Nigerian Journal of Technology (NIJOTECH)
Vol. 41, No. 3, May, 2022, pp.512-520
www.nijotech.com

Print ISSN: 0331-8443
Electronic ISSN: 2467-8821
http://dx.doi.org/10.4314/njt.v41i3.10

Improving Cybersecurity Incidents Reporting in Nigeria: Micro and Small Enterprises Perspectives

F. E. Ikuero[1], W. Zeng[2]

[1] *Nigeria Computer Emergency Response Team, Abuja, NIGERIA*
[2] *School of Computer Science and Informatics, De Montfort University, Leicester LE1 9BH, UNITED KINGDOM*

Abstract
Leveraging on the provisions of the internet enhances the productivity of Micro and Small Enterprises (MSEs), increases industrial growth and their contributions to national prosperity. Every cyber-attack against their businesses should be reported to the requisite incident response body through the appropriate channels for quick recovery from attack. This research examines how the MSEs in Nigeria report cybersecurity incidents. This study surveyed 100 MSEs. The outcome of the research shows that 72% of the MSEs is unaware of the channel of reporting cyber incidents and does not report cyber incidents. Participants totaling 90% believe that the Sectoral Computer Security Incident Response Team (CSIRT) could improve on reporting of cybersecurity incidents through sensitisation. Amongst others, we recommended the Sectoral CSIRTs were to develop an Incident Report and Response Plan (IRRP) for managing cybersecurity incidents in MSEs.

Keywords: MSEs, Cyber-attacks, Cybersecurity, Incident response, Policy and Strategy

1.0 INTRODUCTION

The computer-driven information era has made communication and transactions across the globe easier, facilitate, and enhance business growth. It steers up vast opportunities for the prosperity of the MSEs to thrive, which enhances national, economical, and industrial development. Although the cyber-age provides ease for MSEs in doing business, it is also prone to rising issues of cyber-attacks, which could negate the sustainability of productivity and developmental contribution to the national growth process [1, 2, 3]. Attacks would be possible when vulnerabilities on the networks, operating systems, users, and processes are exploited [4]. When attacks against MSEs are not reported to the establishments that are responsible for cyber incidents response and mitigation, the Government may not know the nature and trend of such incidents, therefore, marring adequate planning, response, and mitigation strategies [5]. The Federal Government of Nigeria (FGN) established the Nigeria Computer Emergency Response Team (ngCERT) to coordinate incident response and mitigation strategies for the prevention of cybersecurity incidents in Nigeria. Also, it enacted the Cyber-crimes (Prohibition, Prevention, Etc) Act, 2015, and formulated the National Cybersecurity Policy and Strategy (NCPS) 2021 [6]. The policy document provides a blueprint for designated sectors to develop their CSIRT or Security Operation Centre (SOC) for organisations [2]. Consequently, all enterprises are to report cyber-incidents to their Sectoral CSIRT or SOC. The continual widespread of internet usage in Nigeria's MSEs Operation with increasing cyber-attacks could ruin unsuspecting enterprises, lead to poverty and devastation if necessary measures are not emplaced [7]. Cyber-attacks can impede the output of enterprises, lead to business collapse, loss of patent rights, and would negatively affect their contribution to economic growth [8, 9]. In order to sustain its growth and contribution to the economic growth value-chain system, it is required that MSEs report any cybersecurity incidents that occur in their business operations to the CSIRT or SOC in their sector. However, many MSEs are seen to have a very weak defence against cyber-attacks and lack the importance of cybersecurity; thus, they do not have good knowledge of the precautions to adopt in the face of cyber incidents [8-11]. For cybersecurity incidents to be reported, stakeholders of MSEs need to know the medium of reporting, and the organisations they should report attacks to. In order to sustain business growth and increase productivity, we are compassionate in eliminating unawareness in reporting cybersecurity incidents against MSEs, which could increase the national Gross Domestic Product and enhance development. There are some existing works about the

*Corresponding author **(Tel:** +234 (0) 8057725360**)**
Email addresses: fikuero@cert.gov.ng (F. E. Ikuero), wen.zeng.wz@gmail.com (W. Zeng)

cybersecurity incidents on MSEs in Nigeria cyber-attacks. However, these studies are theoretical; the researchers do not have real data to support their study. There are no individuals or groups of people that have conducted research on this topic in the past. Consequently, we consider it crucial to gather our data from MSEs for the originality and all-inclusiveness of the research. Therefore, the aim of this research is to investigate the opinions of MSEs on cyber incidents reporting channels and identify their views on the need for improving on existing mediums.

This paper is structured as follows: Section 2 is the related work; Section 3 is composed of the basic concepts in this paper. Section 4 will discuss the research model and then section 5 clarifies the methodology. Thereafter, section 6 will discuss and analyse the findings of this study. Finally, Section 7 will conclude the paper.

