AN EMPIRICAL SURVEY TO SUBSTANTIATE THE NEEDFOR A CYBER SECURITY FRAMEWORK FOR SMES IN NIGERIA

[1]Vincent Onuwabhagbe OGBEIDE, [2]Osaremwinda OMOROGIUWA, [3]Emmanuel Eturpa SALAMI

[1]Department of Computer Science and Information Technology, Igbinedion UniversityOkada, Edo State, Nigeria
[2]Department of Computer Science and Information Technology, Igbinedion UniversityOkada, Edo State, Nigeria
[3]Department of Computer Science and Information Technology, Igbinedion UniversityOkada, Edo State, Nigeria

Email address: ogbeide.vincent@iuokada.edu.ng, ask4osas@iuokada.edu.ng,Salami.emmanuel@iuokada.edu.ng

Abstract

SMEs have attracted security risks due to the continued use of technology. Technology has brought significant benefits to SMEs and at the same time expose them to cyber security threats . Many of the SMEs are attracts interest from cyber criminals because of weak security and inadequate protection**.** Cyber attack can be costly for SMEs that are not ready to protect their systems, thus risking significant disruption, loss and even forfeiture of business. Many of the SMEs do not have a strategy to improve their cyber security posture despite the known risk to their business. Cybercrime prevention is often neglected within the SME environment because of inadequate funds which makes it expensive for SMEs to adopt complex or International cyber security frameworks. The existing frameworks are generally expensive, broad, require certifications and expert with vast knowledge which makes it difficult for SMEs to implement. This study seek to investigate the need for a cyber security framework for SMEs in Nigeria. The findings from the survey recognized the high response as 76.9% of SMEs attested to the fact that there is need for a cyber security framework for SMEs in Nigeria. The survey also revealed that SMEs are vulnerable to cyber threats because not all SMEs have considered security implication to their businesses and simply because some of them have very little knowledge of IT to understand the impact of security. An Empirical Survey using quantitative descriptive analysis was used to analyze the data collected and the tool used for data collection was a structured questionnaire and Statistical Package for Social Science (SPSS) to code the data for analysis.

Keyword: Cyber Security, Cyber Attacks, Framework, SMEs

1. Introduction

The impact of technology advancement have forced Small and Medium Scale Enterprises (SMEs) to adopt and equip their business models with ever-evolving technologies (Jafari-Sadeghi et al., 2021). This wave in technology has brought an onslaught of cybercrime, wherein criminals attempt to victimize firms or individuals through theft of personal information (Anandarajan et al., 2013). This has also led to new challenges that altered organizational designs, the ability to manage data, and a new source of risks (Calabrese et al., 2019; Jafari-Sadeghi, 2021; Shah et al., 2019). Undermining the size of business, SMEs are faced with the same levels of cyber security issues as large organisations, however, limited resources and capabilities made them fragile against cyber risks (Baggott & Santos, 2020; Benz & Chatterjee, 2020).

The SME sector is the backbone of major developed economies, as well as important contributors to employment, economic and export growth. In Nigeria, SMEs contribute 48% of national Gross Domestic Product (GDP) in the last five years, account for 96% of businesses and 84% of employment. With a total number of about 17.4 million, they account for about 50% of industrial jobs and nearly 90% of the manufacturing sector, in terms of number of enterprises (Pricewaterhousecoopers SME Survey 2020). The capacity of SME to perform their role, as the engine of growth in the economy, is often hampered by challenges such as lack of access to finance, modern technology, and market with unfair competition to imported goods, among others.

SME have become attractive target for cyber attackers because owners often lack the necessary information technology resources and capabilities needed to implement emerging cyber security recommendations (Harris & Patten, 2014). Specifically, the owners regularly lack the proper processes to control evolving cyber security risks and information systems security threats that characterize the use of these technologies (Njenga & Jordaan, 2016). The loss of customers, income, and in some instances forfeiture of business due to expensive litigation costs are among the potential adverse effects on SME owners (Federal Communications Commission (FCC), 2014; Layton & Watters, 2014). Therefore, cyber risk management and preparation is a crucial competencies for not only survival but also the growth of SMEs (Chatterjee, 2019; Hoppe et al., 2021).

