Abu, S. O.; Lateef, O. M.; Echobu, J.

Article

Determinants of cyber fraud investigation in Nigeria

Reference: Abu, S. O./Lateef, O. M. et. al. (2018). Determinants of cyber fraud investigation in Nigeria. In: Accounting and taxation review 2 (2), S. 1 - 14.

ISSN: 2635-2966 (Print), ISSN: 2635-2958 (Online).

Available online at http://www.atreview.org

Original Research Article

Determinants of Cyber Fraud Investigation in Nigeria

S. O. Abu[1], O. M. Lateef[2], & J. Echobu[3]

[1,3] Department of Accounting, Faculty of Management Sciences, Federal University Dutsinma, Katsina State, Nigeria

[2] Department of Accounting and Management, Nigeria Defence Academy (NDA) Kaduna.

*For correspondence, email: seiniabu@yahoo.com

Received: 03/04/2018 Accepted: 25/05/2018

Abstract

This paper examines the determinants of cyber fraud investigation in Nigeria. The use of computer and internet technology in recent times has evolved electronic financial transactions such as e-business, e-commerce, e-payment has resulted to unlawful activities as miscreants use the same application to perpetrate fraudulent acts. This has endangered the businesses of the individuals, groups, institutions and even governments as huge amount of money is lost to these fraudsters. 150 respondents form the sample population drown from three agencies (EFCC, ICPC and Nigeria Police) using primary data only. The sample size was derived using Yamane (1967) statistical formula. The sample size consists of one hundred and nine (109) questionnaire, out of which, one hundred and five (105) were filled and return. Analysis of variance (ANOVA) was used to test the hypotheses. The findings of the study show that there is positive and significant relationship between cyber fraud investigation and computer forensic education, digital forensic education, law enforcement education and seminar, workshop and conferences. Similarly, there is insignificant association between cyber fraud investigation and accounting education. Therefore, the study recommended among others that the personnel of these agencies need to have adequate knowledge of computer forensic education and should be allowed to attend seminars, workshop and conferences in order to update their knowledge, skills and competence to overcome the challenge posed on the agencies.

Keywords: computer forensic education, digital forensic education, accounting education, law enforcement education, and seminar, conference and workshop.

JEL Classification Codes: *M41 M48*

1.0 INTRODUCTION

The introduction of computer and internet into financial transaction facilitates the speedy growth and development of business transaction globally. This is because computer and internet can rapidly change the world of commerce and banking leading to economic development of any nation, both at national and international level. Specifically, internet can make business grow faster and more efficient as it allows people to provide more personalised services to the user or customer. This however, makes it possible for financial services providers to have develop new strategies of adding value and distinguish themselves from the former way of commoditised financial transactions. The use of computers also has assisted many organizations for keeping the records of their customers. Both financial and non-financial organisations, particularly banks are using computers for maintaining accounts and managing financial transactions. It helps the banks in providing online facility to enable the customers to check their account balance through the use of internet. Many organizations through computer and internet can make financial transaction online very easily and quickly with computerised systems as it facilitates payment of bills, making withdrawal without going through long queue at bank's counter, managing their home budgets and other financial transactions.

In spite of these numerous advantages of the use of computer and internet on financial transactions, it has posed danger to businesses, individuals, groups, institutions and states as criminals use the computer for negative activities. The use of computers and internet has created increasing opportunities for the commission of crimes as information technology has enabled potential offenders to commit all sorts of crimes with almost no monetary cost and much lesser risk of being caught (Wang & Huang, 2011). Criminals hack the credit card numbers of people and misuse them or they can steal important data from large organisations. This is possible as the Net allows financial organisation to combine content from multiple service onto one computer desktop. These has resulted into high risks on information system security on the part of customers and organizations as it has cause a counterbalanced at least in part by offered opportunities to criminals in carrying out their nefarious activities such as stealing, cheating, defrauding, hacking and misleading for personal benefits.

Furthermore, Internet connected activities are as vulnerable to fraud and can lead to victimisation as effective as common physical frauds. The types of frauds that are currently occurring have existed long before the Internet was around. However, by virtue of the tools being used today to commit cyber frauds, criminals are now more anonymous and provided with a virtual market of available victims. The responsibility falls on individuals to protect themselves, their families and the law enforcement agencies to track them and punish them accordingly (Bureau of Justice Assistance, 2012). Cyber fraud is any criminal activity involving computers and networks of deliberate deception for unfair or unlawful gain that occur online. According to Singleton and Singleton (2010:40), it takes the forms of trick, cunning, deceit and unfair means by which another is cheated. It also incorporates any information downloaded illegally such as document files or bank account to stealing millions of Naira using online (Ebenezer, 2014). The most common forms of cyber fraud are online credit card theft, non-delivery of paid products purchased online and non-delivery of merchandised or software bought online (BJA, 2012). On the other hand, an internet fraud is the use of internet services or software with internet access to defraud victims or to otherwise take advantage of the victims, particularly to stealing personal information which can

even lead to identity theft. Internet services can also be used to present fraudulent solicitations to prospective victims in order to conduct fraudulent transaction or to transfer the proceeds of illegally acquired wealth to financial institutions or to others connected with the scheme.

