International Journal of Innovative Research in Social Sciences and Strategic Management Techniques
p-ISSN: 2465-728X | e-ISSN: 2467-8155
Volume 8, Number 1 January, 2021
IJIRSSSMT

Impact of Cybercrime on Selected Small and Medium Enterprises (SMEs) in the Federal Capital Tertiary (FCT)

[1]**Fadairo-Cokers Olumide Adegboyega & [2]Ibrahim Gerarh Unaru**
[1&2]*Institute of Governance and Development Studies,*
Nasarawa State University, Keffi

Article DOI: 10.48028/iiprds/ijirsssmt.v8.i1.09

Abstract

The internet brings so many opportunities for economic, social, and other activities. On the other hand, internet activities have created cybercrimes which have been a major challenge to the business environment, especially the small and medium enterprises. Therefore, this study examined the impact of cybercrimes on small and medium enterprise's activities in the Federal Capital Tertiary (FCT). The study used structured questionnaires, a population of two thousand, eight hundred and twenty-five (2825) Small and Medium Enterprises (SMEs) in Federal Capital Tertiary, and a sample size of three hundred and fifty (350). The study used the mean of descriptive analysis and Statistical Package for Social Science (SPSS) for the estimation of the mean values of the cybercrime indicators (Hacking and Spamming cybercrimes (HSC), Cyber Theft and Identity Theft Cybercrimes (CTITC), Financial Fraud and Laundering Cybercrimes (FFLC) and Website Cloning Cybercrimes (WECC)). However, the mean ratings of the various responses were calculated and were used to answer the research questions. The mean of 1, 2, 3, and 4 is 2.50 for this study; a mean rating of 2.51 or above was regarded as significant while a mean rating less than 2.50 was regarded as insignificant in explaining the changes in the variables under study. Also, the study findings revealed that hacking and spamming cybercrimes (HSC), cyber theft and identity theft cybercrimes (CTITC), financial fraud and laundering cybercrimes (FFLC) and website cloning cybercrimes (WECC) have a negative impact on Small and Medium Enterprises (SMEs) activities in Federal Capital Tertiary (FCT). Therefore, the study recommended that the government and all concerned agencies should design measures in controlling and preventing hacking, spamming, financial fraud, and laundering cybercrimes since these are the major cybercrimes affecting SME activities. And also, there need for increased literacy for SMEs to mitigate against hacking, spamming, financial fraud, laundering, and website cloning.

Keywords: *Cybercrime, Small and Medium Enterprises, Cyber security*

Corresponding Author: Fadairo-Cokers Olumide Adegboyega

http://internationalpolicybrief.org/journals/international-scientific-research-consortium-journals/intl-jrnl-of-innovative-research-in-soc-sci-strategic-mgt-techniques-vol8-no1-january-2021

Background to the Study

The commencements of the internet and the widened access to computer technology have created new opportunities for work and business activities especially the activities of the small and medium enterprises and those who perpetrate illegal activities. The increase in technology and online communication has not only produced a dramatic increase in the incidence of criminal activities. Still, it has also brought in what seems to be a new wave of criminal activities (Odumesi, 2014). Thus, the increase in the engagement of computer criminal activities and the possible wave of new sorts of criminal activity poses challenges for legal systems and law enforcement (Brenner, 2007). However, technological development has produced massive shifts in the capability to reproduce, control, distribute and publish information; the internet, in particular, has massively changed the economics and fast of reproduction (Longe and Chiemeke, 2008).

Also, computer networks have massively changed the economics of distribution and transmission speeds approaching a billion characters per second; networks enable sending information products worldwide, cheaply, and almost instantaneously. For Nigeria, a nation saving her face from cybercrime activities, efforts are now being channeled at the sources and channels in which cybercrime activities are perpetuated. The processes of re-stigmatizing cybercrime and re-dignifying honest is not as easy as institutionalizing a deterrence mechanism like the code of conduct bureau, Independent Corrupt Practice Commission (ICPC), Economic and financial crime commission (EFCC), and many more. After some years at the top ladder of the corrupted nations of the world, which is based on Transparency International (TI) index, an anti-corruption crusader group? The internet brings so many opportunities for economic, social, and other activities. However, with cybercrime, the internet also brings its risks (Odumesi, 2014).