2.0 RELATED WORKS

In Saleem, [12], the authors stressed the importance of applying mitigation strategies in deterring cyber-attacks. They posited that one of the ways to mitigate cybersecurity incidents is to ensure that all devices connected to the internet run on the latest patch update of the software and hardware manufacturer. Similarly, [13] argued that hackers usually evaluate patches following the pronouncement by the vendors and exploit vulnerabilities faster than organisations could fix them. Therefore, early dissemination of vulnerability disclosure to MSEs will help to improve cybersecurity in the Nigeria cyber space. However, these studies did not identify the types of computer systems that MSEs use for their daily business transactions. Identifying the types of systems being used by the MSEs would make it easier to be specific in disseminating information such as cybersecurity advisories regarding the kind of systems that require such patches instead of generalising it. Some types of systems commonly used by MSEs are: Desktops, LaptopS, Servers, Phones, and Printers

In [2, 14], the researchers alluded that many MSEs are unaware of cybersecurity incidents against their businesses; hence do not raise concerns regarding the incidents. Similarly, the MSEs in Nigeria lack adequate awareness of cybersecurity and information security policy; therefore, implementation could be a mirage [14]. In another development, many MSEs believed that they face fewer attacks by cyber criminals compared to big enterprises [14]. Therefore, they could ignore attacks on their cyber platforms and sometimes consider them as issues from Internet Service Providers or malfunctioning of the computing devices. The situations that that could make cyber criminals succeed in attacking MSEs are numerous with variations. The variations make it complicated for organisations to have a holistic knowledge about cyber-attacks. In this era of business dependence online with increasing attacks, naivety in the implementing cybersecurity principles needs to be reduced. Thus, there is a need for FGN to educate all stakeholders of MSEs on cybersecurity policy across Nigeria, particularly the regulating body of each sectors that would cascade it to the grassroots with a view to enlighten them on the reporting channel. [15].

However, understanding of the fundamentals on which attacks could take place, organisations can minimise the chances of cyber-attacks and any related danger. MSEs access the internet through their Mobile Network Operators using any of the following:

a. Access points such as Wireless Fidelity (WiFi)
b. SIM Cards
c. Internet Modem
d. Routers

Cybersecurity sensitisation is another aspect that researchers have studied in the past. It refers to the act of engaging stakeholders to know what to do and taking actions in protecting enterprises' information systems. Cybersecurity sensitisation is designed to involve stakeholders in deliberations for them to understand the threats, the impacts of attacks on business, and the actions required to prevent cyber criminals from penetrating into their computer networks and systems; thereby potentially reducing risks [16-17]. In this era of business dependence online, naivety in the application of technology needs to be reduced. Thus, there is a need for FGN to sensitise all stakeholders of MSEs on cybersecurity across Nigeria, particularly the regulating body of each sectors that would cascade it to the grassroots with a view to educating them on cyber incidents reporting channel.

In [18], the authors asserted that MSEs are among those who contribute to the nation's economic development. Therefore, they emphasised the need to sensitise MSEs on information security. Amongst others, they discussed the use of social media platforms, which include Facebook in conducting sensitisation. In [1, 13], the writers affirmed that most cybersecurity incidents in Nigeria are not reported; thus, it is difficult to ascertain the nature and the extent of attacks. According to the survey conducted by [16, 19], the majority of those who participated were unaware of how and where to report cybersecurity incidents. Therefore, [16, 19] connotes increasing sensitisation of the public on where and how to report cyber-attacks. While it is important to beef up sensitisation, we recommend sector-based workshops for

organisations and community campaign for the public with Key Performance Indicators that will measure impact.

2.1 Basic terminologies

MSEs are business ventures that respectively employ less than 10 people with assets worth less than NGN50 Million, from 50 to 49 staff having assets worth of NGN5 Million but less than NGN50 Million with the exclusion of land and building [10]. In Nigeria, high percent of the entire businesses are MSEs [8]. Therefore, they are regarded as the pivot for the growth of the nation's economy [4]. The MSEs play a remarkable role in the growth of Nigeria's economy including job and wealth creation. To this regard, the Nigeria government has put in place the policy and strategy for reporting cyber incidents to protect their business operations against attack for enhancing cybersecurity [2].

Cyber refer to the components of computer, virtual reality as well as information and communication technology. Similarly, cyber-attacks mean the exploitation of the vulnerabilities on any of the components or devices, processes and technology [5]. The rate of cyber-attacks against MSEs is increasing by the day. Despite the increase, many MSEs seem to be ignorant that they are primary targets of cyber-attacks [5, 10]. It is therefore, necessary for CSIRTs to sensitise every MSEs under their purview on the reality of cyber-attacks with a view to taking measures to preventing attacks against their systems.

