a representation of the adoption of cybersecurity technologies by the SMEs.

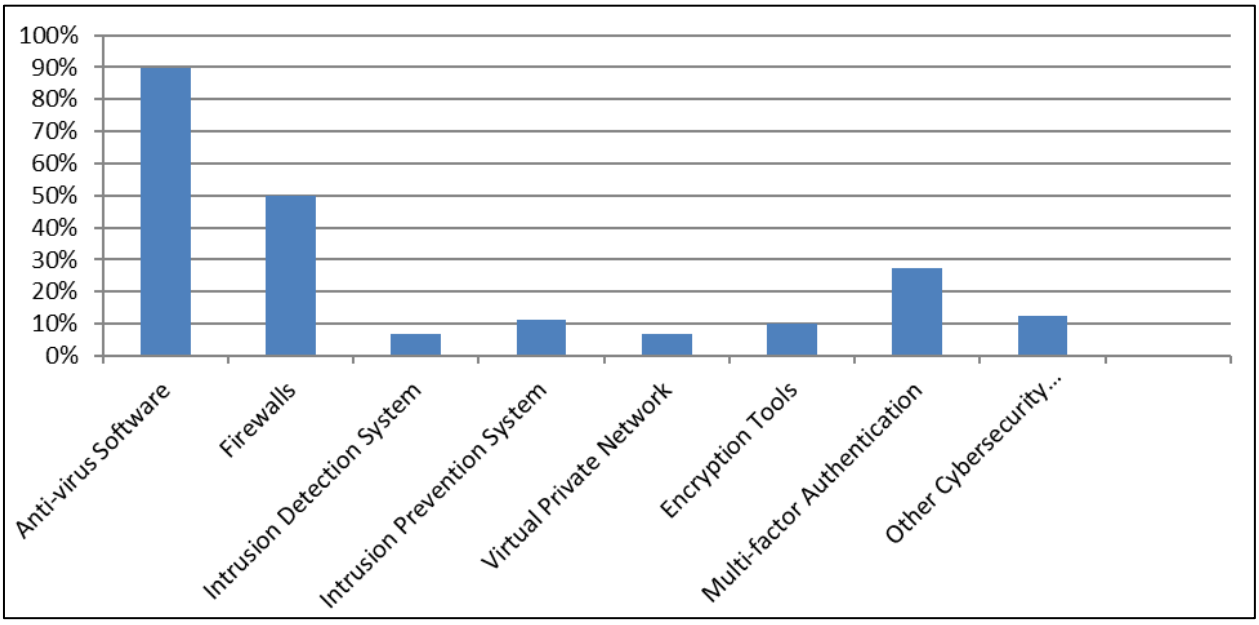

Figure 2 Adoption of Cybersecurity Technologies by the SMES

3.2.3. Risk assessment and vulnerabilities

- **Conduct of Regular Risk Assessment:** SMEs were asked if they conduct regular risk assessments to identify potential cybersecurity vulnerabilities. A significant majority of SMEs (94.32%) reported not conducting regular risk assessments to identify potential cybersecurity vulnerabilities, while a smaller proportion (5.68%) affirm to conducting regular risk assessments to identify potential cybersecurity vulnerabilities.
- **Most Critical Type of Vulnerability:** SMEs were asked the type of vulnerability they consider most critical to their businesses. 89.8% of the respondents considered phishing attacks to be the most critical threat to their business. In contrast, other vulnerabilities were identified at lower percentages. Malware attacks were noted by 4.55% of respondents, followed by insecure passwords at 3.41%, and ransomware at 2.27%. These figures suggest a clear emphasis on the importance of addressing phishing attacks, while also indicating a level of awareness regarding other types of cyber threats.

Figure 3 is a representation of the risk assessment and vulnerabilities by the SMEs.

