DOI: 10.15439/2022M9438
ISSN 2300-5963 ACSIS, Vol. 34

Digital Forensic Readiness of Cybercrime Investigating Institutions in Nigeria: A Case Study of the Economic and Financial Crimes Commission (EFCC) and the Nigeria Police Force

Robinson Tombari Sibe, PhD, CCME
Visiting Fellow
University of South Wales
Newport NP18 3QT, UK
Email – sibe99@yahoo.com

S. Raschid Muller, DBA, PhD
Assistant Professor of Cybersecurity
Capitol Technology University
Laurel, MD, USA
Email – srmuller@captechu.edu
https://orcid.org/0000-0002-1742-7575

***Abstract*—This case study investigates Nigeria's cybercrime agencies' digital forensic readiness and forensic capability and how this affects the cybercrime caseloads and prosecution. The Routine Activity Theory (RAT) and the Technology, Organization, and Environment (TOE) theories were applied. This study used the TOE framework to examine the digital forensic technology adoption and forensic readiness of cybercrime investigators in Nigeria and relates this with the RAT framework and the effectiveness of law enforcement agencies as capable guardians. The research population of this study was the Nigerian Internet fraud investigative agencies – the Economic and Financial Crimes Commission (EFCC) and the Nigeria Police Force (NPF). Eighteen participants from the two organizations were interviewed. The paper concluded that the cybercrime investigators in Nigeria are not forensically ready given the established lack of digital forensic resources (technological gap, human resources gap, skills gap, funding gap), particularly when juxtaposed with the high cybercrime caseloads in the country.**

***Index Terms*—cybercrime, internet fraud, digital forensics, routine activity theory, Nigeria**

I. Introduction

Nigeria is one of the hotbeds of cybercrime in the world. The scale and magnitude have been quite disturbing, not just to Nigeria but also to the international community, given the limitless boundaries of cybercrime [15][34]. The Nigerian Deposit Insurance Company [32] report shows Nigeria lost 15.15 billion Naira (approximately $43 million in 2019) to fraud in the banking sector alone in 2018. This amount represented an increase of 539% from the 2.37 billion Naira recorded in 2017. Cybercrime accounts for most of these. Their victims cut across the financial sector to other institutions and individuals across different jurisdictions. Internet fraud is driven mainly by financial gains [14]. Internet fraud originated from Advance Fee fraud. This fraudulent scheme is said to have a history in West Africa [26]. Globally, this scheme is mainly associated with Nigeria, which has influenced its naming – "419" and "Yahoo Yahoo" - with the "419" code being Nigeria's criminal code for fraud [3][4]. Besides averaging the highest loss per victim, Nigerian "419" scams are the second most reported cybercrime [12]. Symantec Corporation and African Union [38] reported that out of a large pool of email addresses used by online scammers, 46% were Nigerian Internet Protocol (IP) addresses. Unless otherwise determined by the Secretary of Defense (SecDef) or the President of the United States (POTUS), cyber-attacks on the election infrastructure are the first issues of homeland security [22][36]. As a result, the States and local governments should act as first responders to the cyber-attack before directly requesting support from the Cybersecurity and Infrastructure Security Agency (CISA).

II. Literature Review

Nigerian Internet fraudsters have increased in sophistication over the years. They have metamorphosed from sending bulk emails to unsuspecting victims to carrying out spear-phishing attacks and sophisticated Business Email Compromise (BEC) schemes that compromise their corporate email accounts. For instance, Nigerian cybercriminals reportedly caused a breach involving the confidential health records of over 750,000 persons in Los Angeles [7][8]. They now use sophisticated malware tools such as Zeus, Darknet, Predator pain, ISpySoftware, and other malware [24]. This increased sophistication has incentivized more attacks and perhaps explains the high numbers. Such a high prevalence is of significant concern to the country.