Thus, what are the menace cybercrime and cyber security threats pose to Nigeria? Waziri (2009) explained the dreadful level of how corruption has been a threat to our Vision 20:2020 especially in the development of small and medium enterprises. In 2007, an internet crime report itemized Nigeria's name as third in online crime action and cybercrime occurrence amid the sufficient number of young Nigeria (Sesan, 2010). Fadare (2015) opined that information communication technology uprising already has an impact virtually in almost every area of human effort. In the mid-1990s, the banking sector in the utmost part of the world was meek and dependable, but since the arrival of the technology era, the banking area saw exemplar change in marvel, ICT also fetched unintentional penalties for examples: criminal actions, spamming, credit cards frauds, phishing, identity theft, and other interrelated cybercrimes and these cybercrimes have been a threat to business environments in which the small and medium enterprises operate. According to Jegede and Olowookere (2014),cyber-crime represents the negative fallout of internet technology and e-commerce. If left unchecked, it may constitute a major setback in small and medium enterprises development in turn national growth and development. This is because nations with a high rate of cyber fraud could be blacklisted and estranged from international trade and relations which will affect the activities of small and medium enterprises. It is imperative to explore and examine the impact of cybercrimes on small and medium enterprises' activities in Federal Capital Tertiary (FCT).

Literature Review

Conceptual Review

According to Akingunola (2011), 'Small and medium scale enterprises', 'small and medium enterprises', 'small and medium industries', are some of the terms that are used interchangeably to describe this group of business organizations. They are a very heterogeneous group because they embrace a wide variety and diverse forms ranging from village handcraft makers/outfits, small machine shops, restaurants, and computer software firms. They could operate in very different markets and social environments. While some owners are poor, others are not. Some are dynamic, innovative, and growth-oriented; others are traditional and prefer to remain small.

According to World Bank Small enterprises are business organizations between 10 and 50 employees; total assets/total annual sales between US$100,000 and US$3 million. At the same time, Medium-sized enterprises are business organizations between 50 and 300 employees; total assets/total annual sales between US$3 million and US$15 million (Jegede, 2018). While, according to the Central Bank of Nigeria **SME** is any enterprise with a maximum asset base of N500 million excluding land and working capital and with the number of staff employed not less than 10 or more than 300 (**CBN**, 2005).

On the other hand, Schelland Clemens, (2004) see cybercrime as a crime identified with technology, personal computer, and the web. It involves governments, commercial enterprises, including the citizens global, and cybercrime takes the piracy system, procurement of free phone calls, cyberbully, cyber terrorism, and cyber pornography. While, Milhorn,(2007) defines cybercrime activity as that which engages in internet crime and fraudulent activities; in most of the developed countries and some developing countries, there is the main database that has details of all citizens and has links to other databases such as the car registration database held at the driver's vehicle licensing agency and to another powerful computer running the automated fingerprint identification system. The same thing has also applied to foreigners in developed countries. All foreigner fingerprints and international passport numbers are inside the database; this integrated system helps track crime.

Empirical Review

There are several empirical studies on cybercrime, SMEs, and related literature, but for this study, selected studies on cybercrime and SMEs were reviewed; among them is the work of Asokhia, (2010) gave a rough estimate of the cost of risks in the e-commerce arena. In a study comprising 285 merchants, it was reported that the percentage revenue loss per merchant was relatively flat for the years surveyed. However, the total dollar to fraud increased substantially from S1.9 billion in 2003 to S2.6 billion in 2004. The rise in dollar loss over this period was attributed to the exponential increase in the volume of Internet transactions that rose from 25 percent to 30 percent in the same period reviewed. In 2004, merchants estimated that an average of 1.3 percent of their orders was fraudulent. 15 percent of the merchants indicated that the average of fraudulent orders was 263 more than 20 percent of the total orders for the period. The median value of these fraudulent orders was S150 or 50 percent above the average value of all valid orders. 58 percent of merchants surveyed confirmed acceptance of orders outside the USA and Canada where the transaction and study took place.

