UNIZIK JOURNAL OF ENTREPRENEURSHIP (ENTREP) Vol:2 No: 1
ISSN: 2814-2004 eISSN: 2814-2012. December, 2021 Edition
https://unizikentrepjournal.com

PHYSICAL AND OPERATIONAL CYBER SECURITY VULNERABILITIES OF SMALL AND MEDIUM SCALE ENTERPRISES IN ANAMBRA STATE

Onyemaobi, Ngozi, Nwosu, Ngozi Loretta

Amobi, Stella Chinyere (Ph.D)

Department of Technology and Vocational Education,
Faculty of Education, Nnamdi Azikiwe University,
Awka, Anambra State, Nigeria
Email:oluchiobum@gmail.com

Abstract

The study determined the physical and operational cyber security vulnerabilities of small and medium scale enterprises in Anambra State. Two research questions guided the study. The descriptive research design was adopted for the study. The population of the study comprised 150 information technology managers in ICT training centres in Anambra State. Instument for data collection was a validated questionnaire developed by the researcher. Test of reliability of the instrument using Cronbach Alpha method yielded co-efficient values of .84 and 0.86 with an overall reliability co-efficient of 0.85. Mean and standard deviation was used to analyze data for the study. Findings revealed that erratic electric supply, extreme temperature, inadequate physical access control and vandalism among others are physical cyber security vulnerabilities of Small and Medium Scale Enterprises in Anambra State. Finding also showed that failure to resolve of security incidents, poor handling of security incidents, insufficient recording of system activity, failure to ensure control over software installation, poor control over encryption keys and lack of review of system activity records among others are operational cyber security vulnerabilities of Small and Medium Scale Enterprises in Anambra State. Based on these findings the following recommendations were made among others that owners of SMEs should ensure that they ensure that the physical cyber security infrastructures required for ensuring the safety of critical business data and information are provided. It was also recommended that SMEs should ensure that high priority attention is given to the monitoring and review of system information behaviour and log.

Keywords: Physical, Operational, Cyber Security, Vulnerabilities, SMEs

Introduction

The state of insecurity bedeviling Anambra State in particular and Nigeria in general has become an issue for national and international concern. Anambra State in recent times has become a haven for different types of criminal activities ranging from kidnapping, armed robbery, banditry and cyber crimes. Cyber crimes have over the years become a major source of insecurity in Anambra Sate (Udelue & Mathias; Odo & Odo, 2015). More particularly, the Internet is becoming increasingly popular as a means of conducting business for Small and Medium-Sized Enterprises (SMEs), exposing them to cybercrime dangers. As a worldwide means of communication and commercial operation, Information Technology (IT) has provided a variety of opportunities to SMEs over time. However, SMEs' reliance on IT has rendered them exposed to newer IT security concerns. Because of their association with larger corporations as clients, SMEs might be a favorite target for hackers (Amrin, 2019).

Cybercrime is defined as a crime performed on the internet that involves the use of a computer as either a tool or a target victim. Cybercrimes are defined as offenses committed against individuals or groups of individuals with a criminal motive to intentionally harm the victim's reputation or cause physical or mental harm to the victim, either directly or indirectly, through the use of modern telecommunication networks such as the Internet (chat rooms, emails, notice boards, and groups), and mobile phones (SMS/MMS) (Debarati&Jaishankar in Odo&Odo, 2015). According to Raiu (2012), the number of cyber-attacks worldwide is growing year after year, and that this trend will continue. Similarly, Gostev (2012)asserted that cyber-criminals are

growing more skilled in their use of new methods and tools for cyber-attacks in economic activity sectors by targeting enterprises and exploiting the vulnerabilities inherent in IT systems of SMEs.

Vulnerabilities in cyber-security are flaws in and around systems, networks, infrastructures, applications, and procedures (Polkowsi & Dysarz, 2017). In a nutshell, vulnerabilities are flaws in a system that is exploited to jeopardize the system's confidentiality, integrity and availability (CIA) qualities. According to Yeboah-Boateng (2013), when a system's cyber-security vulnerability is exploited, a threat is said to have been achieved, and the system is said to be under cyber-attack. A threat agent or an attacker is the entity that enabled or caused the assault. Some threat agents are human, such as end-users, whose actions may be deliberate or unintentional, and may originate from internal or external sources to the system; due to system problems, such as hardware failures, software failures, failures of related systems, malicious codes such as worms, viruses, and Trojan horses; and other environmental problems, such as power outages, natural disasters, and so on Polkowsi and Dysarz (2017) averred that there appear to be two forms of cyber security vulnerability that SMEs are exposed to. They are physical security vulnerability and operational security vulnerabilities.