Despite the rise in cybercrime among SMEs, many SMEs remain susceptible to cyber attacks due to lack of resources and surprisingly, a lack of knowledge of the threat. In spite of the increasing threats posed by cyber attacks, an astounding one in four SME owners have little to no understanding of the issue whatsoever. Often SMEs do not even know they have been attacked until it is too late. More than ever, sensitive data, intellectual property and personal information of SMEs are targeted by an ever increasing and sophisticated community of cybercriminals. The attack on SMEs are increasing because they present cybercriminals with an easy way to gain access to customer bank accounts, supplier networks and employee financial and personal data. Budgeting resources for cyber security is required for the protection of their assets and data (Aiken et al., 2016).

SME owners assume the scale of cyber attacks is substantially less for them to be compared to larger businesses (Arora, 2016). However, evidence indicates that small businesses experience more online threats than larger businesses primarily due to the lack

of investment in cyber security protection plans (Aiken et al., 2016). It is therefore required of an organisation to invest in Information Technology strategies for prevention and strategic risk management to combat intrusions and to strengthen their network (Srinidhi et al., 2015). Increased cyber security strategies are necessary to protect an organisation's financial assets, data, and intellectual property (Arora, 2016). This paper is aimed at carrying out an empirical survey to substantiate the need for a cyber security framework with an emphasis on SMEs in Nigeria. The objectives of this work are;

i. To ascertain the state of SMEs present Cyber Security Infrastructure.
ii. To ascertain the state of SMEs Owners mode of Cyber Security Strategies.
iii. To determine assessment of Government Policies that affects Cyber Security.
iv. To determine the need for a Cyber Security Framework for SMEs in Nigeria.

2. Review of Related Literatures

Studies have been conducted on cyber security in small businesses internationally and the results from these studies identified some of the challenges small businesses face and why they find it hard to adopt cyber security measures available to them. This study is to address the current cyber security problems experienced by SMEs in Nigeria. Singh et al. (2022) reported in their study that SMEs are not immune to the threats posed by the use of information and communication technologies, and that studies have noted that SMEs may be more vulnerable to cyber threats when compared to larger firms. According to the research of SMEs in developing nations such as South Africa, challenges to implementing cyber security in SMEs include a lack of management support owing to other company objectives, a low budget, and a lack of resources with technical skills and cyber security tools (Armenia et al., 2021; Kabanda et al., 2018). Benz & Chatterjee (2020) reported in their studies that more than 50% of SMEs are lagging far behind to have the latest cyber-risk strategy and the IT leaders don't know starting point to improve cyber security posture. According to a survey of SMEs in the United Kingdom, roughly 73 percent of businesses had trouble accessing cyber security information to adopt. Cyber-attacks and data loss were not considered a significant risk by one-third of businesses (Rae & Patel, 2019). A study conducted by Symantec Corporation (2016) to determine SMEs susceptibility to cyber attacks. The results indicated SMEs are susceptible to cyber attacks because they lack sophisticated security capabilities and the financial resources to prevent potential attacks. In a study conducted for SMEs in Kenya, businesses face two key hurdles when it comes to implementing cyber security. One was a lack of sufficient funds, and another was a lack of leadership support for cyber security implementation, which could be because they have other business-related issues that are a priority for them (Muhati, 2018). Small Business Administration (2014) reported from a survey that cyber criminals are increasing attacks on SME owners who currently may have limited information on cyber security vulnerabilities and protective strategies. Disterer & Kleiner (2013) in their study Using mobile devices with BYOD, reported that the system which reduce a company's indirect costs, one of the biggest risks involves

employees downloading personally identifying or confidential client information to their smart phones and/or tablet devices. Criminals could obtain critical company data if any of those mobile devices were lost, stolen, or otherwise compromised. The study recommended to mitigate the effects of the attack, SME owners can establish policies for employee use of public Wi-Fi zones, and require employees utilize a virtual private network (VPN) for connectivity when connecting to a corporate network. In a study conducted by Jansen et al. (2016), SME owners implemented protective measures when they (i) believe a measure is effective, (ii) are capable of using Internet technology, (iii) have a positive attitude toward online protection, and (iv) are responsible for their own online cyber security. Fedinand (2015) conducted a qualitative multiple case study exploring best practices technology leaders use to minimize security breaches and increase business performance, and the study revealed four major elements that can further reduce security breaches and improving business performance which are:

i. an organizational culture promoting security awareness.
ii. consistent organizational security policies and procedures.
iii. implementation of security awareness education and training to mitigate insider threats.
iv. organizational commitment to adopt new technologies and innovative processes.