Nigeria has responded to these increasing caseloads by implementing reforms and setting up structures to combat Internet fraud. The Economic and Financial Crimes Commission (EFCC) [21] is the primary investigating agency for Internet fraud. Set up by the Economic and Financial Crimes Commission (EFCC) Act 2004 [20], the commission's mandate extends beyond Internet fraud to other financial crimes, both in the online and terrestrial world [33][42]. The commission investigated 15,124 petitions, securing only 568 convictions between 2010 and 2015 [25]. However, other agencies often play overlapping roles in this regard. For instance, the Nigerian Police Force has a dedicated cybercrime unit with a mandate to crack down on cybercrime [30]. This unit investigates and prosecutes Internet fraud [43]. Also, the National Security Adviser (NSA) plays a central role in cybercrime investigation as host to Nigeria's Computer Emergency Response Team [38]. They coordinate the nation's corporate response to cyber-attacks.

A. Routine Activity Theory (RAT)

Cybercrime has grown in popularity in the last two decades and is now an established research area in criminology [27][43]. Routine Activity Theory is a renowned situational theory of crime developed by Cohen and Felson [13].

The theory states that for crime to occur, three conditions must occur. The conditions are a motivated offender, a suitable target, and the absence of a capable guardian. This study is rooted in the third element: the absence of a "capable guardian."

There have been debates about the suitability of this theory in other areas beyond the terrestrial world. Specifically, there are varying perspectives and arguments regarding RAT's suitability to analyze the causation of cybercrime and Internet fraud. For instance, Yar [43] states that RAT cannot reliably explain the causation of Internet crime, given the spatiotemporal nature of cyberspace and the ecological nature of the RAT. Grabosky [23] believes the three conditions applicable in the terrestrial world also apply in the cyber world. Leukfeldt and Yar [27] also agreed that RAT is suitable for cybercrime due to the similarities between cyberspace and the terrestrial world.

The Capable Guardian. This study investigated the lack of digital forensic resources among the financial crime agencies in Nigeria. Looking at the three elements of RAT – motivated offender, a suitable target, and the absence of a capable guardian – the lack of forensic resources amongst law enforcement agencies fits the context of the capable guardian. Tseloni et al. [40] define guardianship as the capability of persons and objects to prevent crime. The concept of capable guardianship may be applied rather widely. Yar [43] suggests this could be the property owner, custodian, law enforcement, Computer Emergency Response Teams, banks, or any other, whose presence may discourage the occurrence of the crime in question. Bello and Griffiths [10] posited that the awareness of the existence of a capable guardian is a demotivating factor to the criminal.

B. Technology-Organization-Environment (TOE) Framework

Adoption refers to an individual's decisions to accept, diffuse and mainstream innovation in an integrated manner [48]. As organizations invest large sums in new technologies, it is essential to study technology adoption. Such investments may not yield positive results, except if the right adoption strategies are implemented (Ahmed, 2020). The rapidly evolving and emerging technological landscape has necessitated studying innovation adoption. Researchers have applied several technology adoption models to explore emerging technologies over the last few years (Leung et al., 2015). For instance, the Theory of Reasoned Action (TRA) [10], the theory of Planned Behaviors [9], the Technology Acceptance Model (TAM) [18], and the Unified Theory of Acceptance and Use of Technology (UTAUT) [54] have all contributed to perspectives in technology adoption.

However, Oliveira and Martins [42] observed that the above models focused more on the individual and suggested that the Technology-Organization-Environment (TOE) framework offers a better explanation of technology adoption at the firm level. Oliveira and Martins [42] noted that an essential feature of the TOE framework is incorporating environmental factors, which help explain technology adoption. As can be seen from the name, the TOE framework considers the three critical elements of adoption: technology, organization, and environment. Technological context includes all relevant technologies in the firm. This context comprises existing related tools and emerging technologies [35].

C. Digital Forensic Readiness

Although a relatively new term, digital forensic readiness has received much attention recently. Used first used by Tan [39], the concept has two primary objectives: to maximize the usefulness of the evidence collected; and to minimize the cost of investigations. Carrier and Spafford [11] further divided forensic readiness into operational and infrastructural readiness, with the former being concerned with adequate training and equipment and the latter with efficient data preservation. There are different ways to view digital forensic readiness, such as time, cost, training, and technology [19]. To be adequately empowered to investigate Nigeria's growing Internet fraud cases, the country's financial crime agencies must attain considerable forensic readiness. This capacity can be measured using any of the digital forensic readiness frameworks.