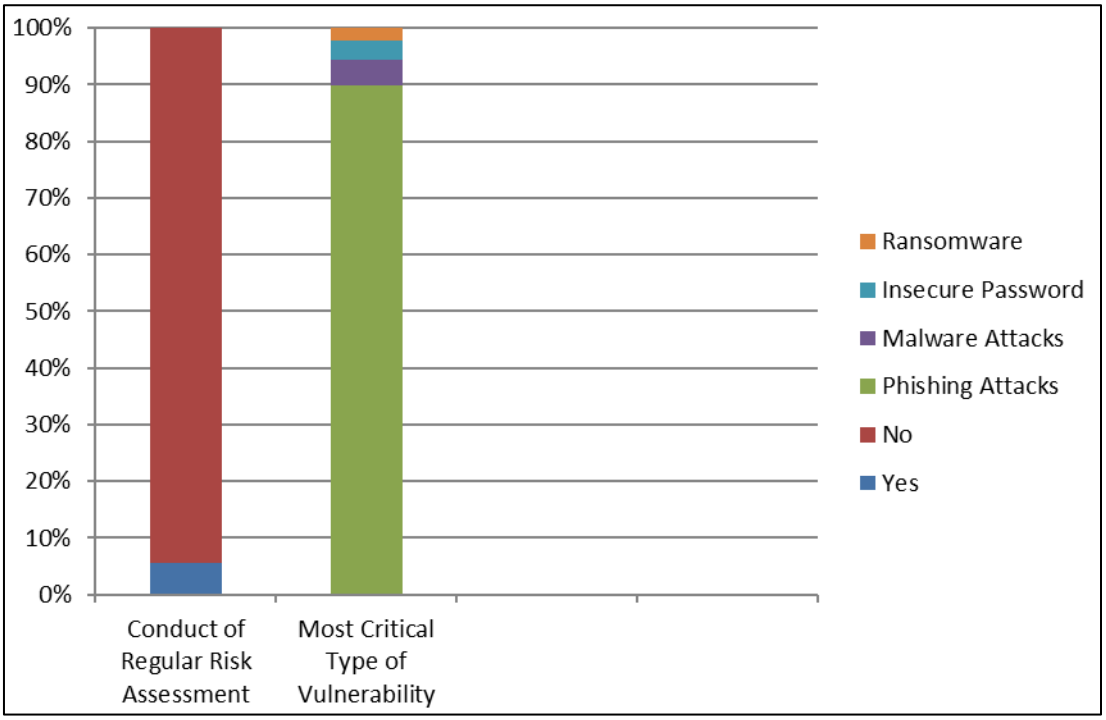

Figure 3 Risk Assessment and Vulnerabilities by the SMES

3.2.4. Cybersecurity incidents

SMEs were asked if they have ever experienced any cybersecurity incident such as phishing attack, malware attack, ransomware attack, etc. The data reveals that a significant portion of SMEs (36.36%) have reported experiencing at least one cybersecurity incident while 63.64% reported they have not experienced any cybersecurity incident. This finding indicates that a substantial number of SMEs in Edo State, Nigeria, have encountered various forms of cyber threats, ranging from phishing attacks and malware infections to potentially more serious incidents like ransomware attacks.

3.2.5. Implications of cybersecurity incidents

SMEs were asked, in case of a cybersecurity incident, how they would rate its impact on the following aspects:

- **Financial Stability:** 50% of respondents believe that cybersecurity incidents would have a very high impact on their SME's financial stability. While 27.27% respondents anticipate a high impact, 15.91% respondents anticipate a low impact and 6.82% anticipate a very low impact on their SMEs financial stability.
- **Reputation:** Nearly half of the respondents (45.45%) expect a very high impact on their SME's reputation in the event of a cybersecurity incident. Additionally, 22.73% respondents anticipate a high impact. While 20.45%

respondents anticipate a low impact, and 11.36% respondents anticipate a very low impact on their SMEs reputation.

- **Business Continuity:** Over half of the respondents (51.14%) believe that a cybersecurity incident would have a very high impact on their SME's business continuity. An additional 26.14% respondent expects a high impact. While 17.05% respondents anticipate low impact and 5.68% respondents anticipate a very low impact on their SMEs business continuity.

Figure 4 is a representation of the implications of cybersecurity incidents by the SMEs.