3. Methodology

This study used an Empirical Analysis as it is obtainable in other Computer Science research (Salami et. al 2022). This entails the use of quantitative descriptive analysis in analyzing the data collated from SMEs owners, managers and other staff that fall in the targeted categories. Empirical analysis is an evidence-based approach for the study and interpretation of information. The sample size chosen for this study is 250 SMEs owners, managers and other staff irrespective of their gender, educational qualification or occupation. The questionnaire was designed using google form and self-administered both physically and online.

The tools used for the study are questionnaires and SPSS (Statistical Product and Service Solutions) for the collection and analysis of data. Descriptive statistical tools such as frequency count, mean, and standard deviation was used. The data collected through the administered questionnaire was collected and subjected to descriptive and inferential analysis. Both Frequency distribution and Percentage were used to determine the number of respondents in every section. The questionnaire was structured into three thematic areas with a total of thirty five questions.

Cronbach's alpha was employed to assess the reliability, or internal consistency, of the set of test items to justify the extent to which it is a consistent measure of the concept. Cronbach's alpha takes values from 0 to 1, with 1 being the highest value, meaning perfect internal consistency. A Cronbach's alpha with value higher than 0.7 is considered as reliable in comparison with values lower than 0.7 which is not considered reliable.

The following Cronbach's alpha formula was used to get a conclusive result.

$$\alpha = \frac{N \cdot \bar{c}}{\bar{v} + (N-1) \cdot \bar{c}} \quad (1)$$

Where:

N = the number of items in a group

$\bar{c}$ = the average covariance between paired items

$\bar{v}$ = the average variance

Cronbach's alpha is thus a function of the number of items in a test, the average covariance between pairs of items, and the variance of the total score.

Therefore, the set of test items gave the following output:

i. Assessment of SMEs Cyber Security Present Infrastructure

Reliability Statistics

Cronbach's Alpha	N of Items
.743	8

ii Assessment of SMEs Owners mode of Cyber Security Strategies

Reliability Statistics

Cronbach's Alpha	N of Items
.739	13

iii Assessment of Government policies that affects Cyber Security in Nigeria

Reliability Statistics

Cronbach's Alpha	N of Items
.725	4

Therefore, since all test items are higher than 0.7, it is considered reliable.

4. Findings and Discussion

A total of 250 questionnaires were distributed out both physically and online to participants and a total of 229 questionnaires was returned. 190 of the returned questionnaires distributed physically were complete and usable, 39 responses were received from the online participants, with an overall response rate of 85%. Only the 229 answered questionnaire returned were useful after data cleaning and filtration

.

Table 4.1 Respondents' Demography

Items	Variables	Frequency	Percent
What is your gender	Male	143	62.4
	Female	86	37.6
	Total	**229**	**100.0**
Items	**Variables**	**Frequency**	**Percent**
What is your age	29 and below	38	16.6
	30-39	83	36.2
	40-49	59	25.8
	50 and above	49	21.4
	Total	**229**	**100.0**
Items	**Variables**	**Frequency**	**Percent**
What is your highest academic qualification	Primary	11	4.8
	Secondary	36	15.7
	Graduate	111	48.5
	Post graduate	67	29.3
	Others	4	1.7
	Total	**229**	**100.0**
Items	**Variables**	**Frequency**	**Percent**
What sector does your organization operate	Financial	48	21.0
	Inform. and comm.	31	13.5
	Manufacturing	29	12.7
	wholesale/retailing	42	18.3
	Health	31	13.5
	Others	48	21.0
	Total	**229**	**100.0**
Items	**Variables**	**Frequency**	**Percent**
How many staff are in your organization	1 - 20	47	20.5
	21 - 40	86	37.6
	41 - 60	48	21.0
	61 - 80	28	12.2
	81 - 100	20	8.7
	Total	**229**	**100.0**
Items	**Variables**	**Frequency**	**Percent**
What is your job area of specialization	Human Resources	35	15.3
	Admin./Operations	57	24.9
	Finance/Accounting	35	15.3
	Sales/Marketing	41	17.9
	Info. Technology	27	11.8