Generally, Cyber fraud are the work of skilled technicians who apply the knowledge of information and communication technology (ICT) through computer and internet for criminal activity (Broadhurst, Grabosky, Alazab & Chon, 2014). This means it is the handwork of those who are believed to be terrestrial or conventional fraudsters who metamorphosed into harness digital technology in furtherance of criminal objectives. It can be committed by individual, groups, organisations and state. This to a great extent poses challenges to the law enforcement agencies in terms of investigation and prosecution. Cyber criminals around the world hook on the Net to penetrate into the financial transactions of businesses to the detriment of their customers, and this poses danger on the investment or wealth of individual, group, institution and economy of a nation as a whole. Consequently, cyber fraud also involves the use of computer and internet facility and as such, the law enforcement agencies in dealing with these types of criminal cases need to have the basic knowledge of computer forensics education, digital forensics education, digital investigation education, accounting education and law enforcement knowledge (Kessler & Schirling, 2006). The underlying goals of having the basics knowledge of all these types of disciplines according to Kessler and Schirling (2006) is to make an investigator a multi-disciplinary professional, bringing together the accounting aspect, law, computer technology and the basics of digital investigation which would equip them with the knowledge of all forms of cyber-crime and the way to handle it. Similarly, for investigator to update his/her knowledge, they need to work closely with the practitioners and academia through an organise workshops, seminars, conferences and other forms of programme in order to bridge the gap. The simple reason for this is that you cannot give what you don't have. The investigator needs to acquire all the necessary skills, knowledge and abilities to qualify him/herself as expert. Therefore, he/she need to study like criminal, reason like criminal, behave/act like criminal and think like criminal in order to overcome the action, tactics, behaviour and technicality of criminal during the course of investigation.

More so, using the Kessler and Schirling (2006) program guidelines or idea in dealing with any financial matter related to cyber fraud, it therefore, requires all investigators in Nigeria to have at least diploma certificate in these five discipline in addition to the certificates of their entry, if they are from different field of study, otherwise, they should be graduate in the fields of computer forensic science, digital forensic science and digital investigation education. In addition, they should also ensure to attend workshops, seminars, conference and other programme organise by practitioners and academia in order to update their knowledge. This would equip them to live above board in all fraud related cases, being it cyber or not. Therefore, the study examine the three agencies (EFCC, ICPC and Anti-Fraud section of Nigeria Police Force) in Nigeria who are charged with the responsibility of investigating and prosecuting all forms of frauds including cyber fraud to determine whether they have the requisite knowledge and skills as prescribed by Kessler and Schirling (2006) in order to overcome the challenges posed to individual, group, institution and government by cyber fraudster in Nigeria.

The recent increase of financial crimes both national and international community using information and communication technology (ICT) facilities such as computers and

internet in the perpetration of criminal activities like credit card frauds, ATM frauds, phishing, identity theft, spamming and a host of other crimes has attributed to the view that ICT is contributing to all forms of cyber fraud in both financial and non-financial sector of the Nigerian economy. This has challenged the intelligence, competence, knowledge, skills and abilities of the law enforcement agencies in Nigeria.

Today, cyber fraudsters can transmit a fraud related information using electronic gadgets from one person to another, each improving or adapting it to his or her own needs and this becomes the perfect fraud business with no evidence and no basis for the victim and perpetrator to identify or confront each other (Curtis & Colwell, 2000). To worsen the situation, law enforcement agencies, particularly, the police force would not know the cyber fraud method used and when and where it was done, it would happen before both the victim and the police could aware. This means that the law enforcement agencies must become much more computer literate just to be able to keep up with the criminal element. More so, the police force, particularly the anti-fraud section of the police and other law enforcement agencies have fallen behind in the computer age and must overcome a steep learning curve as these types of crime is sometimes difficult for police and other law enforcement agencies to comprehend due to its complexity. Therefore, this study investigate the knowledge, skills and abilities of the law enforcement agencies in Nigeria to curb the menace of cyber fraud that perpetrate in the country.