Jegede and Olowookere (2014), examined the opportunities and the negative impacts associated with the use of Internet technology in the era of E-Business. Contextually, it zeroed on the activities of youths as they engage in online fraud as a means of survival in Nigeria. It further postured that the Internet medium tremendously promoted e-commerce and simultaneously created a new form of socio-economic insecurity that is highly unprecedented in world history. The magnitude of vulnerability and concomitantly the monetary loss often attendant of wireless transaction cross-culturally engenders fear, skepticism, and disillusionments among Internet users in the cyber environment. To minimize this trend, the authors were of the view that a special inbuilt security mechanism attachable to the Internet technology hardwires be provided for the censorship of online monetary related interactions. This unique configuration is expected to serve as checks against fraud and other maladaptive uses of the technology by cyber predators. Fadare (2015) considered cybercrime and its impact on online banking in Nigeria. Adoption of ICT in banks helps them to enhance customer services, assisted precise records, guarantee suitable business hours, improve quicker services, also there has been advancement in the image of the banks which hints to a broader, quicker, and more effectual market. Also, it has enabled work to be easier and more stimulating. The study set out to observe the impact of ICT tools for combating cybercrime in Nigeria online banking, the study approached the concern issue of cybercrime from the theoretical & practical contribution perspectives. Data gotten from these research instruments were subjected to descriptive analysis & regularity tallies in ways to describe the actions of Nigerian cybercriminals based on online banking and to know the way to use ICT tools to prevent these crimes.

Jegede (2018), examined the issue of survival in the dynamic environment of Nigeria. The study made use of a survey method for data collection using a structured questionnaire. The analysis was done using the Mean Maximum Correlation Vector (MMCV) algorithm/model developed by the researcher. It also made use of the r-factor and r2 –factor, the t-distribution. The study revealed that the innovative ability is a sine-qua-non for the survival of the entrepreneur and growth of the small business to a large business. It also revealed that a pecking order import and value exist for the characteristics needed by the would-be entrepreneur. It also noted that while finance is of value the possession of entrepreneurial spirit is more of import for the survival and growth of small business in a very dynamic environment like that of Nigeria. The study recommended that policymakers should develop training not only for skill acquisition but one that will target innovative ability formation and entrepreneurial spirit acquisition. However, there is no direct empirical study on cybercrime and SMEs especially in the FCT this shows that this study is significant.

Theoretical Framework

The study adopted the institutional anomie theory (IAT) as the theoretical framework and the theory was developed by Steven Messner and Richard Rosenfeld in 1994. The features of institutional anomie theory hypothesized that an over-emphasis on economic goals, also with a devaluation of the non-economic institutions in society, results in higher rates of crime and re-offending behavior (Bjerregard and Cochran, 2008). Messner and Rosenfeld (2007) agree that developing countries like Nigeria places an over-emphasis on material and monetary

success. The theory also explained that crime is an indirect consequence of the dominance of the economy over other sectors of society. If a society is primarily shaped by economic interests, economic logic permeates other social institutions and areas (such as education). This results in utilitarian behaviour on the part of members of society, a decline in social control, and an increase in crime. Therefore, this theory agrees that cybercrimes can affect economic activities like small and medium enterprises and this also suggests that there is a functional relationship between cybercrimes and small and medium enterprises activities.

Methodology

Population and Sample Size of the Study

The population of this study is two thousand, eight hundred and twenty-five (2825) Small and Medium Enterprises (SMEs) in Federal Capital Tertiary (FCT) as reported by SMEDAN and NBS Collaborative Selected Survey findings on SMEs and MSMEs in Nigeria (SMEDAN & NBS, 2017). The Yamane formula for calculating the sample size of a finite population shall be used. i.e.

$$n = \frac{N}{1 + N(e)^2}$$

Where, n = Sample Size 0, N = Population, 1 = Constant and e = exponential (usually 5% or 0.05).

$$\therefore n = \frac{2825}{1 + 2825(0.05)^2} = 350$$

Using Taro Yamane's formula, the sample size of this study is approximated to three hundred and fifty (350) respondents which are SMEs owners in Federal Capital Tertiary (FCT).

Validation of Research Instrument

The instrument is said to be valid when it measures what it is intended to be measured (Creswell, 2012). To ensure the face and content validity of the items on the instrument measuring the different variables in the study, the questionnaire will be submitted to two experts in educational research and statistics and one expert in test and measurement, to ascertain whether the items measured what they purported to measure. These experts in conjunction with my supervisor certified the instrument as being valid to measure what it set out to measure at least in content and face validity. During this process, their comments and corrections led to changes being affected on the items in the questionnaire in terms of appropriateness and precision of words, sentences, and expressions. Flaws and errors in terms of phraseology, tautology, grammar, and organization of the instrument were identified and the necessary corrections were affected.