	Others	34	14.8
	Total	**229**	**100.0**
Items	**Variables**	**Frequency**	**Percent**
What is your work experience in years?	less than 5 years	47	20.5
	between 5 - 10 years	82	35.8
	between 10 - 15 years	100	43.7
	Total	**229**	**100.0**

As seen in Table 4.1, there is a growing occurrence among the young age group that are venturing into entrepreneurship with respondents between the ages of 30 – 39. SMEs in Nigeria contribute 48% of national Gross Domestic Product (GDP) in the last five years, account for 96% of businesses and 84% of employment (Pricewaterhousecoopers SME Survey 2020). 48.5% of respondents are well educated with a first degree, while the highest response with 37.6% was received from organisations with 21 – 40 employees. The respondents that have the highest work experience is between 10 – 15 years with 43.7%.

Table 4.2 **Assessment of SMEs Cyber Security Present Infrastructure**

Items	**Variables**	**Frequency**	**Percent**
Does your organization currently have a website or social media account	No	14	6.1
	Indifferent	2	.9
	Maybe yes	13	5.7
	Yes	200	87.3
	Total	**229**	**100.0**
Items	**Variables**	**Frequency**	**Percent**
Does your organization and employees use email	No	11	4.8
	Indifferent	1	.4
	Maybe yes	14	6.1
	Yes	203	88.6
	Total	**229**	**100.0**
Items	**Variables**	**Frequency**	**Percent**
Do you use online payment options for your organization and customers	No	12	5.2
	Indifferent	1	.4
	Maybe yes	14	6.1
	Yes	202	88.2
	Total	**229**	**100.0**
Items	**Variables**	**Frequency**	**Percent**
Does your organization allow employee use personally owned devices such as smart phones, tablets, home laptops or desktop computers to carry out regular business activities	No	59	25.8
	Indifferent	1	.4
	Maybe yes	33	14.4
	Yes	136	59.4
	Total	**229**	**100.0**
Items	**Variables**	**Frequency**	**Percent**
Which of the cyber attack have your	Computers becoming infested	40	17.5

organization experience	with viruses, spyware or malware		
	Money stolen electronically	38	16.6
	Breaches from personally owned devices from social media	28	12.2
	Personal information stolen electronically	23	10.0
	None	100	43.7
	Total	**229**	**100.0**
Items	**Variables**	**Frequency**	**Percent**
What or who do you think was the source of the cyber attacks	Website	21	9.2
	Third party suppliers	35	15.3
	Emails attachments	22	9.6
	Employee	51	22.3
	Indifferent	100	43.7
	Total	**229**	**100.0**
Items	**Variables**	**Frequency**	**Percent**
If any, approximately how much do you think the cyber attack have cost your organization financially	Less than N5,000,000	73	31.9
	Less than N10,000,000	8	3.5
	Above N10,000,000	5	2.2
	Above N20,000,000	3	1.3
	Indifferent	140	61.1
	Total	**229**	**100.0**
Items	**Variables**	**Frequency**	**Percent**
How often does your organization provide employees with internal cyber security trainings?16. How often does your organization provide employees with internal cyber security trainings?	Variables	Frequency	Percent
	Weekly	4	1.7
	Monthly	33	14.4
	Quarterly	55	24.0
	Annually	53	23.1
	None	84	36.7
	Total	**229**	**100.0**

Table 4.2 shows that most of the respondents have a website or social media account with a high percentage of 87.3% (200) and 86.6% (203) use email services. This implies that SMEs are vulnerable to cyber attack since they use these platforms either for sales or advertising their goods and services. In the Table 4.2, 88.2% (202) of respondents also use online payment options for their organization and customers and 59.4% (136) of respondents allow employee use personally owned devices which has heightened security concerns such as unauthorized access, theft and fraud which make SMEs vulnerable to cyber attack. Table 4.2 shows that majority of respondents have experience at least one type of attack and 22.3% (51) of respondents indicated that employees were the major source of cyber attack because they are still unaware of the danger this can cause to their businesses. It was observed in Table 4.2 that the effect of a cyber attack have cost 31.9% (73) of respondent less than N5,000,000. Though as seen in Table 4.2 that majority of the SMEs provide internal training some SMEs still need to do more in providing regular awareness and training to their employees to keep them informed of the latest cyber

threat and what to expect. Training empowers employees with an up to date know how on how to recognize and mitigate a cyber threat.