The main objective of this study is to examine the determinants of cyber fraud investigation by law enforcement agencies in Nigeria. However, it is set to achieve the following objectives:

To determine the impact of computer forensic knowledge on cyber fraud investigation in Nigeria; evaluate the influence of digital forensic knowledge on cyber fraud investigation in Nigeria; investigate the impact of accounting knowledge on cyber fraud investigation in Nigeria; examine the influence of law enforcement education on cyber fraud investigation in Nigeria; evaluate the impact of workshop, seminar and conference on cyber fraud investigation in Nigeria. In line with the objectives of this study, the following hypotheses have been formulated in null form: Computer forensic knowledge has no significant impact on the cyber fraud investigation in Nigeria. Digital forensic knowledge has no significant influence on the cyber fraud investigation in Nigeria. Accounting knowledge has no significant impact on the cyber fraud investigation in Nigeria. Law enforcement education has no significant influence on the cyber fraud investigation in Nigeria. Attending workshops, seminars and conferences have no significant impact on cyber fraud investigation in Nigeria

2.0 LITERATURE REVIEW

Cyber fraud is any type of fraud that involves the use of computers and network, where the computers facility may or may not have played an instrumental part in the commission of the fraud (Luminita, Viorica & Adrian, 2011). This means that the cyber fraudster knowing full well that it might be difficult for the law enforcement agents during the course of investigation to come up with an evidence linking a particular computer or instrumental part or network facility used by them in perpetrating the crime. Clough (2010) document that the idea of cyber fraud emanated from the knowledge of computer as people discovered that computers and internet became the mainstream of business transactions globally. This is because the application of computers and internet has promoted the business activities tremendously, particularly, in the areas of procurement, shopping, business collaboration, customer services,

recruitments, revenue generation, cost reduction etc. These has helped in transforming the business transactions in a wide range in this 21st century in both national and international community. However, these applications (computers and internet) instead of utilizing them for improving business transactions in Nigeria, skilled technologists, computer and Network service provider and other computer technologists in Nigeria used the opportunity for criminal benefits (Folashade & Abimbola, 2013).

In view of the above aforementioned value in the use of computers and internet, it is presumed that the computers and internet usage in Nigeria for business transactions is intensifying due to enlargement availability of Net transferring data fast linking all business functional areas and their important tasks to one another across the globe thereby making all forms of services available for customer consumption (Olasanmi, 2010). This perceived intense of computer and internet usage in Nigeria for business transactions has made the computer and internet a favourite means of passing business and other information as well as communication or collaboration between business world and customers which in turn become a meeting point for internet discussion. This internet meeting point assists in all forms of internet transactions, such as e-banking, e-payment, e-commerce and host of other transactions using internet (Ehimen & Bola, 2009). More so, the use of the computer and internet in the business industry or banking sector helps in providing a variety of services, such as internet service provision (ISP), or institution like T.Com or CARNet; AT & T ; FTP and cyber cafes which facilitates the speedy of all forms of e-transactions but now turned to be a cobweb that attracted all types of unlawful businesses like credit card, ATM frauds, phishing, identity theft, spamming, stealing, and a host of other crimes in Nigeria (Ayantokun, 2006).

The development of computer and internet services has brought in happiness and curses to individual, group and institutions in Nigeria. According to Curtis (2000), the use of computer and internet has simplified the ability of the individual, group and institution to communicate and attract business information that speed up the inflow of e-transactions worldwide. This implies that computer and internet services facilitates the dissemination of business information to the interested party (ies) at any particular point in time, whether at home, office or anywhere they are. Similarly, it also brought in curses as it enables the miscreants to use the same application for fraudulent activities for personal benefits (Curtis, 2000). This is because the criminals were the first to acquire the knowledge and skills long before any other persons including the law enforcement agencies, and as such they became expert in the field which they utilize the opportunity for unlawful benefits.

McConnel (2000 in Folashade & Abimbola, 2013) argue that cyber fraud differ from other forms of crimes in four different ways. This is because they are: simple to learn and understand; require little resources to support the talent to caused damage or destruction; the offence can be committed in an environment or area without the physical appearance of the criminal; and the legality of the case may be difficult to prove. This in turn become challenging to the law enforcement agencies to investigate and prosecute the culprit at the law court. The simple reason for this is due to the fact that the law enforcement agencies are not well grounded with the application of computer, digital and forensic investigation in handling internet fraud related cases (Mohammed, Hamza & Mahmoud, 2013). The investigator in cyber fraud must be well trained and should be expert in forensic science and computer application in order to identifying, collecting, documenting, preserving, analyzing, examining and presenting evidence from computer devices,

networks, and other electronic devices at the law court (Mohammed et al., 2013).