Cybersecurity refers to the protection of the confidentiality, integrity, and availability (CIA) of information systems as well as data in the face of attacks [18]. It also means a combination of rules emplaced in order to protect the cyber domain [12]. Confidentiality entails protecting information and data from disclosure to unauthorised individual or group of persons and parties. It means ensuring that information could be accessed by only those who has been authorised to do so. Integrity of data refers to protection of data from alteration. While availability is when information, data and services are accessible to those who have the authority access it whenever they need it [4, 12]. Cybersecurity attempts to ensure that users or enterprises' information infrastructure and assets are protected against all related risks.

Cybersecurity Incident Response (CIR) refers to actions undertaken when compromise exists or is suspected on interconnected systems such as computer networks. Actions of CIR involve organising capabilities, handling incidents and post incidents activities [20, 21]. It is the responsibility of the incident response bodies such as national CERT, sectoral CSIRT, and organisational SOC to detect and prevent all MSEs from cyber-attacks. Those affected by cyber-attacks should report to the appropriate authority. However, the efficacy of these bodies hinge on the capabilities of the technologies and manpower [2].

Policy is a set of principles proposed by an organisation. Implementing cyber security policy is a great challenge to every nation. However, the FGN have developed its cybersecurity policy in order to promote business growth through digitalisation, protect the privacy of their citizenry and prevention of cybercrimes [7]. The existing cybersecurity policy effort of the FGN in addressing cybersecurity issues has not satisfactorily tackled the urgent challenges threatening its cyberspace [7, 22, 23]. When policies are implemented accordingly, it will enable MSEs and their relevant stakeholders to reduce threats on their computer systems, enforce security programs according to standards and effectively communicates security measures to all stakeholders [24, 25, 26]. Improving cybersecurity incidents reporting through policy enforcement could be achieved when coordinating bodies and organisations adopts most suitable approach to reach the target audience [25, 27, 28].

Some approaches that could be adopted by Sectoral CSIRT to improve reporting of cybersecurity incidents in MSEs include:

a. Sensitisation
b. Developing Information Security Policy (ISP)
c. Enforcement of ISP

Cybersecurity threat mitigation connotes the application of security policies and procedures for reducing the impact of cybersecurity threats in organisations, nations and worldwide [29, 30]. At the present times, mitigating cybersecurity threat is an essential concern to every organisation that is internet savvy and operates digitally online [3, 31]. Cybersecurity incidents mitigation is challenging for the organisations even as they put in efforts to prevent threats against their information systems [3, 9, 32]. MSEs may not have the capability that could fight complex cybersecurity concerns, but compliance to cybersecurity policies will mitigate some threats associated with their cyber systems.

2.2 Research Model

This Section highlights the approach of the research. It generated questionnaire to investigate respondents' opinion on cybersecurity incidents reporting in MSEs. The paper collated data from every respondent, which are presented in tabular form. Participants' opinions, which form the data, were evaluated for recommendations that would improve on mitigating cyber-attacks. Respondents were required to provide answers to five (5) questions as follows:

a. Which computer system does your organisation use mostly?
b. Has cyber incident occurred in your organisation's computer/network systems?
c. How does your organisation reports cybersecurity incidents?
d. What is the main reason responsible for non-reporting of cyber-attacks in your organisation?
e. How would cybersecurity incidents reporting in MSEs be improved through Sectoral CSIRT?

3.0 METHODOLOGY

The study used primary and secondary sources of methodologies. It physically administered questionnaires in hard copy paper format to participants in 100 MSEs. Microsoft Excel application was used in analysing the feedback from the respondents. These questions were administered to employees of MSEs. These MSEs were chosen for this study because they use information systems for their daily business transaction including file and documents transfers, place order for goods and services. Others include browsing the internet, learning, buying and selling amongst others. Additionally, the chosen MSEs render services that cut across all sectors of the Nigeria's economy such as telecommunications, aviation, defence, security, education and power. The relevance of their services in these sectors and their contributions to the economy was another reason why the research chooses the MSEs for the investigation. For example, if the MSEs' cyber platforms are massively attacked, the country will experience the impact of colossal losses. Physical distribution of questionnaires was considered because some micro and small enterprises would need elaborate explanation on cyber terminologies used in the investigation. Where necessary, we used our findings to juxtapose opinions from previous researchers, which form secondary sources from literature including books, journals as well as publications relating to cyber incidents and ways of reporting incidents. The survey, which was conducted in the Abuja Municipal Area council of Abuja in Nigeria, investigated the opinions of participants that are 18 years and above. It is our opinion that as adults, they are capable of providing information from informed and uninfluenced knowledge. The study carefully considered the participants bearing in mind their job functions and the authority they have in disseminating company's information. From the pilot the questionnaire, we found that the managers, Information Security Officer, Information and Communication team would be suitable for the survey as these categories of employees are responsible for making decisions and handling issues of cybersecurity matters in their organisations.

4.0 FINDINGS AND ANALYSIS

The findings will be illustrated in Tabular form while some of them will be further shown in graphical format.