Method of Data Analysis

The study used the mean of descriptive analysis. Thus, responses of each subject were coded on the computer coding sheet, and thereafter, entered and processed, using the Statistical Package for Social Science (SPSS), mean and simple percentages were used for analysis and interpretation of the results. The frequency distributions of the various response categories

were calculated. To obtain the item and section mean ratings, frequencies were weighed in the following manner: strongly agreed - 4 points, agreed - 3 points, disagreed -2 points, and strongly disagreed -1 point. The mean ratings of the various responses were calculated and were used to answer the research questions. The mean of 1, 2, 3, and 4 is 2.50 for this study; a mean rating of 2.51 or above was regarded as significant while a mean rating less than 2.50 was regarded as insignificant in explaining the changes in the variables under study. In the analysis there are four indicators for cybercrime activities related to Small and Medium Enterprises (SMEs) in Federal Capital Tertiary (FCT) and these indicators are Hacking and Spamming cybercrimes (HSC), Cyber Theft and Identity Theft Cybercrimes (CTITC), Financial Fraud and Laundering Cybercrimes (FFLC) and Website Cloning Cybercrimes (WECC).

Data Presentation and Analysis

The results of the data collected are analyzed below based on each research question, out of the 350 questionnaires distributed, 342 questionnaires were well completed and valid for analysis for this study.

Table 1: Percentages of Sex, Age and year of Experience of respondents

Sex distribution of respondents	**Frequency**	**Percentage %**
Male	198	58
Female	144	42
Total	**342**	**100**
Age distribution of respondents	**Frequency**	**Percentage %**
10-25	41	12
26-40	106	31
41-60	130	38
61-above	65	19
Total	**342**	**100**
Years of Experience of respondents	**Frequency**	**Percentage**
1-10	58	17
11-20	103	30
21-30	133	39
31-above	48	14
Total	**342**	**100**

Source: Administered Questionnaires, 2020.

Tables 1 shows that58 percent of the total respondents are males, while 42 percent of the total respondents are females. The result implies that males are in self-employment jobs than females. Also, Table 1 shows that12 percent of the total respondents are between the age brackets of 10-25, 31 percent of the total respondents are between the age brackets of 26-40, 38 percent of the total respondents are between the age brackets of 41-60, while 19 percent of the total respondents are between the age brackets of 61-above. Furthermore, 17 percent of the total respondents are between 1-10 years of experience, 30 percent of the total respondents are between 11-20 years of working experience, 39 percent of the total respondents are between 21-30 years of working, 14 percent of the total respondents are between 31-above years of working experience. The results show clearly that a larger percent of the respondents is experienced in their various fields of business.

Table 2: Percentages of forms of business, capital base, sources of capital, the model of production, and number of employees in the SMEs organization

Businesses of SMEs	**Frequency**	**Percentage**
Services and Manufacturing	109	32
Power and Energy	82	24
Construction and Mining	89	26
Others	62	18
Total	**342**	**100**
The capital base of business organizations in Naira	**Frequency**	**Percentage**
4,999,999-Less	44	11
5,000,000-9,999,999	96	28
10,000,000-14,999,999	86	25
15,000,000-Above	123	36
Total	**342**	**100**
Sources of initial business finance	**Frequency**	**Percentage**
Personal savings	157	46
Family and friends	58	17
Cooperative societies	72	21
Banks	55	16
Total	**342**	**100**
Number of employees under each organization	**Frequency**	**Percentage**
1-10	116	34
11-20	92	27
21-30	75	22
31-above	58	17
Total	**342**	**100**

Source: Administered Questionnaires, 2020.

Table 2 shows that 32 percent of the total respondents are into services and manufacturing activities, 24 percent are into power and energy activities, 26 percent are into construction and mining and 18 percent of the total respondents are into other businesses. Also, 11 percent of total respondents have ₦4,999,999and less as their business capital base, 28 percent have ₦500,000,000-₦9,999,999 as their business capital base, 25 percent have ₦10,000,000-₦14,999,999 as their business capital base, while 36 percent of the total respondents have ₦15,000,000-above as their business capital base.