Physical vulnerabilities are cyber security vulnerabilities related to insufficient physical access restrictions, inadequate equipment citation, insufficient temperature and humidity controls, insufficiently conditioned electrical power, and so forth (Raiu, 2012).In the same vein, are operational vulnerabilities are cyber threats that has to do with lack of change management, insufficient separation of duties, insufficient control over software installation, insufficient

control over media handling and storage. Others include insufficient control over system communications, insufficient access control or weaknesses in access control procedures, insufficient recording or review of system activity records, insufficient control over encryption keys, insufficient reporting, handling, and resolution of security incidents (Yeboah-Boateng, 2013). Despite being aware of the growing trend of cyber-attacks and their sophistication around the world, official statistics are unable to identify the exact volume of cyber incidents and cyber security vulnerabilities SMEs in Anambra State are exposed to. It is against this background that the physical and operational cyber security vulnerabilities of SMEs in Anambra State.

Statement of the Problem

The safety of online business transaction has continued to generate missed reaction among owners and management of SMEs in Anambra State. This is further made evident by the rising cases of crimes committed by internet fraudsters on unsuspecting SMEs and customers. Unfortunately, the use of technology has exposed SMEs to cyber security threats, which have threatened to halt their growth and, in some cases, resulted in the extinction of the company enterprise. Cyber security crimes are becoming a common occurrence in Anambra State. This is visible in ATM frauds committed by criminal syndicates looking for ATM data. Furthermore, several SMEs have lost significant sums of money to internet fraudsters and hackers who have cleaned their funds using data obtained through online activity. This threatens the growth and development of these SMEs and the overall development of Anambra State.

Purpose of the Study

The main purpose of the study was to determine the physical and operational cyber security vulnerabilities of Small and Medium Scale Enterprises in Anambra State. Specifically, the study;

1. Determined the physical cyber security vulnerabilities of Small and Medium Scale Enterprises in Anambra State.
2. Ascertained the operational cyber security vulnerabilities of Small and Medium Scale Enterprises in Anambra State.

Research Questions

The following research questions guided the study:

1. What are the physical cyber security vulnerabilities of Small and Medium Scale Enterprises in Anambra State?
2. What are the operational cyber security vulnerabilities of Small and Medium Scale Enterprises in Anambra State?

Hypotheses

The following hypotheses were tested at 0.05 level of significance:

1. There is no significant difference in the mean rating of experienced and highly experienced IT managers on the physical cyber security vulnerabilities of SMEs in Anambra State.

2. There is no significant difference in the mean rating of experienced and highly experienced IT managers on the operational cyber security vulnerabilities of SMEs in Anambra State.

Literature Review

Vulnerability is a flaw in an asset or collection of assets that is typically exploited by threat agents. A resource that is valuable to the company for the purposes of business operations and continuity is referred to as an asset. Vulnerabilities can be classified as technological, human, physical, operational, business, or compliance (Polkowsi & Dysarz, 2017). The research concentrated on physical and operational cyber vulnerabilities of SMEs. Physical vulnerabilities includes insufficient physical access restrictions, inadequate equipment citation, insufficient temperature and humidity controls, insufficiently conditioned electrical power, and so forth. Lack of change management, insufficient separation of duties, insufficient control over software installation, insufficient control over media handling and storage, insufficient control over system communications, insufficient access control or weaknesses in access control procedures, insufficient recording and/or review of system activity records and insufficient control over encrypted data are some examples of operational vulnerabilities (Yeboah-Boateng, 2013). Ojiagu and Nzewi (2019) investigated the link between physical security and the survival of small and medium-sized firms (SMEs) in Southeast Nigeria The study's aims are to establish the nature of the correlations that exist between fire outbreaks and entrepreneurial vision, burglary attacks, and product delivery time by SMEs in Southeast Nigeria. The study used a correlation survey research design. The Pearson product moment correlation coefficient was

employed to test the hypotheses at a threshold of significance of 5% (percent). The findings found that there are negative significant correlations between fire breakouts and the entrepreneurial aspirations of SMEs' owners, burglary assaults, and the time it takes for SMEs in the region to supply items to consumers. Similarly, Yeboah-Boateng (2013) determined the security challenges of SMEs in developing economies. Cyber-security and business KPIs, SMEs were polled and strategically interviewed. To analyze the cyber-security vulnerability assessment (CSVA) model, the elicited experts' opinions were used to model the risk function using neuro-fuzzy techniques, which combine the human inference style and linguistic expressions of fuzzy systems with the learning and parallel processing capabilities of neural networks. The findings suggest that the CSVA model is straightforward and intuitive, and that it can be used by SMEs to identify vulnerabilities in their assets and the risks that they face. The CSVA model was evaluated and validated utilizing adaptive network-based fuzzy inference system (ANFIS) tests using accessible sample datasets. The fuzzy similarity measures technique was used to rank vulnerability and threat taxonomies, which are benchmarked to aid SMEs in being proactive. Finally, the fuzzy cognitive map (FCM) technique is utilized to assess the presence and potential consequences of vulnerabilities in SMEs asset disposal strategies. It has been demonstrated that vulnerabilities caused by policies or their absence can have a negative influence on others. Abdulmajeed and Bob (2020) in their systematic review of literature on cyber security vulnerabilities of SMEs revealed that threats, behaviors, practices, awareness, and decision-making are the five essential factors that play a crucial role in SMEs' cyber security