Table 4.3 **Assessment of SMEs Owners mode of Cyber Security Strategies**

Items	Variables	Frequency	Percent
What is your position in your organisation?	Manager	64	27.9
	Owner of business	53	23.1
	Supervisor	44	19.2
	Others	63	27.5
	None	5	2.2
	Total	**229**	**100.0**
Items	**Variables**	**Frequency**	**Percent**
How would you rate your knowledge or understanding of Cyber security strategies?	Very low	15	6.6
	Low	36	15.7
	Indifferent	4	1.7
	High	70	30.6
	Very high	104	45.4
	Total	**229**	**100.0**
Items	**Variables**	**Frequency**	**Percent**
How many desktop and laptop computers does your organisation have?	0 - 5	74	32.3
	6 - 10	68	29.7
	11 - 15	33	14.4
	16 - 20	13	5.7
	21 and above	41	17.9
	Total	**229**	**100.0**
Items	**Variables**	**Frequency**	**Percent**
Does your organization have any security measures deployed? (The use of antivirus on Computers)	No	16	7.0
	Maybe yes	26	11.4
	Yes	187	81.7
	Total	**229**	**100.0**
Items	**Variables**	**Frequency**	**Percent**
Is your security mechanism effective and updated?	No	17	7.4
	May be no	2	.9
	Indifferent	3	1.3
	Maybe yes	34	14.8
	Yes	173	75.5
	Total	**229**	**100.0**
Items	**Variables**	**Frequency**	**Percent**
What is your organizations level of awareness of a cyber attack	Very low	19	8.3
	Low	33	14.4
	High	70	30.6
	Very high	107	46.7
	Total	**229**	**100.0**

Items	**Variables**	**Frequency**	**Percent**
How does your organization decision makers rate cyber security	Very low	19	8.3
	Low	24	10.5
	Indifferent	2	.9
	High	78	34.1
	Very high	106	46.3
	Total	**229**	**100.0**
Items	**Variables**	**Frequency**	**Percent**
Has the use of cyber security technology and strategies had any significant impact on your organizations operation	No	8	3.5
	Indifferent	6	2.6
	Maybe yes	90	39.3
	Yes	125	54.6
	Total	**229**	**100.0**
Items	**Variables**	**Frequency**	**Percent**
If yes to the above, how would you rate the level of impact	Very low	19	8.3
	Low	15	6.6
	Indifferent	22	9.6
	High	63	27.5
	Very high	110	48.0
	Total	**229**	**100.0**
Items	**Variables**	**Frequency**	**Percent**
Does your organization see Information Technology (IT) as a crucial part of its strategy	No	13	5.7
	Maybe yes	78	34.1
	Yes	138	60.3
	Total	**229**	**100.0**
Items	**Variables**	**Frequency**	**Percent**
Does your organization have a Cyber Security Strategic Plan that is part of its overall	No	36	15.7
	Indifferent	5	2.2
	Maybe yes	59	25.8
	Yes	129	56.3
	Total	**229**	**100.0**
Items	**Variables**	**Frequency**	**Percent**
Does your organization have a dedicated budget for cyber security	No	48	21.0
	Indifferent	4	1.7
	Maybe yes	66	28.8
	Yes	111	48.5
	Total	**229**	**100.0**
Items	**Variables**	**Frequency**	**Percent**
If yes, approximately how much is	Less than N1,000,000	78	34.1

budgeted for cyber security	Between N1,000,000 and N2,000,000	23	10.0
	Between N3,000,000 and N5,000,000	8	3.5
	Above N6,000,000	4	1.7
	Indifferent	116	50.7
	Total	**229**	**100.0**