According to David and Karl (1995), computer and internet fraud come in different forms and are complex due to various types of electronic transactions which make the investigation process cumbersome for forensic and digital investigators to trace, detect and prevent the occurrence of the crime. These different forms of cyber frauds pose challenges to the law enforcement agents, particularly, police organization and other agents charged with the responsibility to investigate and prosecute the perpetrate of this crime. The implication of the different forms or types of electronic transactions, such as e-commerce, e-payment, e- business, e-service etc. Each form of these e-transactions has a peculiar crime and investigator need to understand its application. This means for investigators to overcome the challenge of cyber fraud, they need to have an idea or knowledge of computer forensic science, digital forensic science and digital investigation education through formal education. If the investigator is a graduate of any of these disciplines, such investigator needs to have diploma in accounting or finance and law in addition as a backup. But if the investigator is a graduate from a different field, he/she equally needs to have a diploma in computer forensic education, digital forensic science or digital investigation education in order to overcome the technicality of cyber fraud investigation.

Numerous studies that examines the determinants of cyber fraud investigation provide mixed results. Mohammed et al. (2013) examine the challenges of computer crime investigation in North Africa's countries, such as Libya, Tunis, Algeria and Morocco in the year 2011-2012 using library style approach of methodology. The findings of the study show that cybercrime investigation can assists in detecting and preventing unauthorized access to any digital source of information with intent of modifying, destroying or stealing the digital data or information since the actions of the fraudster can cause financial damages or important information loss. The study also find that lack of adequate legislation, nonchalant attitudes from both private and public sector, poor investigative procedures and lack of dedication to work among others which hamper the prosecution of the offenders.

Brown (2015) examines the systemic impediments which obstruct police investigations, prosecutions, and digital forensic interrogations in Australia in the year 2013. The study utilize library style approach of research methodology and personal experience as a retired police officer. The study find that existing academic research on cyber fraud investigation only highlight the theoretical perspectives in explaining the technology aided crime but do not present practical insights from actually tasked with working cyber fraud cases. The study also encourages policy makers to reevaluate strategies for combating all forms of cybercrimes that posed threat by cyber fraudsters. This implies that investigating and prosecuting cybercrimes, being it fraud or otherwise has been proving difficult to law enforcement agents since there is no lay down rules and regulations, penal code or criminal procedure to accommodate or handling e-transaction cases which would be used to punish the offender of e-transaction cases.

3.0 METHODOLOGY

The study adopts a descriptive survey approach. This enabled us to have a systematic and descriptive approach of the study area. The primary sources of data collection was utilize through the administration of questionnaires. The questionnaire was closed ended with agreed, strongly agreed, disagreed, strongly disagreed and undecided responses. The study covers the three agencies (EFCC, ICPC and Anti-fraud unit of Nigeria Police)

in Nigeria who are charged with the responsibility of investigating and prosecuting all forms of fraud cases including that of cyber fraud. From these a clear and precise population of one hundred and fifty (150) personnel from these three agencies.

The study derived its sample size statistically using Yamane (1967 as cited in Adebisi & Gbegi, 2013) as shown below:

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

Where n = Sample size
N = Population
e = Level of Significance (0.05)

$$n = \frac{150}{1+150(0.05)^2}$$

$$n = \frac{150}{1+150\ (0.0025)}$$

$$n = \frac{150}{1+0.375}$$

$$n = \frac{150}{1.375}$$

$$n = 109.091$$

Therefore, the sample size consists of one hundred and nine (109) respondents from these agencies.

Data collected were systematically arranged and presented in the table using simple percentage. In addition, the data were further classified into Agreed and Disagreed and are dichotomize as one (1) or zero (0), if the percentage of the responses on any question is fifty (50) percentage and above (1) or otherwise zero (0) (Adeniyi & Mieseigha, 2013). The hypotheses were tested used analysis of variance (ANOVA) to determine the relationship between the cyber fraud investigation and the knowledge of computer forensic science, digital forensic science, accounting education, law enforcement education and seminars, conferences and workshops.