risk management. Abdulmajeed and Bob noted that empirical study on cyber security risk management in SMEs is also required. It is this gap that the study filled.

Method

The descriptive survey design was adopted for the study. The population of the study consists of 150 information technology managers from ICT Training Centers in Anambra State. The instrument for data collection in this study was a structured questionnaire on a four point rating scale of Strongly Agree (SA), Agree (A), Disagree (D) and Strongly Disagree (SD). The instrument was face validated by three lecturers in the Department of Technology and Vocational Education, Faculty of Education in Nnamdi Azikiwe University, Awka. The instrument was subjected to a pilot test. The pilot test was conducted on 10 IT managers in Asaba Metropolis of Delta State who are not included in the population of the study. The Cronbach Alpha reliability method on the obtained data yielded co-efficient values of 0.84and 0.86 with an overall reliability co-efficient of 0.85.The researcher administered copies of the instrument personally and with the aid of three research assistants.Out of the 150 copies of the questionnaire administered, 128 copies were returned. This accounted for 85.33 percent return rate of the questionnaire distributed.The data collected from the respondents were analyzed using descriptive statistics like mean and standard deviation. The mean value was used to answer the research question while the standard deviation was used to ascertain the homogeneity or otherwise of the respondents' ratings.Any item with mean rating between 2.50 and above was regarded as agree while any item with mean value less than 2.50 was regarded as disagree.

To analyze the hypotheses, t-test was used to analyze the null hypotheses at 0.05 level of significance using Microsoft excel. Where the calculated t-value is less than the critical value of it, it means that there is no significant difference and the hypothesis was upheld. Conversely, where the calculated t-value is equal to or greater than the critical t value, it means that there is significant difference and the hypothesis was not upheld.

Results

Research Question 1

What are the physical cyber security vulnerabilities of Small and Medium Scale Enterprises in Anambra State?

Table 1: Respondents Mean Ratings on the Physical Cyber Security Vulnerabilities of Small and Medium Scale Enterprises (N=128)

S/No.	Item Statements	$\overline{X}$	SD	Remarks
1.	Erratic electric power supply	3.28	0.83	Agree
2.	Extreme temperature	3.81	0.90	Agree
3.	Inadequate physical access control	3.19	0.85	Agree
4.	Inadequate equipment citation	3.33	0.84	Agree
5.	Insufficient humidity controls	3.12	0.81	Agree
6.	Theft	3.35	0.87	Agree
7.	Vandalism	3.84	0.86	Agree
8.	Accidental damages	3.90	0.94	Agree
	Cluster Mean	**3.47**		**Agree**

Data in Table 1 revealed that agreed on 8 of the items, listed with mean responses ranging from 3.12 to 3.90 asphysical cyber security vulnerabilities of Small and Medium Scale Enterprises in

Anambra State. The cluster mean of 3.47 reveal that erratic electric supply, extreme temperature, inadequate physical access control and vandalism among others are physical cyber security vulnerabilities of Small and Medium Scale Enterprises in Anambra State. The standard deviation scores of the items range from 0.81 to 0.94. This shows that the respondents' opinions are homogenous.

Research Question 2

What are the operational cyber security vulnerabilities of Small and Medium Scale Enterprises in Anambra State?

Table 1: Respondents Mean Ratings on the Operational Cyber Security Vulnerabilities of Small and Medium Scale Enterprises (N=128)

S/No.	Item Statements	$\overline{X}$	SD	Remarks
1.	Lack of change management in SMEs	3.20	0.79	Agree
2.	Failure to ensure control over software installation	3.55	0.82	Agree
3.	Insufficient recording of system activity	3.65	0.87	Agree
4.	Lack of review of system activity records	3.33	0.74	Agree
5.	Poor control over encryption keys,	3.48	0.70	Agree
6.	Poor handling of security incidents	3.70	0.76	Agree
7.	Failure to resolve of security incidents	3.77	0.74	Agree
8.	Poor control over system communications	3.40	0.88	Agree
9.	Weaknesses in access control procedures	3.34	0.79	Agree
	Cluster Mean	**3.49**		**Agree**

Data in Table 1 revealed that agreed on 9 of the items, listed with mean responses ranging from 3.20 to 3.77 asoperational cyber security vulnerabilities of Small and Medium Scale Enterprises in Anambra State.The cluster mean of 3.49 reveal that failure to resolve of security incidents, poor handling of security incidents, insufficient recording of system activity, failure to ensure control over software installation, poor control over encryption keys and lack of review of system activity records among others are operational cyber security vulnerabilities of Small and Medium Scale Enterprises in Anambra State.