4.1 Popular computer systems used in organisations

In Table 1 and figure 1, we established that the 100 MSEs investigated have phones for their business transactions while 60, 40 and 20 organisations respectively owns desktops, laptops and printers. Furthermore, 15 organisations each have servers and other computing devices. Also, it was gathered that 60% of the MSEs use phones more than any other computer systems. While 22% of the respondents affirms that their organisation use desktop than other devices, 18% of the participants opined that their organisations depends on laptops than any other computer systems in their businesses.

4.1.1 Analysis on popular computer systems used in organisations

The findings regarding the type of computer systems used in organisations revealed that all the investigated MSEs have phones that they use for running their businesses. This is a reflection that the generality of MSEs rely on the usage of phones more than any other computer systems in the conduct of their businesses. These phones could be the desk or mobile type. However, the survey observed that mobile phones are mostly deployed by MSEs in their businesses. The reason for this could be due to the capabilities and services those mobile phones, particularly the GSM offers.

Table1: **Popular systems used in organizations**

Which of the following computer systems does your organisation have?						
	Desktops	**Laptops**	**Servers**	**Phones**	**Printer**	**Others**
Number of Organization	60	40	15	100	20	15
Which of the systems is mostly used by your organisation?						
	Desktops	**Laptops**	**Servers**	**Phones**	**Printer**	**Others**
Responses (%)	22	18	Nil	60	Nil	Nil

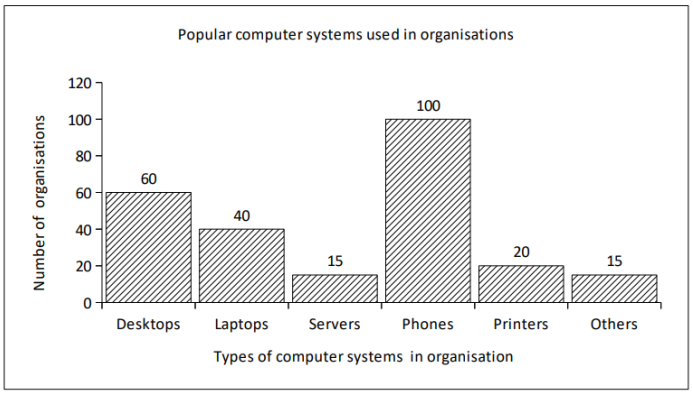

Figure 1: Types of computer systems used in organisation

Additionally, mobile phones are handy, smart and they have different price ranges making it easily affordable by users. This may in no doubt allow increase in the number of devices that engage the use of mobile phones for businesses leading to increasing MSEs connected to the internet. To this regard, stakeholders and employees of MSEs should be exposed to the fundamental practices for safe online presence via phone connectivity. More so, there is need for further investigation into phone applications that are commonly used by MSEs with a view to addressing vulnerabilities associated with them.

4.2 Cybersecurity incidents occurrence in organisations

In Table 2 and figure 2, 25% of the respondents affirmed that their organisation has experienced cyber-attacks.

Table 2: Cybersecurity incidents occurrence

Have your organization ever experienced attack on its computer/network systems?			
	Yes	No	Unknown
Responses (%)	25	60	15

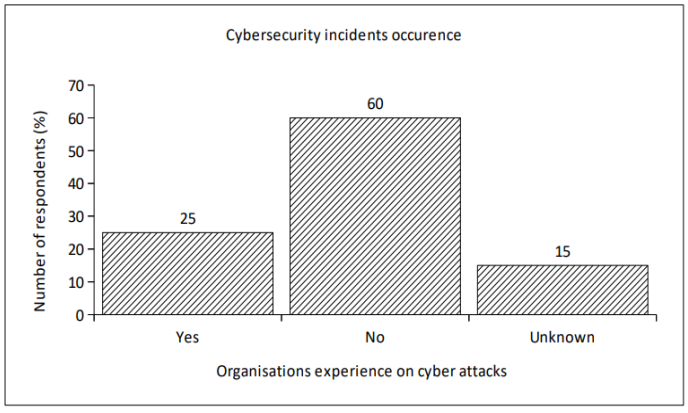

Figure2: Cybersecurity incidents occurrence

On the other hand, 60% had never experienced attacks while 15% respondents were unknown to attacks.

4.2.1 Analysis on Cybersecurity incidents occurrence

The findings in Table 2 as illustrated in figure 2, clearly shown that majority of the MSEs investigated have never been attacked. This corroborates the viewpoint of [2] that some MSEs are ignorant of cybersecurity incidents against their companies. Weighing this result, it raises the concerns that they may have been attacked but they did not know about the incident occurrence. With the increase in the number of devices connected to the internet, regulatory authorities must ensure a corresponding increase in the level of cyber incidents awareness among the MSEs; otherwise the organisations will be increasingly exposed to the dangers associated with the internet. Consequently, the regulatory bodies; especially the ngCERT and all Sectoral CSIRTs would be required to develop and implement awareness program to educate MSEs on how to identify cybersecurity incidents.