In order to determine the relationship between cyber fraud investigation and the knowledge of computer forensic education, digital forensic education, accounting education, law enforcement education and seminar, workshop and conferences, the analysis of variance (ANOVA) model used by Adebisi and Gbegi (2013) is adopted with modification as thus:

CFE	=	SSB	=	$r \Sigma (xij - x)^2$	and	SSW	= $\Sigma\Sigma (xij - x)^2$—
DFI	=	SSB	=	$r \Sigma (xij - x)^2$	and	SSW	= $\Sigma\Sigma (xij - x)^2$—
ACE	=	SSB	=	$r \Sigma (xij - x)^2$	and	SSW	= $\Sigma\Sigma (xij - x)^2$—
LEE	=	SSB	=	$r \Sigma (xij - x)^2$	and	SSW	= $\Sigma\Sigma (xij - x)^2$—
SCW	=	SSB	=	$r \Sigma (xij - x)^2$	and	SSW	= $\Sigma\Sigma (xij - x)^2$—

Where:

CFS	=	Computer Forensic Science
DFI	=	Digital Forensic Investigation
ACK	=	Accounting Computer Knowledge
LEE	=	Law enforcement Education
SCW	=	Seminars, Conferences and Workshops
SBB	=	Between Treatment Sum of Square
SSW	=	Within treatment Sum of the Square
Xij	=	Individual Observation around their Column Mean
Ẍ	=	Ground mean column
DF	=	Degree of Freedom (c - 1) (n - 1)
C	=	Number of column
N	=	Number of Observation
R	=	Number of Row
Σ	=	Summation

Level of Significance (0.05)

4.0 RESULTS AND DISCUSSION

Data presented in this study are those collected from the field in the course of this work. This will form the basis for testing and analyzing the research hypotheses. One hundred and nine (109) copies of questionnaire were administered, out of which, one hundred and five (105) representing 100% were filled and returned.

Table 1: The application of computer forensic science enhances the skills, ability and intelligence of the investigator of all fraud related cases.

Options	Frequency	Percentage (%)
Agree	40	38.10%
Strongly Agree	61	58.10%
Disagree	2	1.90%
Strongly Disagree	1	0.95%
Undecided	1	0.95%
Total	105	100%

Table 1 above shows that 61 respondents representing 58.10% of the total respondents strongly agree that the application of computer forensic education enhances the skills, ability and intelligence of the investigator in all fraud related cases. Similarly, 40 respondents representing 38.10% of the total respondents agree with the above view, while 2 respondents representing 1.90% of the total respondents disagree with the above statement. However, 1 respondent representing 0.95% of the total respondents strongly disagree with the above view and 1 respondent representing 0.95% of the total respondents is undecided.

Table 2: The application of digital forensic science helps the investigators to combat all cyber fraud and other cyber crime related cases in Nigeria.

Options	Frequency	Percentage (%)
Agree	48	45.72%
Strongly Agree	50	47.62%
Disagree	5	4.76%
Strongly Disagree	1	0.95%
Undecided	1	0.95%
Total	105	100%

From the above table, 50 respondent representing 47.62% of the total respondents strongly agree that the application of digital forensic education helps the investigators to combat all cyber fraud and other cyber crime related cases in Nigeria, 48 respondents representing 45.72% of the total respondents agree with the above statement. Consequently, 5 respondents representing 4.76% of the total respondents disagree with the view, 1 respondent representing 0.95% strongly disagree with the above statement, while 1 respondent representing 0.95% of the total respondents is undecided whether the application of digital forensic education assists the investigators in combating cyber fraud and other cyber crime related cases in Nigeria or not.

Table 3: The knowledge acquired from the use of digital investigation education has helps in improving the skills and ability of the investigator to obtain evidences in all cyber crime related cases including cyber fraud in Nigeria.

Options	Frequency	Percentage (%)
Agree	64	60.95%
Strongly Agree	30	28.57%
Disagree	6	5.71%
Strongly Disagree	2	1.90%
Undecided	3	2.87%
Total	105	100%

Table 3 above indicates that 64 respondents representing 60.95% of the total respondents agree that the knowledge acquired through the use of digital investigation education has helps in improving the skills and ability of the investigator in obtaining evidences in all cyber-crime related cases including cyber fraud in Nigeria, 30 respondents representing 28.57% of the total respondents strongly agree with this statement. However, 6 respondents representing 5.71% of the total respondents disagree with the above statement, 2 respondents representing 1.90% of the total respondents strongly disagree with the above view, while 3 respondents representing 2.87% of the total respondents is yet to decide over the statement whether the use of digital investigation education has helped in improving the skills and ability of the investigator to obtain evidence in all cyber-crime related cases including cyber fraud in Nigeria or not.

Table 4: An investigator who does not have a sound knowledge of accounting education will find it difficult to obtain substantial evidence against the fraudster.

Options	Frequency	Percentage (%)
Agree	25	23.81%
Strongly Agree	12	11.43%
Disagree	33	31.43%
Strongly Disagree	19	18.10%
Undecided	16	15.24%
Total	105	100%

From the above table 4, 25 respondents representing 23.81 of the total respondents agree that an investigator without sound knowledge of accounting education will experience difficulty in obtaining substantial evidence against the fraudster, 12 respondents representing 11.43% of the total respondents strongly agree with this view. However, 33 respondents representing 31.43% of the total respondents disagree with this statement, 19 respondents representing 18.10% of the total respondents strongly disagree with the above statement, while 16 respondents representing 15.24% of the total respondents are undecided whether sound knowledge of accounting education helps or not.