Discussion

Finding of the study revealed that erratic electric supply, extreme temperature, inadequate physical access control and vandalism among others are physical cyber security vulnerabilities of Small and Medium Scale Enterprises in Anambra State. This finding is in agreement with Raiu (2012) who reported that SMEs are faced with physical security cyber threats which expose their business information and assets. According to Polkowsi and Dysarz (2017), exposures to high temperatures, vandalism and theft were major physical cyber security vulnerabilities of SMEs. Yeboah-Boateng (2013) stated that most SMEs struggle to provide the needed infrastructure and environment that would facilitate the security of their cyber space. The struggle to ensure proper cyber security among SMEs have been blamed on their inability to access funds and failure to attract the best IT security experts to man their digital security space.

Furthermore, finding revealed that failure to resolve of security incidents, poor handling of security incidents, insufficient recording of system activity, failure to ensure control over software installation, poor control over encryption keys and lack of review of system activity records among others are operational cyber security vulnerabilities of Small and Medium Scale Enterprises in Anambra State. This finding is in line with Yeboah-Boateng (2013) who stated that SMEs are exposed to cyber vulnerabilities because of the failure of its management to engage in proper operational procedures that could ensure the safety of their cyber assets. According to Amrin (2019), SMEs are have limited expertise in managing cyber security measures unlike the big companies. Amrin noted that SMEs do not pay adequate attention to operational protocols that would facilitate the protection of their cyber assets. Thus,Yeboah-Boateng (2013) emphasized the use of highly experienced professionals who are knowledge in the management of cyber securities.

Conclusion

Based on the findings of the study the research concludes that small and medium scale enterprises in Anambra State are faced with problems of physical and operational cyber security vulnerabilities. SMEs need to ensure that necessary measure to protect their critical information assets are put in place to ensure the safety of their business operations. It is therefore imperative that measures to assess and evaluate their cyber vulnerabilities are taken seriously.

Recommendations

The following recommendations are made based on the findings of the study:

1. Owners of Small and Medium Scale Enterprises (SMEs) should ensure that they ensure that the physical cyber security infrastructures required for ensuring the safety of critical business data and information are provided.
2. Owners of Small and Medium Scale Enterprises (SMEs) should ensure that high priority attention is given to the monitoring and review of system information behaviour and log.
3. Managers of SMEs engage in security awareness, training and education for their employees. This will help to keep them abreast on the enterprise policies on cyber security and current trends in cyber security in business organizations.

References

Abdulmajeed, A. & Bob, D. (2020). *Cyber security risk management in small and medium-sized enterprises: a systematic review of recent evidence*. https://www.researchgate.net/publication/342933159

Amrin, N. (2019). *The impact of cyber security on SMEs*. A Master's Thesis, Faculty of Electrical Engineering, Mathematics and Computer Science, University of Twente.

Gostev, A. (2012). Cyber-threat evolution: The year ahead. *Computer Fraud & Security*, 9-12

Odo, Chinasa R & Odo, A. I. (2015).The extent of involvement in cybercrime activities among students' in tertiary institutions in Enugu State of Nigeria. *Global Journal of Computer Science and Technology: H Information & Technology, 15*(3), 1-8.

Ojiagu, N.C. & Nzewi, H.N. (2019) Physical security and survival of small and medium scale enterprises (SMEs) in Southeast, Nigeria. *American Journal of Industrial and Business Management, 9,* 1284-1300. https://doi.org/10.4236/ajibm.2019.95085

Polkowsi, Z &Dysarz, J. (2017). IT security management in small and medium scale enterprises. *Scientific Bulletin-Economic Sciences, 16*(3), 134-148

Raiu, C. (2012). Cyber-threat evolution: The past year. *Computer Fraud & Security*, 5- 8.

Udelue, M.C. & Mathias, B. (2019).Prevalence of cybercrimes among youths in Onitsha South Local Government Area of Ananmbra State, Nigeria. *International Journal of Health and Social Inquiry, 5*(1), 82-106.

Yeboah-Boateng, E. O. (2013). *Cyber-security challenges with SMEs in developing economies: Issues of confidentiality, integrity & availability (CIA)* (1 ed.). Institut for Elektroniske Systemer, Aalborg Universitet.