4.3 Cybersecurity incidents reporting

Table 3 represented the investigated views of respondents on cybersecurity incidents reporting based on three questions. Firstly, respondents were asked if they knew any channel for reporting cybersecurity incidents.

Table 3: Cybersecurity incidents reporting

Do you know any channel/medium of reporting cybersecurity incidents?		
	Yes	No
Responses (%)	25	75
Do you know the organisation to report cybersecurity incidents?		
	Yes	No
Responses (%)	30	70
Does your organisation report cybersecurity incidents?		
	Yes	No
Responses (%)	15	85

While 75% of the participants were not aware, 25% of them were aware of the channel for reporting cyber-attacks. In another instance as depicted in figure 3, 70% did not know the organisation to report attacks. However, 30% knew the organisation to report attacks. Similarly, Fig. 4 graphically illustrated the investigation that revealed 15% of the MSEs report cybersecurity incidents while 85% do not.

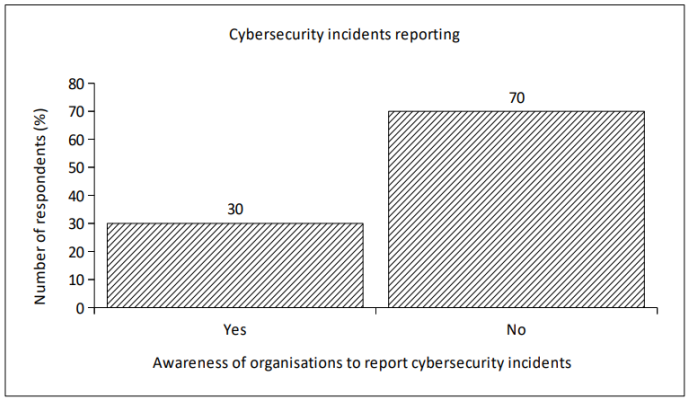

Figure 3: Awareness of organisation in reporting incidents

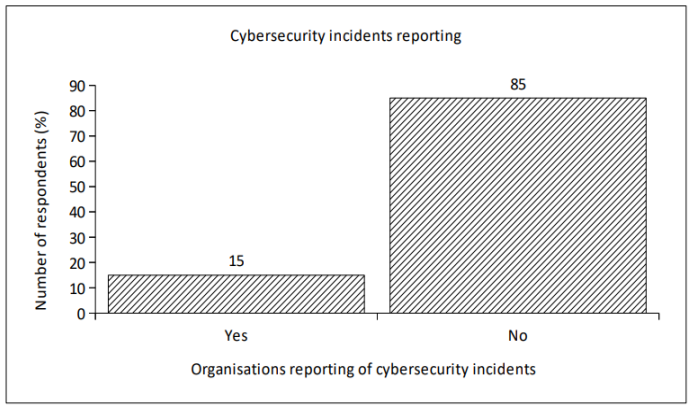

Figure4: Cybersecurity incidents reporting

4.3.1 Analysis on cybersecurity incidents reporting

The response from the participants on cyber attack reporting revealed that 75%, which represent the majority were of the opinion that they do not know any channel for reporting the cyber attack. Essentially, transactions occur in MSEs on daily basis. During the transactions, occurrences of attacks on computer networks of companies are inevitable. However, the knowledge of the attacks and how to report such attacks is headway to proffering solutions that will mitigate its future occurrence. We, therefore, recommend all major stakeholders at the strategic level; the ngCERT and Sectoral CSIRT at the operational level to continually sensitise stakeholders on their roles in implementing the NCPS 2021. Also, 70% of the respondents are unaware of the organisation to report incidents when attacks occur in their organisation's computer and network systems. Similarly, 85% of the MSEs do not report attacks occurrence in their business cyber infrastructure. The foregoing could be due to the lack of the implementation of NCPS 2021 by the Sectoral CSIRT. However, for some sectors where implementation exists, there may be issues of cascading it down to the MSEs. Therefore, it is important that ngCERT enforce implementation and compliance with the MSEs.

4.4 Reasons for non-reporting of cyber attacks

In Table 4, which is shown in figure 5 graphically, we examined the reasons why MSEs do not report cyber-attack. A total of 72% of the respondents were unaware of cybersecurity incidents reporting channels, and 28% were ignorant of organisation to report attack.