Table 5: An investigator who acquires law enforcement education has advantage in terms of obtained evidence, presentation of evidence and prosecution of fraudster than those without law enforcement education.

Options	Frequency	Percentage (%)
Agree	44	41.91%
Strongly Agree	49	46.67%
Disagree	9	8.57%
Strongly Disagree	2	1.90%
Undecided	1	0.95%
Total	105	100%

Table 5 above show 44 respondents representing 41.91% of the total respondents agree that an investigator with law enforcement education will gain advantage in terms of obtaining evidence, presentation of evidence and prosecution of fraudster than those without law enforcement education, 49 respondents representing 46.67% of the total respondents strongly agree with the above statement. Consequently, 9 respondents representing 8.57% of the total respondents disagree with this view, 2 respondents representing 1.90% of the total respondents strongly disagree with the above statement, while 1 respondent representing 0.95% of the total respondents is undecided as per whether the law enforcement education contributing in obtaining evidence, presentation and prosecution or not.

Table 6: Investigators who attend seminars, conferences or workshops seem to be more intelligent and sound in cyber fraud cases as knowledge acquired from the programme has helped in improving their investigation skill.

Options	Frequency	Percentage (%)
Agree	58	55.24%
Strongly Agree	42	40.00%
Disagree	3	2.86%
Strongly Disagree	1	0.95%
Undecided	1	0.95%
Total	105	100%

From table 6 above, 58 respondents representing 55.24% of the total respondents agree that investigators who attend seminars, conferences or workshop stand to gain than those who did not attend these programmes, 42 respondents representing 40% of the total respondents strongly agree with the above statement. Similarly, 3 respondents representing 2.86% of the total respondents disagree with this view, 1 respondent representing 0.95% of the total respondents strongly disagree with the above statement, while 1 respondent representing 0.95% of the total respondents is undecided as per effect of seminars, conferences or workshops on investigator whether positive or negative.

4.1 Test of Hypotheses

Table 7 below is used to test our hypotheses. The rejection of null hypotheses and acceptance of alternative hypotheses is based on the analysis of variance (ANOVA). Also, our decision rule whether to reject or accept any hypotheses depend upon the ANOVA test at 5% in this table 7 below:

ANOVA TEST STATISTICS

		Sum of Squares	Df	Mean Square	F	Sig.
CFS	Between Groups	3.622	1	3.622	128.178	.000
	Within Groups	2.911	103	.028		
	Total	6.533	104			
DFI	Between Groups	3.333	1	3.333	52.691	.000
	Within Groups	6.515	103	.063		
	Total	9.848	104			
ACK	Between Groups	.516	1	.516	2.268	.135
	Within Groups	23.446	103	.228		
	Total	23.962	104			
LEE	Between Groups	3.262	1	3.262	45.614	.000
	Within Groups	7.366	103	.072		
	Total	10.629	104			
SCW	Between Groups	3.772	1	3.772	392.381	.000
	Within Groups	.990	103	.010		
	Total	4.762	104			

Having given a diligent analysis of the responses obtained from the respondents questionnaire administered, the hypotheses formulated were tested. In the course of

testing the hypotheses, SPSS 20 was utilized to perform the statistical analysis of various hypotheses formulated using analysis of variance (ANOVA) with a value of 0.05 (level of significance) that corresponds to 95% confidence level. The acceptance or rejection of these values depend upon the respective values of the significance given in the above output table.

The respective significance values of hypothesis one, two, four and five formulated are all within the decision criterion values except hypothesis three that fall outside the decision criterion value. This implies that all variables related to these hypotheses are well correlated except that of hypothesis three. Therefore, we accept all the alternative hypotheses given in the above test statistical table except hypothesis three which we agree with on its null form. This means Hypothesis1: Computer forensic science has significant impact on the cyber fraud investigation in Nigeria (F.STA 128.178 and SIG. VAL .000). Hypothesis 2: Digital forensic science has significant influence on the cyber fraud investigation in Nigeria (FSTA. 52.691 and SIG. VAL .000). Hypothesis3: Accounting knowledge has no significant impact on the cyber fraud investigation in Nigeria (F. STA. 2.268 and SIG. VAL .135). Hypothesis4: Law enforcement education has significant influence on the cyber fraud investigation in Nigeria (FSTA 45.614). Hypothesis5: Seminars, Conferences and workshops has significant impact on the cyber fraud investigation in Nigeria (FSTA 392.381 and SIG. VAL .000). In line with our hypotheses and analysis, hypothesis 1, 2, 4 and 5, the null hypotheses is rejected while hypothesis 3, the null hypothesis is accepted. This is an indication that for all fraud cases, be it cyber fraud or traditional fraud , the investigator needs to have the knowledge of computer forensic science, digital forensic science, law enforcement education and must attend seminars, conferences and workshops. This will make him/her to live above board in handling cyber fraud crime and all other cyber-crime related cases in Nigeria.