D. Digital Forensics Readiness Models

Different researchers have come up with many frameworks for Digital Forensic Readiness. For instance, Ngobeni et al. [31] developed a conceptual model for wireless networks. Makutsoane and Leonard [28] developed a forensic readiness model for a cloud service provider. Alenezi et al. [5] developed a framework for measuring an organization's forensic readiness for cloud services. Almarzooqi and Jones' [7] framework for digital forensic readiness narrowed their model to assessing the core capabilities of a Digital Forensic Organization. Garba and Bade [22] proposed a Digital Forensic Readiness model for Nigerian banks. This improved previous research work with Zenith Bank, Nigeria, as a case study [21]. Englbrecht et al. [20] proposed a capability model for digital forensic readiness. Pooe and Labuschagne [36] identified five critical components of the digital forensic readiness model: people, process, policy, technology, and data. There is literature on existing digital forensics models, leaving the forensic expert with many choice models.

E. Digital Forensic Readiness of the Nigerian Financial Crimes Agency

Nigerian investigative agencies must attain considerable forensic readiness to investigate Internet fraud and online financial crimes efficiently. In Nigeria, the primary law enforcement agency for cybercrimes is the EFCC and a complementary role by the Cybercrime division of the Nigerian Police [1] [2]. It is noteworthy that some agencies play a critical role in combatting cybercrime. For instance, the Office of the National Security Adviser plays a central role in cybercrime investigation as host to Nigeria's Computer Emergency Response Team [10] [38]. They coordinate the nation's corporate response to cyber-attacks. The scope of this research is limited to the investigative agencies – the EFCC and the Nigerian Police.

F. Processing and Thematic qualitiAnalysis

The researcher used a digital audio recorder for the interviews, with the consent of the participants. The researcher used the qualitative software NVivo to analyze the transcription of recorded interviews. This tool codifies themes from the interview transcripts. This study used inductive thematic analysis for the categorization of interview data. A thematic analysis could come in three forms: inductive analysis, theoretical analysis, and that which comes with constant comparison [45]. This study adopted the inductive thematic analysis. This method ensured the analysis of interviews without any pre-existing categories. The data collected was analyzed to look out for repeating patterns and themes. The study was structured to follow the analytic procedure Marshall and Rossman [33] recommended. The procedure adopted in this research is summarized below as:

1. Interview transcripts were studied, organized, and loaded into NVIVO.
2. Interview transcripts were further analyzed, read, and re-read.
3. The researcher generated categories and themes using NVivo
4. The researcher used NVivo to code data.
5. The research interpreted data analyzed by NVivo.
6. Searched for alternative understandings
7. The researcher presented research findings.

III. Research Design and Methodology

This study examined the digital forensic readiness of law enforcement agencies in Nigeria. This research used the qualitative case study method to investigate the digital forensic readiness of Nigeria's two primary cybercrime and financial crime prevention and prosecution agencies – the EFCC and the Nigerian Police Force. A qualitative study is suitable when investigating a relatively unknown phenomenon or subject of interest, and the resources available will allow for interviews and reviews of related documents [6]. It is exploratory and, therefore, more suitable in the context of this study.

Specifically, the research adopted the case study approach, a qualitative paradigm. Yin [44] gave four scenarios suitable for qualitative case studies. The four scenarios are:

1. When answers to the "how" and "why" questions are critical to research.
2. When it is impossible to manipulate research participants.
3. When the contextual conditions are relevant to the study; and
4. There is an unclear boundary between the phenomenon of interest and the prevailing contexts.

This research used the steps outlined by Baxter and Jack [9]. An essential first step in a case study is determining the case. Miles and Huberman [29] define a "case" as a phenomenon occurring in a bounded context. It is the unit of analysis. This research established the lack of digital forensic resources in Nigeria's financial crime agencies, as the case. The definition of the boundary followed once the "case" was determined [37] [44]. Defining the boundaries will keep the research focused. This research is limited to the law enforcement agencies in Nigeria responsible for combatting internet fraud - EFCC and the Nigeria Police Force.