Table4: Reasons for non-reporting of cyber attacks

What do you think is the main reason why MSMEs do not report cyber-attack?		
	Unaware of reporting channels	Ignorant of organization to report attack
Responses (%)	72	28

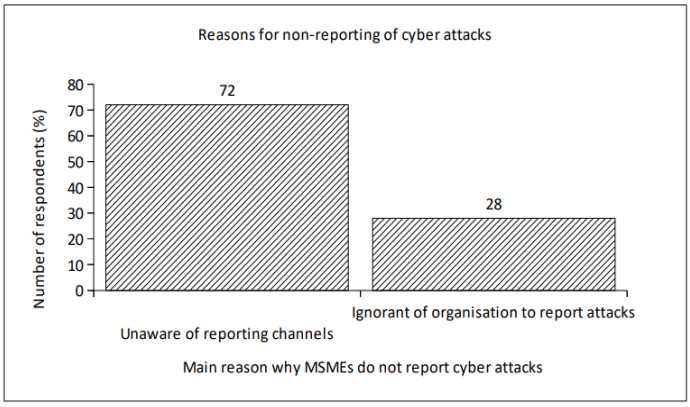

Figure5: Reasons for non-reporting of incidents

4.4.1 Analysis on reasons for non-reporting of cyber attacks

Two criteria were used to investigate the opinions of respondents on the reasons why MSEs do not report cyber-attacks. The first criterion (unaware of reporting channels) had 72% opinions while the second criterion (ignorant of organisation to report attack) recorded 28% views. This outcome might not be unconnected to the fact that many Sectoral CSIRTs have not done enough in cascading the NCPS 2021 implementation to the various MSEs under their various industries.

More so, ngCERT could collaborate with the relevant Law Enforcement Agencies to implement compliance policy by enforcing Section 21 of Nigeria Cybercrimes (Prohibition, Prevention, ETC) ACT, 2015. This Section of the Acts mandates all operators and users of the computer system to report any cyber incident within the period of 7 days to ngCERT, which is the national CERT. As stipulated therein, failure to report such incidents will be penalised accordingly. If this Section is enforced, users, operators, MSEs will learn lessons and be responsible for all their actions regarding cyber-attack reporting. In this regard, ngCERT should consider the

enforcement of Section 21 of the Nigeria Cybercrimes (Prohibition, Prevention, ETC) ACT, 2015.

Collaboration between ngCERT and Sectoral CSIRTs in developing an Incident Report and Response Plan (IRRP) could be an effective way of managing cybersecurity incidents in MSEs. To this end, MSEs could report incidents through their regulatory Sectoral CSIRTs. For example, MSEs under telecommunications sector are required to report incidents through the Nigeria Communications Commission's CSIRT while those in the Defence sector are to report cybersecurity incidents to the Defence Space Administration's CSIRT.

4.5 Improving cybersecurity incidents reporting in MSEs through Sectoral CSIRT

Table 5 demonstrates the opinions of respondents' view on the role of Sectoral CSIRT for improving reporting of cybersecurity incidents in MSEs. In the findings, 10% said no while 90% affirmed yes as shown in Figure 6.

Table 5: Improving cybersecurity incidents reporting in MSMEs through Sectoral CSIRT

Do you think Sectoral CSIRT could improve reporting of cybersecurity incidents in MSMEs?			
	Yes	No	
Responses (%)	90	10	
Which approach do you think would be most effective for Sectoral CSIRT to improve reporting of cybersecurity incidents in MSMEs?			
	Sensitization	Developing Information Security Policy (ISP)	Enforcement of ISP
Responses (%)	70	10	20

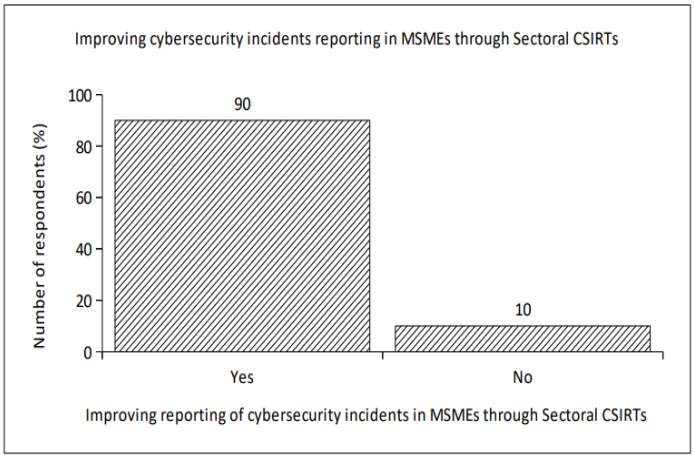

Figure 6: Improving cybersecurity incidents reporting

Additionally, respondents totalling 70% affirms that sensitisation would be the best approach to improve reporting of cybersecurity incidents in MSEs. Furthermore, developing and enforcing ISP respectively pulled 10% and 20%.

4.5.1 Analysis on Role of Sectoral CSIRT in cybersecurity incidents reporting in MSEs

In Table 5, majority of the respondents believed that Sectoral CSIRT could improve the reporting of cybersecurity incidents in MSEs through sensitisation approach. Therefore, Sectoral CSIRTs should collaborate with all stakeholders including ngCERT, ISPs, organisations in their sector to conduct sensitisation programs every quarter. An efficient way of sensitising those in the academia and the public is to incorporate cyber education curriculum across all the levels of education in Nigeria. Furthermore, Sectoral CSIRTs should consider taking cybersecurity awareness campaigns to organisations and employees under their domain. For measuring the effectiveness of the sensitisation, Sectoral CSIRT could develop an Impact Assessment Framework (IAF).