More so,46 percent of the total respondents have personal savings as their source of initial business finance, 17 percent have family and friends as their initial business finance, 21 percent have cooperative societies as their source of initial business finance, and 16 percent have banks as their source of initial business finance. Finally, 34 percent of the total respondents have 1-10 employees under their organizations, 27 percent have 11-20 employees in their organizations, 22 percent have 21-30 employees in their organizations, 17 percent of the total respondents have a 31-above employee in their organizations.

Table 3: Frequencies and percentages of SMEs activities and Cybercrimes in the FCT

SMEs are faced with various forms of cybercrimes in FCT	**Frequency**	**Percentage**
Agreed	233	68
Disagreed	62	18
Undecided	48	14
Total	**342**	**100**
There are high levels of SMEs cybercrimes in FCT	**Frequency**	**Percentage**
Agreed	216	63
Disagreed	82	24
Undecided	44	13
Total	**342**	**100**
Which of the following is the most common of SMEs cybercrime in FCT?	**Frequency**	**Percentage**
Hacking and Spamming	55	16
Cyber Theft and Identity Theft	109	32
Financial Fraud and Laundering	130	38
Website Cloning	48	14
Total	**342**	**100**
SMEs have the required capacity and information to overcome SMEs related cybercrimes	**Frequency**	**Percentage**
Agreed	82	24
Disagreed	216	63
Undecided	44	13
Total	**342**	**100**
The SMEs cybercrimes can be reduced and prevented if all the related agencies are optimum in delivering their functions	**Frequency**	**Percentage**
Agreed	198	58
Disagreed	82	24
Undecided	44	13
Total	**342**	**100**

Source: Administered Questionnaires, 2020.

Table 3 shows that 68 percent of the total respondents agreed that SMEs are faced with various forms of cybercrimes in FCT, 18 percent of the total respondents disagreed that SMEs are faced with various forms of cybercrimes in FCT and 14 percent of the total respondents are undecided. Also, 63 percent of the total respondents agreed that there are high levels of SMEs cybercrimes in FCT,24 percent of the total respondents disagreed that there are high levels of SMEs cybercrimes in FCT and 13 percent of the total respondents are undecided.

More so, 16 percent of the total respondents believed that Hacking and Spamming are the most common cybercrimes of small and medium enterprises in Federal Capital Tertiary (FCT), 32 percent of the total respondents believed that cyber theft and identity theft are the most common cybercrimes of small and medium enterprises in Federal Capital Tertiary (FCT), 38 percent of the total respondents believed that financial fraud and laundering are the most common cybercrimes of small and medium enterprises in Federal Capital Tertiary (FCT) and 14percent of the total respondents believed that website cloning is the most common cybercrime of small and medium enterprises in Federal Capital Tertiary (FCT).

Besides Table 3 shows that 24 percent of the total respondents agreed that SMEs have the required capacity and information to overcome SMEs related cybercrimes in FCT, 63 percent of the total respondents disagreed that SMEs have the required capacity and information to overcome SMEs related cybercrimes in FCT and 13percent of the total respondents are undecided. Finally, 58 percent of the total respondents agreed that SMEs cybercrimes can be reduced and prevented if all the related agencies are optimum in delivering their functions, 24 percent of the total respondents disagreed that SMEs cybercrimes can be reduced and prevented if all the related agencies are optimum in delivering their functions and 13 percent of the total respondents are undecided.

Table 4: Percentage of Cybercrime indicators and their impact on SMEs

Hacking and Spamming have a negative impact on SMEs activities in FCT	**Frequency**	**Percentage %**
Strongly agreed	116	34
Agreed	130	38
Disagreed	51	15
Strongly disagreed	45	13
Total	**342**	**100**
Cyber Theft and Identity Theft have a negative impact on SMEs activities in FCT	**Frequency**	**Percentage %**
Strongly agreed	109	32
Agreed	130	38
Disagreed	55	16
Strongly disagreed	48	14
Total	**342**	**100**
Financial Fraud and Laundering have a negative impact on SMEs activities in FCT	**Frequency**	**Percentage %**
Strongly agreed	147	43
Agreed	96	28
Disagreed	51	15
Strongly disagreed	48	14
Total	**342**	**100**
Website Cloning has a negative impact on SMEs activities in FCT	**Frequency**	**Percentage %**
Strongly agreed	130	38
Agreed	113	33
Disagreed	48	14
Strongly disagreed	51	15
Total	**342**	**100**

Source: Administered Questionnaires, 2020.