This study was structured to investigate Nigeria's digital forensic readiness of cybercrime agencies. To this end, the research sample consisted of officers of the two principal agencies responsible for fighting financial crimes and internet fraud. They are the Economic and Financial Crimes, set up by the EFCC Act 2004 [16], and the Nigerian Police Force [33] [41]. The sample consisted of personnel from only departments directly involved or impacted by the use of or the lack of digital forensic technology in financial crimes prosecution to keep this study focused.

The sample consisted of five persons from the Cybercrime department of the Nigerian Police and thirteen officers of the EFCC, drawn from four related (forensic-dependent) departments within the organization – Digital Forensic department, Cybercrime Department, Advance Fee Fraud Department, and Legal (Cybercrime Prosecution) Department. This diversity was necessary to ensure broad perspectives. Participants had varying years of experience, ranging from four to over 20 years. Participants had the requisite work experience to discuss the subject, with fourteen out of the eighteen with more than ten years of experience.

While semi-structured interviews were used for this study, guiding questions ensured a focused and organized discussion. The five critical components of the Digital Forensic Readiness model identified by Pooe and Labuschagne [36] shaped the interview questions. The five components are people, Processes, Policy, Technology, and data. The researcher grouped the primary interview questions under the components identified by Pooe and Labuschagne [36]. This grouping helped to keep things focused and organized. The researcher also created a general theme for generic questions.

IV. Results

The qualitative analysis tool was used to generate a word cloud, shown in Figure 1. The thematic analysis produced five themes and nine subthemes. The main themes are personnel, digital forensic technology, digital forensic training, processes, and policy. The personnel theme had subthemes for personnel adequacy and personnel capability. The digital forensic technology theme had the following subthemes: tool availability and the impact of the lack of digital forensic technology. The digital forensic training theme had one subtheme: structured training. The process theme had the fol-

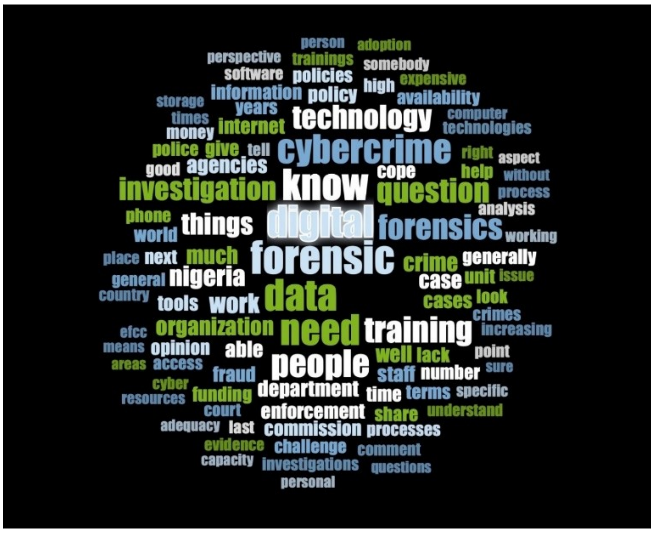

Fig 1 - Word Cloud Generated from Interview Files. *Note.* This figure shows frequently used words by participants as generated by NVivo.

lowing subthemes: defined processes and structured process reviews. The policy theme had two subthemes: policy framework and the roadmap for digital forensic readiness. The themes reveal the perspectives shared by participants drawn from the two agencies. The researcher analyzed the research questions within the context of these themes.

V. Conclusion

Seven themes emerged from participants' responses. The result was discussed by analyzing each theme against existing scholarly literature. The seven themes are personnel adequacy, capability, tools availability, tool licensing challenge, defined processes, structured process review, and policy framework. The study investigated the lack of digital forensic resources and the digital forensic readiness of Nigeria's cybercrime agencies using these themes in the digital forensic readiness framework. These themes fit into Pooe and Labuschagne's [36] five critical components of a Digital Forensic Readiness model of people, process, policy, technology, and data.

This study shows that the cybercrime investigating agencies in Nigeria lack digital forensic resources. The findings suggest they are not forensically ready and fall short of the expected capability maturity needed to perform efficiently and optimally in investigating cybercrime. This result which harvested views from the practitioners' point of view (Law Enforcement Agencies), is consistent with other scholarly works. Odumesi [41] submitted that the law enforcement agencies in Nigeria, particularly the Nigerian Police, lack the computer forensic laboratories to investigate and analyze cybercrime effectively.