5.0 CONCLUSION

This study discussed cybersecurity incidents reporting in Nigeria's MSEs. It highlighted the consequences of non-reporting of incidents. It further stresses the measures that the Nigerian government has put in place to ensure safe cyberspace that is resilient to attacks. For clarity and easy comprehension, vital terminologies and concepts were explained in the paper. They include cyber-attacks, policy, and cybersecurity mitigation amongst others. Questionnaires were administered to participants on a face-to-face approach to enable us to exploit the views of employees of 100 MSEs regarding cybersecurity incidents reporting. Thereafter, we analysed the data collected, made deductions and recommendations accordingly. The research advocates many MSEs are unaware of the channels and organisation to report cybersecurity incidents. With the opinion of the participants, it is believed that Sectoral CSIRT are capable able of improving the reporting of cybersecurity incidents in MSEs through sensitisation approach in Nigeria. The contributions, future works and recommendations drawn from the study are highlighted subsequently.

5.1 Contributions

a. The study enriches cybersecurity in Nigeria.
b. As MSEs become more aware of the how and where to report cybersecurity incidents, it will help

the FGN in identifying the prevailing type and trend of cyber attacks.

c. As ngCERT, Sectoral CSIRT and other stakeholders play their roles; the Nigeria cyberspace would be more resilient and safer for MSEs to conduct transactions.
d. It strengthens the security of the global cyber space.
e. It contributes a novel literature to the academia.
f. It exposes incident reporting more realistic to the academic world.
g. Future researchers could consider researching into the most common phone applications used by MSEs in order to unravel the vulnerabilities that exist in such platform and thereafter develop a solution that will eliminate the weakness.

5.2 Future Works

This study did not consider medium and large enterprises as well as cloud computing. In future, research could consider investigating cybersecurity reporting in the medium and large enterprises both in the traditional and cloud computing. Future works could research on the costs of cyber attacks on MSEs and Nigeria both in monetary value and materials.

5.3 Recommendations

From the research analytical deductions, we recommend as follows:

a. The ngCERT should consider enforcing implementation and compliance of Section 21 of the Nigeria Cybercrimes (Prohibition, Prevention, ETC) ACT, 2015 in MSEs.
b. Sectoral CSIRTs should collaborate with ngCERT to develop an IRRP for managing cybersecurity incidents in MSEs.
c. Sectoral CSIRTs should conduct sensitisation programs for MSEs every quarter.
d. Sectoral CSIRTs should consider developing IAF to measure the effectiveness of the sensitisation program.

REFERENCES

[1] Alya Geogiana Buja. ''Cyber security features for national e-learning policy''. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, 12(5), 2021, pp. 1729–1735.

[2] David Koeppe. ''Towards guidelines for medical professionals to ensure cybersecurity in digital health care'', *In The Ethics of Cybersecurity, Springer Cham*, 2020, pp. 331–345.

[3] Mu'azu Abdullahi Saulawa and MK Abubakar. "Cyber-crime in Nigeria: An overview of cybercrime act 2013'', Journal of Law and Policy Rate *Globalization*, 32 (23), 2014.

[4] Yeongjin Jang, Chengyu Song, Simon P Chung, Tielei Wang, and Wenke Lee. "A11y attacks: Exploiting accessibility in operating systems'', *In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, 2014, pp. 103–115.

[5] ABM Kamrul Riad, Hossain Shahriar, Maria Valero, and Mokter Hossain. ''Cybersecurity risks and mitigation techniques during covid-19'', *IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC)*, 2021, pp. 1351–1356.

[6] Adewunmi James Falode, Babajimi Oladipo Faseke, and Chukwuma Ikeanyichukwu. ''Artificial intelligence: The missing critical component in nigeria's security architecture'', *SSRN*, 2021, 3896657.

[7] Sanya Ojo. "*A Case of Internet Insecurity on SMEs in Nigeria: A Cybercafé Entrepreneur Experience",* SAGE Publications, SAGE Business Cases Originals, 2021.

[8] Yuchong Li and Qinghui Liu. ''A comprehensive review study of cyber-attacks and cyber security; emerging trends and recent developments'', *Energy Reports*, 7, 2021, pp. 8176– 8186.

[9] Davide Settembre-Blundo, Rocío González-Sánchez, Sonia Medina-Salgado, and Fernando E García-Muiña. "Flexibility and resilience in corporate decision making: A new sustainability-based risk management system in uncertain times'', *Global Journal of Flexible Systems Management*, 22(2), 2021, pp. 107–132.

[10] Tracey Caldwell. "Securing small businesses–the weakest link in a supply chain?'', *Computer Fraud & Security*, (9), 2015, pp. 5–10.