Table 5 shows that 34 percent of the total respondents strongly agreed that hacking and spamming have a negative impact on SMEs activities in Federal Capital Tertiary (FCT), 38 percent of the total respondents agreed that hacking and spamming have a negative impact on SMEs activities in Federal Capital Tertiary (FCT), 15 percent of the total respondents disagreed to the fact that hacking and spamming have a negative impact on SMEs activities in

Federal Capital Tertiary (FCT) and 13 percent of the total respondents strongly disagreed to the fact that hacking and spamming have a negative impact on SMEs activities in Federal Capital Tertiary (FCT). Also, 32 percent of the total respondents strongly agreed that cyber theft and identity theft have a negative impact on SMEs activities in Federal Capital Tertiary (FCT), 38 percent of the total respondents agreed that cyber theft and identity theft have a negative impact on SMEs activities in Federal Capital Tertiary (FCT), 16 percent of the total respondents disagreed to the fact that cyber theft and identity theft have a negative impact on SMEs activities in Federal Capital Tertiary (FCT) and 14 percent of the total respondents strongly disagreed to the fact that cyber theft and identity theft have a negative impact on SMEs activities in Federal Capital Tertiary (FCT).

In addition, 43 percent of the total respondents strongly agreed that financial fraud and laundering have a negative impact on SMEs activities in Federal Capital Tertiary (FCT), 38 percent of the total respondents agreed that financial fraud and laundering have a negative impact on SMEs activities in Federal Capital Tertiary (FCT), 15 percent of the total respondents disagreed to the fact that financial fraud and laundering have a negative impact on SMEs activities in Federal Capital Tertiary (FCT) and 13 percent of the total respondents strongly disagreed to the fact that financial fraud and laundering have a negative impact on SMEs activities in Federal Capital Tertiary (FCT). Finally, 38 percent of the total respondents strongly agreed that website cloning has a negative impact on SMEs activities in Federal Capital Tertiary (FCT), 33 percent of the total respondents agreed that website cloning has a negative impact on SMEs activities in Federal Capital Tertiary (FCT), 14 percent of the total respondents disagreed to the fact that website cloning has a negative impact on SMEs activities in Federal Capital Tertiary (FCT) and 15 percent of the total respondents strongly disagreed to the fact that website cloning has a negative impact on SMEs activities in Federal Capital Tertiary (FCT).

Table 5: Descriptive Statistics

Descriptive Statistics					
	N	**Minimum**	**Maximum**	**Mean**	**Std. Deviation**
HSC	341	1.00	4.00	2.9355	1.00085
CTITC	341	1.00	4.00	2.8827	1.01069
FFLC	341	1.00	4.00	3.0117	1.05434
WECC	341	1.00	4.00	2.9267	1.07535

Note: *The mean of 1, 2, 3 and 4 is 2.50 for this study; a mean rating of 2.51 or above was regarded as a positive impact while a mean rating of 2.50 and less was regarded as no impact in explaining the changes in the variables under study.*

Source: SSPS Computation, 2020

Table 5 shows the impact of cybercrime indicators on Small and Medium Enterprises (SMEs) in Federal Capital Tertiary (FCT). Table 5 revealed that the calculated mean statistic is 2.94 which means that hacking and spamming cybercrimes (HSC) have a negative impact on Small and Medium Enterprises (SMEs) activities in Federal Capital Tertiary (FCT). Since the calculated mean is greater than 2.50, the alternative i.e., **H_1 is accepted** meaning that hacking

and spamming cybercrimes have a negative impact on Small and Medium Enterprises (SMEs) activities in Federal Capital Tertiary (FCT)and while the H_0 is rejected meaning that cybercrimes have no negative impact on Small and Medium Enterprises (SMEs) activities in Federal Capital Tertiary (FCT).

Also, the calculated mean statistic is 2.88 which means that cyber theft and identity theft cybercrimes (CTITC) have a negative impact on Small and Medium Enterprises (SMEs) activities in Federal Capital Tertiary (FCT). Since the calculated mean is greater than 2.50, the alternative i.e., H_1 is accepted meaning that cyber theft and identity theft cybercrimes have a negative impact on Small and Medium Enterprises (SMEs) activities in Federal Capital Tertiary (FCT)and while the H_0 is rejected meaning that cyber theft and identity theft cybercrimes have no negative impact on Small and Medium Enterprises (SMEs) activities in Federal Capital Tertiary (FCT).