Table 4.3 show different positions held by respondents in their organisations on SMEs Owners mode of Cyber Security Strategies. 45.4% (104) have knowledge and understanding of cyber security strategies. SMEs must make cyber security a core aspect of their business strategy as they are in fact one of the most common targets for cyber attackers. As seen in Table 4.3, 81.7% (187) of respondent deploy the use of antivirus software in their systems. Although antivirus software is good and necessary, it is only a part of security measure. SMEs can be attacked from anywhere, as many of these attacks are designed to avoid antivirus software. Table 4.3 shows that 75.5% (173) of respondents indicated that their security mechanism are effective and updated. Antivirus software is not the only protection businesses need to stay secure, one thing antivirus software can't protect you from are insider threats. It also show that respondents awareness level of an attack is very high, and that SMEs owners or decision makers rate cyber security very high. 54.6% (125) however, respondents indicated that the use cyber security technology and strategies had significant impact in their organizations operation and also sees Information Technology (IT) as a crucial part of its strategy with 60.3% (138). Irrespective of their responses, most SMEs still fall prey to cyber criminals, this is worrisome and calls for concern. In Table 4.3, 56.3% (129) have Cyber Security Strategic Plan as part of their overall organizational strategic plan and 48.5% (111) of respondent have a dedicated budget for cyber security. Despite the impressive responses from respondent, it does not mean that the plan put in place are actually followed as more SMEs still experience cyber attacks. Lastly, Table 4.3 shows that 34.1% respondents budgeted less than N1,000,000, while 10.0% budgeted between N1,000,000 and N2,000,000. The researcher drew a conclusion that though budgeting is based on the size of the business because most SMEs do not have enough funding and resources to invest in cyber security. Cyber criminals recognize that they have higher chances of succeeding when they attack SMEs as compared to large organizations because of poor cyber security strategies.

Table 4.4 **Assessment of Government policies that affects Cyber Security in Nigeria**

Items	Variables	Frequency	Percent
Is your organization aware of any specific compliance requirements and regulation regarding cyber security	No	29	12.7
	Indifferent	3	1.3
	Maybe yes	64	27.9
	Yes	133	58.1
	Total	**229**	**100.0**

Items	Variables	Frequency	Percent
If yes, what is the level of knowledge of your employees about the related legislation requirements	Very low	23	10.0
	Low	27	11.8
	Indifferent	24	10.5
	High	58	25.3
	Very high	97	42.4
	Total	**229**	**100.0**
Items	**Variables**	**Frequency**	**Percent**
If No, what is the pace of urgency with which it is required for the purpose of a robust SME business environment	Not urgent	34	14.8
	Fairly urgent	41	17.9
	Indifferent	40	17.5
	Immediate urgency	51	22.3
	Very urgent	63	27.5
	Total	**229**	**100.0**
Items	**Variables**	**Frequency**	**Percent**
Would your organization be open to considering having a strategic cyber security plan or framework for SMEs in Nigeria	No	1	.4
	May be no	1	.4
	Indifferent	3	1.3
	Maybe yes	48	21.0
	Yes	176	76.9
	Total	**229**	**100.0**

In Table 4.4, 58.1% (133) are aware of specific compliance requirements and regulation regarding cyber security and majority of the respondent have a high knowledge of related requirements. Also, 27.5% (63) of respondents indicated the need for a robust SME business environment is very urgent. This can be achieved by producing user security policies showing what acceptable and secure use of systems should be. The policies should include staff training at all levels in the organisation to create a culture where cyber security is prioritized. In Table 4.4, 76.6% (176) respondents indicated the need for a cyber security framework for SMEs in Nigeria because SMEs are more vulnerable to cyber threats, regardless of the many existing cyber security standards or frameworks. The existences of SMEs are threatened if an attack by a cyber criminal is successful. Therefore, there is a need to understand the challenges SMEs are facing and how to mitigate cyber attacks.

4.1 Key Findings:

The following are key findings made from the research.

i. There is an appreciable level of SMEs that own at least website or social media account and use e-mail services while a substantial level of SMEs (45.4% and 30.6%) responded that they have knowledge and understanding of cyber security

strategies, but the level at which they provide training for employees calls for concerns as only 1.7% and 14.4% provide weekly and monthly training respectively.

ii. Some of the SMEs admitted that they have experience at least one type of attack. 46.7 % of respondents have very high level of awareness of a cyber attack, and business owners rate cyber security very high. Despite the awareness level, it is worrisome to note that most SMEs still fall prey to cyber criminals.

iii. More SMEs are still likely to be expose to cyber attacks because 59.4% allow employee use personally owned devices such as smart phones, tablets, home laptops to carry out regular business activities that might not have proper security configuration.

iv. The result shows that 76.9% of SMEs admitted that they are opened to having a cyber security framework for SMEs in Nigeria.