4.2 Discussion

From table 1, the study revealed that the application of computer forensic science enhances the skills, ability and intelligence of the investigator in dealing with cyber fraud and all other cyber-crime cases. This implies that the investigator of cyber fraud needs to be well trained and should be an expert in forensic science and computer application in order to identify, collect, document, preserve, analyze, examine and present evidence from computer devices, networks, and other electronic devices at the law court (Mohammed et al., 2013).

Table 2 revealed that the application of digital forensic science enables the investigators to combat all cyber fraud and other cyber-crime related cases. The use of digital forensic science assists and equips the investigator to be on top of the situation in all cases of cyber-crime particularly, detecting and preventing unauthorized access to any digital source of information with intent to modifying, destroying or stealing (Clough, 2010).

From table 3 above, the study revealed that an investigator of cyber fraud can make meaningful impact in his /her investigation without accounting knowledge. This implies that sound knowledge of accounting education is not a prerequisite to cyber fraud investigation. It means that once the fact in respect of the case is been established, the investigator will succeed or make much impact on his / her investigation with or without knowledge of accounting knowledge.

Table 4 in Anova test statistics also revealed that an investigator with law enforcement education has additional advantage in terms of obtaining evidence, presentation of evidence and prosecution of fraudster than

those without law enforcement education. This is because, the knowledge of law education will assist the investigator to determine the nature of the case, the relevant charges, evidence require to back up the case, previous decided cases related to the case at hand and professional advantage.

Table 5 testified that an investigator who attends seminars, conferences or workshops stand to be skillful and intelligence than those who do not attend these programmes. This is because the knowledge acquired through academic research on cyber fraud investigation will highlight the theoretical perspectives in explaining technology aided crime. This can only be achieved through seminars or conferences, while workshops will present practical insights of the actual tasks, showing the tools, instruments or gadgets used in perpetrating the crime. All these can only be achieved through attending these programmes. The essence of this is to improve the skills, ability and intelligence of the investigators.

5.0 CONCLUSION

The study established that the challenges posed on cyber fraud investigation in Nigeria is due to low knowledge of computer forensic education, digital forensic education, law enforcement education, and seminars, conferences and workshops. Agencies, such as Nigeria police, ICPC and EFCC which are charged with the responsibility of investigating and prosecuting cyber fraudsters and all other cyber culprits have low understanding and knowledge of the tools, instruments, gadgets and facilities used by these fraudsters to perpetrate the crime. This hampers the investigation as well as the prosecution of these criminals at the law court. The study also emphasized on the relationship between cyber fraud investigation and computer forensic education, digital forensic education, law enforcement education, and seminars, conferences and workshops. For an investigator to be in control of cyber fraud investigation, he/she needs the knowledge of all these programmes as stated above.

The Federal Government which established these institutions (Nigeria police, ICPC and EFCC) should come up with policies which will encourage and allow staff of the agencies to attend and participate fully in seminars, conferences or workshops once in every year. The policy should make it compulsory for all investigators irrespective of their ranks or positions occupied to have knowledge of forensic science and be computer literate. This will go a long way to improve their skills, competence, capability and intelligence in handling cyber fraud and all other cyber-crimes in Nigeria. The policy should also encouraged or mandate these institutions not to allow any officer or personnel who has not been called to bar (i.e who is not a lawyer by profession) not to be posted to the court as a prosecutor. This will go a long way to strengthen the prosecution process as the prosecutors will have the knowledge of law enforcement education, whether rules and regulations, penal code or criminal procedure to deal with all cases of e-transactions which might result to cyber fraud.

6.0 RECOMMENDATIONS

In the light of the above, the following recommendations are put forward:

(i) Education is one of the most vital warfare weapon that any nation can use to break through and as such, the Federal Government should initiate policies through Tet fund to organize seminars, conferences or workshops to be attend by the officers or personnel of these institutions from time to time. The emphasis should be on cyber fraud investigation so that all officers and staff particularly those who are working in investigation departments will learn through this programme in order to improve their skills, ability and competence in handling all forms of cyber-crime including cyber fraud.