Odumesi [41] further posited that beyond having enabling laws, law enforcement agencies need to acquire more tools and more training for their personnel if they wish to be effective. Oraegbunam [35] also echoed this position by submitting that there was a need to upscale the digital forensic capabilities of law enforcement agencies across the various formations and not just restricted to an elite law enforcement squad. Ehimen and Bola [18] asserted that the Nigerian Police are not technologically savvy and lack the computer forensic skills needed for investigating cybercrimes.

A. *Limitations of the Study*

While the two agencies chosen as the population for this study are principally responsible for prosecuting financial crimes in Nigeria, in reality, there are also overlapping roles by other related agencies. For instance, the Office of the National Security Adviser plays a central role in cybercrime investigation, as host to Nigeria's Computer Emergency Response Team (Symantec Corporation and African Union, 2016). They coordinate the nation's corporate response to cyberattacks and therefore play a role in the fight against Internet fraud. However, because they are not frontline agencies in financial crime investigation, this study did not capture them.

B. *Implications for Practice*

This study was limited to the EFCC and the Nigeria Police Force. The research was delimited to sample of the staff of the digital forensics unit of the EFCC and the Cyber crime unit of the Nigeria Police Force. Expectedly, these are elite units of small teams. For instance, the EFCC digital forensics unit at the agency's head office has an 8-man team (Okolorie, 2020). Extending the sample far beyond this might affect the focus of the study.

The sample for the Police was also limited to staff of the unit at the Force Headquarters. It is noteworthy to mention that the 36 states in Nigeria all have fraud units in the states. Therefore, limiting the study to just the force headquarters may not be representative of the entire opinion of the rank and file of the Police. Further studies could benefit from the outcome of this study to extend the study to all the 36 states and beyond just the cybercrime unit.

C. *Summary*

In summary, this research was conducted to identify themes for reference to be taken into consideration that could potentially shape policy formulation in both organizations and, by extension, in law enforcement agencies in Nigeria. It established the lack of digital forensic resources and made specific findings. The research made novel contributions by identifying themes needed by Nigeria's cybercrime agencies. The study sought to investigate the digital forensic readiness of Nigeria's financial crime agencies. Previous studies highlighted the gaps in forensic resources of law enforcement agencies as a significant impediment to the fight against cybercrime. For instance, Odumesi [41], Oraegbunam [35], and Bello and Griffiths [10] all pointed to this lack of forensic capabilities of law enforcement agencies. These studies only pointed to the lack without drilling into the specifics. Therefore, this study investigated the specifics of this lack – technology, human resources, capabilities, and others - both from the insider's perspective and available literature and documents.

The finding of this research establishing the digital forensic readiness and the extent of lack of digital forensic resources is an essential first step to developing a practical roadmap to forensic readiness for both organizations. This research outcome could help strengthen the cybercrime investigation capability of the Nigerian Police Force and the Economic and Financial Crimes Commission in Nigeria by inserting the identified themes that this study produced.

References

[1] O. S. Adesina, "Cybercrime and poverty in Nigeria", 2017. Canadian social science, 13(4), 19-29.

[2] R. Ajetunmobi, C. Uwadia, and F. Oladeji, Computer forensic guideline: A Requirement for fighting cyber crime in Nigeria now?, 2016. UNILAG research conference 2016, Nigeria. https://ir.unilag.edu.ng/handle/123456789/5833

[3] O. Akanle, J. Adesina, and P. Akarah, "Towards human dignity and the Internet: The cybercrime (yahoo yahoo) phenomenon in Nigeria" 2016. African Journal of Science, Technology, Innovation and Development, 8(2), 213-220.

[4] O. Akanle and B. Shadare, Yahoo-plus in Ibadan: Meaning, characterization, and strategies, 2019. International Journal of Cyber Criminology, 13(2).

[5] A. Alenezi, R. Hussein, R. Walters, and D. Wills, A framework for cloud forensic readiness in organizations. 2017 5th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud), 199–204. https://doi.org/10.1109/MobileCloud.2017.12

[6] B. Algozzine, and D. Hancock, Doing case study research: A practical guide for beginning researchers. Teachers College Press, 2017.