5. Conclusion and Recommendation

Considering the evidence from the survey, it is easy to perceive that SMEs are vulnerable to cyber threats regardless of many existing cyber security standards or frameworks. The existing frameworks are generally expensive, broad, require certifications and expert with vast knowledge which makes it difficult for SMEs to implement. It is clear that most of the existing frameworks are not understood by SMEs because of its complexity and this has led to a growing concern among SMEs as 76.9% of SMEs attested to the fact that there is need for a cyber security framework for SMEs in Nigeria. Not all SMEs have considered security implication that their website, social media account, using online payment options and allowing employees use personal owned devices have simply because some of them have very little knowledge of IT to understand the impact of security. This can expose SMEs to unauthorized access, theft, fraud and device hacking which can be catastrophic to the business. Therefore, the framework will be robust and easy to implement and it will address security concerns faced by SMEs in Nigeria. The significance of the study is to address the current cyber security problems experienced by SMEs in Nigeria and it will serve to aid SMEs in Nigeria to identify and mitigate specific risks and steps that can be taken to address them in a cost effective manner and achieving the same aim as a global framework**.**

References

Aiken, M., Mc Mahon, C., Haughton, C., O'Neill, L., & O'Carroll, E. (2016). A consideration of the social impact of cybercrime: examples from hacking, piracy, and child abuse material online. Contemporary Social Science, 11(4), 373–391. https://doi.org/10.1080/21582041.2015.1117648

Anandarajan, M., D'Ovidio, R., & Jenkins, A. (2013). Safeguarding consumers against identity-related fraud: examining data breach notification legislation through the

lens of routine activities theory. International Data Privacy Law, 3(1), 51–60. https://doi.org/10.1093/idpl/ips035

Armenia, S., Angelini, M., Nonino, F., Palombi, G., & Schlitzer, M. F. (2021). A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs. Decision Support Systems, 147, 113580. https://doi.org/10.1016/j.dss.2021.113580

Arora, B. (2016). Exploring and analyzing Internet crimes and their behaviours. Perspectives in Science, 8, 540–542. https://doi.org/10.1016/j.pisc.2016.06.014

Baggott, S. S., & Santos, J. R. (2020). A risk analysis framework for cyber security and critical infrastructure protection of the U.S. electric power grid. Risk Analysis, 40(9), 1744– 1761. https://doi.org/10.1111/risa.13511

Benz, M., & Chatterjee, D. (2020). Calculated risk? A cybersecurity evaluation tool for SMEs. Business Horizons, 63(4), 531–540. https://doi.org/10.1016/j.bushor.2020.03.010

Calabrese, R., Andreeva, G., & Ansell, J. (2019). "Birds of a feather" fail together: Exploring the nature of dependency in SME Defaults. Risk Analysis, 39(1), 71–84. https://doi.org/10.1111/risa.12862

Chatterjee, D. (2019). Should executives go to jail for cybersecurity breaches? Journal of Organizational Computing and Electronic Commerce, 29(1), 1– 3.

Disterer, G., & Kleiner, C. (2013). Using mobile devices with BYOD. International journal of web portals, 5(4), 33–45. https://doi.org/10.4018/ijwp.2013100103

Eturpa Salami, E., OMOROGIUWA, O., & Joseph Ogbogbo, L. (2022). AN EMPIRICAL SURVEY TO SUBSTANTIATE THE NEED FOR IMPROVEMENT IN USER SECURITY AWARENESS IN MOBILE BANKING IN NIGERIA. International Journal of Research Publications, 108(1). https://doi.org/10.47119/ijrp1001081920223844

Federal Communications Commission. (2014). Cyber Security Planning Guide. https://www.fcc.gov/sites/default/files/cyberplanner.pdf

Fedinand, J., & Kongnso. (2015). ScholarWorks Best Practices to Minimize Data Security Breaches for Increased Business Performance. https://scholarworks.waldenu.edu/cgi/viewcontent.cgi?article=2928&context=dissertations