(ii) The Federal Government should increase the annual budget of these institutions (Nigeria police, ICPC and EFCC) or set aside funds for these institutions and make it mandatory for the management of these institutions to compel all the investigators using the funds for forensic science and computer training in a reputable institution national or international. This will enable them to stand the test of time in order to overcome the challenges posed on them by the fraudsters.

(iii) The institutions (Nigeria police, ICPC and EFCC) should designed a template based on hierarchy, that is, seniority and on rotational bases to nominate all the officers and personnel in the investigation department to attend seminars, conferences or workshops at least once in every year. Similarly, those who are in investigation departments and are without the knowledge of forensic science and computer should equally be nominated to attend the training too. This will contribute in improving their skills and intelligence to combat all forms of cyber-crime.

(iv)The institutions (Nigeria police, ICPC and EFCC) should formulate a policy in order to keep and maintain the officers and personnel trained on this field not to transfer them to any other department, rather they should devise a way of encouraging and motivating them for improvement. This will go a long way to making them experts in areas of cyber fraud investigation.

(v) The Nigeria police should design a policy of working towards professionalism. By so doing, only those policemen who are lawyers should be posted to court as prosecutors and those with diploma in law should be posted as investigators at different departments. This will go a long way in sanitizing the system and strengthening the legal section of the force.

REFERENCES

Adebisi, J. F & Gbegi, D.O (2013). Effect of tax avoidance and tax evasion on personal income tax administration in Nigeria. *American Journal of Humanities and Social Sciences*, 1 (.3),125-134

Adeniyi, S.I & Mieseigha, E. G (2013). Audit tenure: An assessment of its effects on audit quality in Nigeria. *International Journal of Academic Research in Accounting, Finance and Management Sciences*, 3 (3), 275-283

Ayantokun, O. (2006), Fighting Cyber crime in Nigeria: Information-system.www.tribune.com

Broadhurst, R., Grabosky, P., Alazab, M & Chon, S (2014). Organizations and Cyber Crime: An Analysis of the Nature of Groups engaged in Cyber Crime. *International Journal of Cyber Criminology*,8 (1), 1-20

Brown, C .S. D (2015). Investigating and prosecuting cyber crime: Forensic dependencies and barriers to justice. *International Journal of Cyber Criminology*, 9 (1), 55-119

Clough, J.. (2010) Principles of Cybercrime. Cambridge*: Cambridge University Press*.

Curtis, P. A (2000). An overview of the challenges faced by law enforcement while investigating computer Crime. Criminal Justice Institute, school of Law Enforcement Supervision, USA.

Curtis, P.A & Colwell, L (2000). Cyber Crime: The next challenge: An overview of the challenges faced by law enforcement while investigating computer crime in the Year 2000 and beyond. School of Law Enforcement Supervision, USA.

David I. & Karl S.(1995). Computer crime: A crime fighter's Handbook, *OReilly Associates*, Inc, Sebastopol, CA

Ebenezer, J. A (2014). Cyber fraud, global trade and youth crime burden: Nigerian experience. *Afro-Asian Journal of Social Sciences*, 5 (4), 1-21.

Ehimen, O.R. & Bola, A,(2010), Cybercrime in Nigeria. *Business Intelligence Journal*, 3(1), 93-98.

Folashade, B. O & Abimbola, K.A (2013) The nature, causes and consequences of cyber crime in Tertiary Institutions in Zaria- Kaduna State, Nigeria. *American International Journal of Contemporary Research*, 3 (9), 98-114.

Kessler, G. C & Schirling, M. C (2006). The design of an undergraduate degree program in computer and digital forensics. Available through www. gary.kesseler@champain.edu or mschirling@bpdvt.org

Luminita, I., Viorica, M & Adrain, B (2011). Fraud, corruption and cyber-crime in a global digital network. *Economics, Management and Financial Markets*, 6 (2), 373-380

Mohammed, S., Hamza, A & Mahmoud, E (2013) Challenges of computer crimes investigation in North Africa's. *The International Arab Conference on Information Technology* (ACIT) 1-6.

Olasanmi, O.O (2010). Computer crimes and counter measures in the Nigerian banking sector. *Journal of Internet Banking and Commerce*,15(1), 1-10

Singleton, T. W & Singleton, A. J. (2010) Fraud auditing and forensic accounting, Fourth Edition, New Jersey: John Wiley & Sons, Inc.

Wang, S-Y. K & Huang, W (2011). The evolutional view of the types of identity thefts and online fraud in the era of the internet. Available through www.internetjournalofcriminology.com