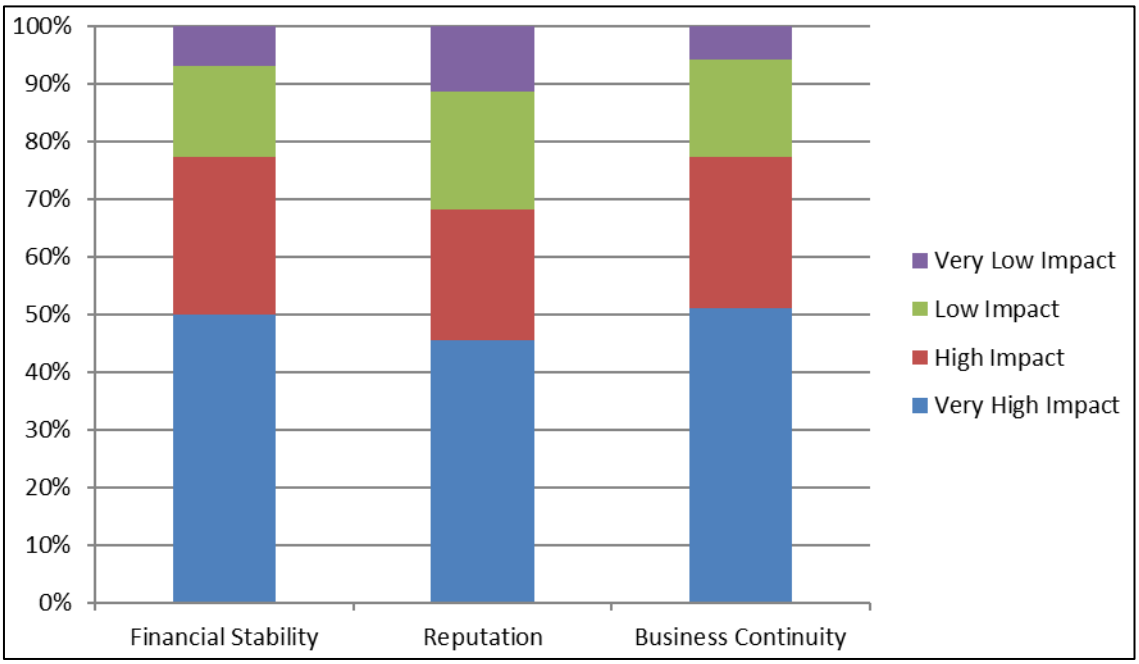

Figure 4 Implications of Cybersecurity Incidents by the SMES

3.2.6. Reporting and communication

SMEs were asked if they experienced a cybersecurity incident, if they would report it to any external entities such as regulatory bodies, law enforcement agencies, etc. The data reveals that just over half of the respondents (54.55%) would report a cybersecurity incident to external entities, while a significant portion (45.45%) would opt not to report such incidents externally.

4. Discussion

The findings from this study provide valuable insights into the state of cybersecurity awareness, practices, and incidents among Small and Medium-sized Enterprises (SMEs) in Edo State, Nigeria. The sample description reflects a well-rounded representation of industry sectors and workforce sizes, indicating a diverse cross-section of the local economy. The prevalence of retail, services and manufacturing sectors underscores the economic diversity of SMEs in the region.

4.1. Cybersecurity Awareness and Practices

The study reveals a critical gap in cybersecurity awareness and training within SMEs. While a majority of respondents demonstrated awareness of the term "cybersecurity," a significantly low percentage reported receiving formal training. This suggests that while SMEs may recognize the importance of cybersecurity, there is a need for more structured education and training programs to equip them with the necessary skills and knowledge to protect their operations.

Additionally, the absence of written cybersecurity policies in the majority of SMEs highlights a potential area for improvement. Formalized policies play a crucial role in establishing clear guidelines for cybersecurity practices, and their limited adoption indicates a need for greater emphasis on policy development within SMEs.

4.2. Adoption of Cybersecurity Technologies

The adoption of cybersecurity technologies reveals a mixed picture. While a high percentage of SMEs reported using antivirus software, the utilization of other essential technologies such as firewalls, intrusion detection systems, and intrusion prevention systems appears to be lower. This suggests a potential vulnerability in the cybersecurity posture of SMEs, as these technologies are fundamental in safeguarding against a range of cyber threats.

4.3. Risk Assessment and Vulnerabilities

One of the most striking findings is the limited conduct of regular risk assessments among SMEs. The overwhelming majority of respondents reported not conducting regular risk assessments to identify potential vulnerabilities. This is a significant concern, as risk assessments are a cornerstone of effective cybersecurity management. The prevalence of phishing attacks as the most critical vulnerability further underscores the importance of proactive risk assessment and mitigation strategies.

4.4. Cybersecurity Incidents and Implications

The data highlights that a substantial number of SMEs in Edo State have experienced cybersecurity incidents This indicates the pervasive nature of cyber threats and the pressing need for SMEs to fortify their defenses. The perceived impact of these incidents on financial stability, reputation, and business continuity is substantial, with a majority of respondents anticipating very high or high impact. This underscores the potentially devastating consequences of cyber incidents and emphasizes the urgency for SMEs to prioritize cybersecurity measures.