[7] A. Almarzooqi and A. Jones, A framework for assessing the core capabilities of a digital forensic organization. In IFIP international conference on digital forensics (pp. 47-65). Springer, Cham 2016.

[8] Associated Press, "Nigerian man charged with hacking Los Angeles County emails", 2016. Guardian newspaper. https://www.theguardian.com/us-news/2016/dec/18/los-angeles-county-email-hack-kelvin-onaghinor

[9] I. Ajzen, The theory of planned behavior. Organizational Behavior and Human Decision Processes, 50, 179–211, 1991.

[10] I. Ajzen and M. Fishbein, Understanding attitudes and predicting social behavior. Prentice-Hall Englewood Cliffs, 1980.

[11] T. Barboza, "LA County targeted in phishing cyberattack; Private information of 750,000 people compromised", 2016. Los Angeles times. https://www.latimes.com/local/lanow/la-me-ln-county-cyberattack-20161217-story.html.

[12] P. Baxter and S. Jack, Qualitative case study methodology: Study design and implementation for novice researchers. The qualitative report, 13(4), 544-559, 2008.

[13] M. Bello and M. Griffiths, Routine activity theory and cybercrime investigation in Nigeria: How capable are law enforcement agencies? In Rethinking Cybercrime (pp. 213-235), 2021. Palgrave Macmillan, Cham.

[14] B. Carrier and E. Spafford, An event-based digital forensic investigation framework, 2004. Digital Investigation. https://dfrws.org/wp-content/uploads/2019/06/2004_USA_paper-an_event-based_digital_forensic_investigation_framework.pdf

[15] K. Choi, C. Lee, and E. Louderback, Historical evolutions of cybercrime: From computer crime to cybercrime. The Palgrave Handbook of International Cybercrime and Cyberdeviance, 27-43, 2020.

[16] L. Cohen and M. Felson, Social change and crime rate trends: A routine activity approach. American Sociological Review, 588-608, 1979.

[17] C. Cross, Victims' motivations for reporting to the 'fraud justice network.' Police Practice and Research, 19(6), 550-564, 2018.

[18] F. D. Davis, "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology" 1989. MIS Quarterly, 13(3), 319–340. https://doi.org/10.2307/249008

[19] F. E. Eboibi, A review of the legal and regulatory frameworks of the Nigerian Cybercrimes Act 2015. Computer Law & Security Review, 33(5), 700-717, 2017.

[20] Economic and Financial Crimes Commission, UK government donates forensic equipment to EFCC, 2013. https://efccnigeria.org/efcc/news/576-uk-government-donates-forensic-equipment-to-efcc

[21] Economic and Financial Crimes Commission, UK to support EFCC's anti-corruption fight with digital forensic technology, 2018. https://efccnigeria.org/efcc/news/3328-uk-to-support-efcc-s-anti-corruption-fight-with-digital-forensic-technology

[22] O. Ehimen and A. Bola, Cybercrime in Nigeria. Business Intelligence Journal, 3(1), 93-98, 2010.

[23] M. Elyas, S.B. Maynard, A. Ahmad, and A.Lonie, Towards a systemic framework for digital forensic readiness. Journal of Computer Information Systems, 54(3), 97-105, 2014.

[24] L. Englbrecht, S. Meier, and G. Pernul, "Towards a capability maturity model for digital forensic readiness". Wireless Networks, 1-13, 2019.

[25] A. Garba and M. Siraj, A holistic–based digital forensic readiness framework for Zenith Bank, Nigeria. International Conference on Computational and Social Sciences, 551-560, 2015.

[26] A. Garba and A. Bade, A recommended digital forensics readiness framework for Nigerian banks. International Journal of Development Research, 9(08), 2019.

[27] P. Grabosky, Virtual criminality: Old wine in new bottles? Social & Legal Studies, 10(2), 243-249, 2001.

[28] A. Hinchliffe, "A Nigerian princes to kings of malware: The next evolution in Nigerian cybercrime". Computer Fraud & Security, 2017(5), 5-9, 2017.

[29] I. Jamo, Economic and Financial Crimes Commission (EFCC) and Anti-Corruption Crusade in Nigeria: Success and Challenges. Gusau International Journal of Management and Social Sciences, 4(2), 13-13, 2021.