[11] Karen Renaud and Jacques Ophoff. "A cyber situational awareness model to predict the implementation of cyber security controls and precautions by smes'' *Organizational Cybersecurity Journal: Practice, Process and People*, 2021.

[12] Alireza Shojaifar and Heini Järvinen. "Classifying smes for approaching cybersecurity competence and awareness'', *In The 16th International Conference*

on Availability, Reliability and Security, 2021, pp 1–7.

[13] Linan Huang and Quanyan Zhu. ''Duplicity games for deception design with an application to insider threat mitigation'', *IEEE Transactions on Information Forensics and Security,* 16, 2021, pp. 4843–4856.

[14] James A Lewis. *Raising the bar for cybersecurity*. Center for Strategic and International Studies, 2013.

[15] Adewale Adegoke Alawiye-Adams and Bosede Awoyemi. "Cash-less economy policy and remote on-us'atm transaction fee in nigeria'', Available SSRN 2014, 2528608.

[16] Salah Kabanda, Maureen Tanner, and Cameron Kent. ''Exploring sme cybersecurity practices in developing countries'', *Journal of Organizational Computing and Electronic Commerce*, 28(3), 2018, pp. 269–282.

[17] Andrei-Laurent,iu MITROFAN, Elena-Veronica Cruceru, Andreea Barbu, et al. "Determining the main causes that lead to cybersecurity risks in smes'', *Business Excellence and Management*, 10(4), 2020, p.38.

[18] Christopher A Moturi, Nabihah R Abdulrahim, and Daniel O Orwa. "Towards adequate cybersecurity risk management in smes'', *International Journal of Business Continuity and Risk Management*, 11(4), 2021, pp. 343–366.

[19] Peter RJ Trim and Yang-Im Lee. "The role of b2b marketers in increasing cyber security awareness and influencing behavioural change'', *Industrial Marketing Management*, 83, 2019, pp.224–238.

[20] Ahmad Zamsuri, Wenni Syafitri, and Eddis Syahputra Pane. "Evaluation of information security awareness on digital marketing (case study of msme in indonesia)'', *Advances in Humanities and Contemporary Studies*, 2021, 2(1) pp.192–210.

[21] Kwasi Adomako, Nabeel Mohamed, Aminata Garba, and Martin Saint. "Assessing cybersecurity policy effectiveness in Africa via a cybersecurity liability index'', *TPRC*, 2018.

[22] Alexandra Gaillard. "Cybersecurity challenges and governance issues in the cyberspace' when stronger passwords are not enough: Governing cyberspace in contemporary African nations' case study: Can South Africa and Nigeria secure cyberspace without a lock?'', *SSRN*, 2021, 3877526.

[23] Abayomi Jegede, Grace Odii, Marcus Magaji, Gilbert Aimufua, et al. "Assessment of security awareness level of mobile device users in tertiary institutions in plateau state of Nigeria'', *Journal of Advanced Computing Technology and Application (JACTA)*, 2021, pp 1–8.

[24] Ahmad Rufai, Salisu Modi, and Buhari Wadata. "A survey of cyber-security practices in Nigeria'', *International Research Journal of Advanced Engineering and Science*, 2021, pp 222–226.

[25] Andrea Calderaro and Anthony JS Craig. "Transnational governance of cybersecurity: policy challenges and global inequalities in cyber capacity building'', *Third World Quarterly*, 2020, 41(6) pp. 917–938.

[26] Adamu A Garba and Aliyu M Bade. ''The current state of cybersecurity readiness in Nigeria organizations''. *Educational Research (IJMCER)*, 3(1), 2021, pp. 154–162.

[27] Gurdip Kaur, Ziba Habibi Lashkari, and Arash Habibi Lashkari. ''Introduction to cybersecurity In Understanding Cybersecurity Management in FinTech'', *Springer*, 2021, pp. 17–34.

[28] Ibikunle Frank and Eweniyi Odunayo. "Approach to cyber security issues in Nigeria: challenges and solution'', *International Journal of Cognitive Research in science, engineering and education*, 2013, 1(1) pp.100–110.

[29] Odumesi John Olayemi. "A socio-technological analysis of cybercrime and cyber security in Nigeria'', *International Journal of Sociology and Anthropology*, 6(3), 2014, pp. 116–125.

[30] Andrea Calderaro and Anthony JS Craig. "Transnational governance of cybersecurity: policy challenges and global inequalities in cyber capacity building'', *Third World Quarterly*, 41(6), 2020, pp. 917–938.

[31] Eric C Thompson, *Cybersecurity incident response: How to contain, eradicate, and recover from incidents*, Apress, 2018.

[32] Shari L Pfleeger. "Improving cybersecurity incident response team (CSIRT) skills, dynamics and effectiveness'', *Technical report, Trustees of Dartmouth College Hanover United States, 2017*.