4.5. Reporting and Communication

The findings regarding reporting of cybersecurity incidents to external entities indicate a moderate willingness among SMEs to engage in external reporting. However, a significant portion remains hesitant to do so. This suggests a potential gap in understanding the benefits of external reporting and highlights the need for further education and support in this area.

Finally, this research sheds light on the critical need for enhanced cybersecurity measures within SMEs in Edo State, Nigeria. The study underscores the importance of structured education, policy development, technology adoption, risk assessment and incident response planning. Addressing these areas can significantly strengthen the cybersecurity resilience of SMEs and contribute to the overall economic security of the region.

5. Conclusion

This research highlights the imperative for Small and Medium-sized Enterprises (SMEs) in Edo State, Nigeria, to fortify their cybersecurity architecture in the face of escalating cyber threats. The findings reveal a notable gap in cybersecurity preparedness, with limited formal training and policy implementation. SMEs must prioritize structured education programmers and the development of clear, actionable cybersecurity policies. The study serves as a clarion call for SMEs in Edo State to elevate their cybersecurity resilience. By investing in education, policy development, technology adoption, risk assessment, and incident response planning, SMEs can fortify their defenses and contribute to the economic security of the region. The imperative is clear: proactive cybersecurity measures are not just a business necessity but a foundational pillar of sustainable growth and resilience in an increasingly interconnected digital environment.

Recommendations

Based on the findings of this research, the following recommendations are made to enhance the cybersecurity architecture of Small and Medium-sized Enterprises (SMEs) in Edo State, Nigeria:

- **Prioritize Cybersecurity Education and Training:** SMEs should invest in comprehensive cybersecurity training programmers for both management and employees. These programmers should cover essential topics, including threat awareness, secure practices, and incident response protocols.
- **Develop and Implement Formal Cybersecurity Policies:** SMEs should establish written cybersecurity policies and guidelines tailored to their specific operations. These policies should encompass best practices, incident reporting procedures, and compliance with relevant regulations.
- **Strengthen Technological Defenses:** SMEs should consider a holistic approach to cybersecurity technology adoption. This includes the deployment of essential tools such as firewalls, intrusion detection systems, and multi-factor authentication, alongside regular updates and patches.

- **Conduct Regular Risk Assessments:** SMEs should integrate routine risk assessments into their cybersecurity strategy. These assessments should identify vulnerabilities, prioritize risks, and inform the development of targeted mitigation strategies.
- **Implement an Effective Incident Response Plan:** SMEs should establish and regularly test incident response plans to ensure a swift and coordinated reaction in the event of a cybersecurity incident. This plan should encompass reporting procedures, containment measures, and recovery strategies.
- **Promote Information Sharing and Reporting:** Industry associations, government agencies, and cybersecurity organizations should collaborate to facilitate information sharing and reporting mechanisms. This will enable SMEs to benefit from collective intelligence and gain access to resources for threat mitigation.
- **Engage in Continuous Monitoring and Threat Intelligence:** SMEs should invest in cybersecurity monitoring tools and services to proactively detect and respond to emerging threats. Access to threat intelligence sources will provide valuable insights into evolving cyber risks.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Globalnaps (2017). Small and medium-sized enterprises. URL: https://globalnaps.org/issue/small-medium-enterprises-smes/

[2] WTO (2016). World trade report 2016, Levelling the trading field for SMEs. URL: https://www.wto.org/english/res_e/publications_e/wtr16_e.htm

[3] Pawar, S., and Palivela, H. (2022). A framework for least cybersecurity controls to be implemented for small and medium enterprises (SMEs). International Journal of Information Management Data Insights, 2, 100080.

[4] Enisa General Report (2012). Availble:http://www.enisa.europa.eu/publications/programmes-reports/general-report-2012.

[5] Amrin, A. (2015). The Impact of Cybersecurity on SMEs. University of Twente, Faculty of Electrical, Mathematics and Computer Science.

[6] PCMag Staff (2011). Cyber Crime Costs $114B Per Year, Mobile Attacks on the Rise. https://www.pcmag.com/archive/cyber-crime-costs-114b-per-year-mobile-attacks-on-the-rise-287406

[7] Jang-Jaccard, J. and Nepal, S. (2014). A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences, Vol. 80, pp. 973-993.

[8] Global Report (2013). Cost of Cyber Crime Study. Available: http://www.hpenterprisesecurity.com/ponemon-2013-cost-of-cyber-crime-study-reports