Harris, A. M., & Patten, P. K. (2014). Mobile device security considerations for small- and medium-sized enterprise business mobility. Information Management & Computer Security, 22(1), 97–114. https://doi.org/10.1108/imcs-03-2013-0019

Hoppe, F., Gatzert, N., & Gruner, P. (2021). Cyber risk management in SMEs: insights from industry surveys. Journal of Risk Finance, 22(3/4), 240–260. https://doi.org/10.1108/JRF-02-2020-0024

Jafari-Sadeghi, V. (2021). Internationalisation, risk-taking, and export compliance: A comparative study between economically advanced and developing Country. International Journal of Entrepreneurship and Small Business, 43(3), 384– 408. https://doi.org/10.1504/IJESB.2021.10039076

Jafari-Sadeghi, V., Garcia-Perez, A., Candelo, E., & Couturier, J. (2021). Exploring the impact of digital transformation on technology entrepreneurship and technological market expansion: The role of technology readiness, exploration and exploitation. Journal of Business Research, 124(2021), 100–111. https://doi.org/10.1016/j.jbusres.2020.11.020

Jansen, J., Veenstra, S., Zuurveen, R., & Stol, W. (2016). Guarding against online threats: why entrepreneurs take protective measures. Behaviour & Information Technology, 35(5), 368–379. https://doi.org/10.1080/0144929x.2016.1160287

Kabanda, S., Tanner, M., & Kent, C. (2018). Exploring SME cybersecurity practices in developing countries. Journal of Organizational Computing and Electronic Commerce, 28(3), 269–282. https://doi.org/10.1080/10919392.2018.1484598

Layton, R., & Watters, P. A. (2014). A methodology for estimating the tangible cost of data breaches. Journal of Information Security and Applications, 19(6), 321–330. https://doi.org/10.1016/j.jisa.2014.10.012

Muhati, E. (2018). Factors affecting cyber-security in Kenya -a case of small medium enterprises. URL:https:// su-plus.strathmore. edu/ bitstream/ handle/ 11071/ 6013/ Factors%20affecting%20cyber%20-%20security%20in%20Kenya%20-%20A%20Case% 20of%20Small%20Medium%20Enterprises.pdf?sequence=3.

Njenga, K., & Jordaan, P. (2016). We want to do it our way: The neutralization approach to managing information systems security by small businesses. The African Journal of Information Systems, 8(1), 3. 42-63. Retrieved from http://digitalcommons.kennesaw.edu/ajis/

Pricewaterhousecoopers. (2020). *PwC's MSME Survey 2020 Building to Last Nigeria* report. https://www.pwc.com/ng/en/assets/pdf/pwc-msme-survey-2020-final.pdfRae, A., & Patel, A. (2019). Defining a new composite cybersecurity rating scheme for SMES in the U.K. URL: http://eprints.staffs.ac.uk/5922/2/ISPEC19V3Comments.pdf.

Shah, M. H., Jones, P., & Choudrie, J. (2019). Cybercrimes prevention: promising organisational practices. Information Technology and People, 32(5), 1125–1129. https://doi.org/10.1108/ITP-10-2019-564

Singh, R., Chandrashekar, D., Subrahmanya Mungila Hillemane, B., Sukumar, A., & Jafari-Sadeghi, V. (2022). Network cooperation and economic performance of

SMEs: Direct and mediating impacts of innovation and internationalisation. Journal of Business Research, 148, 116–130. https://doi.org/10.1016/j.jbusres.2022.04.032

Srinidhi, B., Yan, J., & Tayi, G. K. (2015). Allocation of resources to cyber-security: The effect of misalignment of interest between managers and investors. Decision Support Systems, 75, 49–62. https://doi.org/10.1016/j.dss.2015.04.011

Symantec Corporation . (2016). Internet Security Threat Report Internet Security Threat Report CONTENTS. https://docs.broadcom.com/doc/istr-21-2016-en

United States Small Business Administration (SBA). (2014). Do small businesses need to worry about cyber security? Washington, DC. Retrieved from https://www.sba.gov/blogs/do-small-businesses-need-worry-about-cyber-security