More so, the calculated mean statistic is 3.01 which means that financial fraud and laundering cybercrimes (FFLC) have a negative impact on Small and Medium Enterprises (SMEs) activities in Federal Capital Tertiary (FCT). Since the calculated mean is greater than 2.50, the alternative i.e.H_1 is accepted meaning that financial fraud and laundering cybercrimes have a negative impact on Small and Medium Enterprises (SMEs) activities in Federal Capital Tertiary (FCT) and while the H_0 is rejected meaning that financial fraud and laundering cybercrimes have no negative impact on Small and Medium Enterprises (SMEs) activities in Federal Capital Tertiary (FCT).

Finally, the calculated mean statistic is 2.93 which means that website cloning cybercrimes (WECC) have a negative impact on Small and Medium Enterprises (SMEs) activities in Federal Capital Tertiary (FCT). Since the calculated mean is greater than 2.50, the alternative i.e.H_1 is accepted meaning that website cloning cybercrimes (WECC) have a negative impact on Small and Medium Enterprises (SMEs) activities in Federal Capital Tertiary (FCT)and while the H_0 is rejected meaning that website cloning cybercrimes (WECC) have no negative impact on Small and Medium Enterprises (SMEs) activities in Federal Capital Tertiary (FCT).

Conclusion and Recommendations

In conclusion, the study revealed that hacking and spamming cybercrimes (HSC), cyber theft and identity theft cybercrimes (CTITC), financial fraud and laundering cybercrimes (FFLC) and website cloning cybercrimes (WECC) have a negative impact on Small and Medium Enterprises (SMEs) activities in Federal Capital Tertiary (FCT). Therefore, the study recommended the following based on the findings.

i. Government and all concerned agencies should design measures in controlling and preventing hacking, spamming, financial fraud, and laundering cybercrimes since these are the major cybercrimes affecting SME activities.
ii. There need for increased literacy for SMEs to mitigate against hacking, spamming, financial fraud, laundering, and website cloning.

References

Akingunola, R. O. (2011). Small and medium scale enterprises and economic growth in Nigeria: An assessment of financing options, *Pakistan Journal of Business and Economic Review*, 2 (1).

Asokhia, M. O. (2010). Enhancing national development and growth through combating cybercrime/internet fraud: A comparative approach, *Journal of Social Sciences*, 23 (1), 13-19.

Bjerregard, B., & Cochran, J. K. (2008). A cross-national test of institutional anomie theory, *Western Criminology Review*, 9 (1), 31-48.

Brenner, S. (2007). *Law in an era of smart technology*, Oxford: Oxford University Press, 374.

Fadare, O. A., (2015). Impact of ICT tools for combating cyber crime in Nigeria online banking: A conceptual review, *International Journal of Trade, Economics, and Finance*, 6 (5),272-277

Frank, M. A., Bassey, E. A. & Ironbar, V. E (2018). Accessibility of credit facilities by farmers and rural Industrialization in cross river state. *Social Sciences Journal of policy review & development strategies, 5* (1), 75-84

Jegede, C. A., (2018). Empirical analysis of survival and growth of small and medium scale business in developing economy: The case of Nigeria, *Sumerianz Journal of Business Management and Marketing*, 1(1), 26-32

Jegede, A. E., & Olowookere, I. E. (2014) Cyber risks and fraud in Nigeria's business environment: A postmortem of youth crime, *Journal of Social and Development Sciences*, 5(4), 258-265

Messner, S. F., & Rosenfeld. R. (2007). *Crime and the American drea*m, Belmont, CA: Wadsworth.

Odumesi, J. O. (2014). A socio-technological analysis of cybercrime and cyber security in Nigeria, *International Journal of Sociology and Anthropology,* 6 (3), 116-125.

Schell, B. H., & Clemens, M., (2004). *Cybercrime: A reference handbook*, ABC- CLIO.

Sesan, G. (2010). *The new security war*, [Online]. Available: http://www.pcworld.com/article/122492/the_new_security_war.htm# tk.mod-rel

Wazir, F. (2009). Antigraft campaign: The war the worries, *The Punch, 1st March 2009*, p.1.

Milhorn, H. (2007). *Cybercrime: How to avoid becoming a victim by true crime, 2007*,