[30] A. Kigerl, Spam-Based Scams. In Holt T. & Bossler A. (Eds.), The palgrave handbook of international cybercrime and cyber deviance, 2020. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-319-78440-3_42

[31] E. Leukfeldt and M. Yar, Applying routine activity theory to cybercrime: A theoretical and empirical analysis. Deviant Behavior, 37(3), 263-280, 2016.

[32] M. Makutsoane, and A. Leonard, A conceptual framework to determine the digital forensic readiness of a cloud service provider, July 2014. In Proceedings of PICMET'14 Conference: Portland International Center for Management of Engineering and Technology; Infrastructure and Service Integration (pp. 3313-3321).

[33] C. Marshall and G. Rossman, Designing qualitative research, 2014. Sage publications.

[34] M. Miles and A. Huberman, Qualitative data analysis: An expanded sourcebook, 1994. Sage.

[35] S. R. Muller and D. N. Burrell, "Social Cybersecurity and Human Behavior. International Journal of Hyperconnectivity and the Internet of Things (IJHIoT)", 6(1), 1-13, 2022.

[36] S. R. Muller and M.L. Lind, "Factors in information assurance professionals' intentions to adhere to information security policies". International Journal of Systems and Software Security and Protection (IJSSSP), 11(1), 17-32, 2020.

[37] News Agency of Nigeria , "Police to create a special unit to tackle cybercrime", 2016. Guardian Newspaper. https://guardian.ng/news/police-to-create-special-unit-to-tackle-cybercrime/

[38] S. Ngobeni, H. Venter, and I. Burke, "A forensic readiness model for wireless networks". In K.-P. Chow & S. Shenoi (Eds.), Advances in Digital Forensics VI (Vol. 337, pp. 107–117), 2010. Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-15506-2_8

[39] Nigerian Deposit Insurance Company, NDIC annual report 2018, 2019. https://ndic.gov.ng/wp-content/uploads/2019/09/NDIC-2018-ANNUAL-REPORT.pdf

[40] E. Obuah, Combatting corruption in Nigeria: The Nigerian economic and financial crimes (EFCC). African Studies Quarterly, 12(1), 2010.

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

[42] T. Oliveira and M. Martins, Literature review of information technology adoption models at firm level. Electronic Journal of Information Systems Evaluation, 14(1), pp110-121, 2011.

[43] B. Omodunbi, P. Odiase, O. Olaniyan and O. Esan, Cybercrimes in Nigeria: Analysis, detection, and prevention. Journal of Engineering and Technology, 1(1), 37-42, 2016.

[44] I. Oraegbunam, "The Nigerian police and problems of cybercrime investigation: Need for adequate training". Nigerian Law Journal, 18(1), 1-28, 2015.

[45] W. Percy, K. Kostere and S. Kostere, Generic qualitative research in psychology. The qualitative report, 20(2), 76-85, 2015.

[46] A. Pooe and L. Labuschagne, A conceptual model for digital forensic readiness, August 2012. In 2012 Information Security for South Africa (pp. 1-8). IEEE.

[47] R. Stake, The art of case study research. Sage, 1995.

[48] E. Straub, Understanding technology adoption: Theory and future directions for informal learning. Review of educational research, 79(2), 625-649, 2009.

[49] Symantec Corporation and African Union,Cybercrime & cybersecurity trends in Africa, 2016. www.thehaguesecuritydelta.com/media/com_hsd/report/135/document/Cyber-security-trends-report-Africa-en.pdf

[50] J. Tan, Forensic readiness. Cambridge, MA:@ Stake, 1-23, 2001.

[51] A. Tseloni, K. Wittebrood, G. Farrell, and K. Pease, Burglary victimization in England and Wales, the United States and the Netherlands: A cross-national comparative test of routine activities and lifestyle theories. British Journal of Criminology, 44(1), 66-91, 2004.

[52] I. Umar, R. Samsudin, and M. Mohamed, Understanding the successes and challenges of Anti-Corruption Agency (ACA) in Nigeria: A case of Economic and Financial Crimes Commission (EFCC). Asian Journal of Multidisciplinary Studies, 4(5), 27-33, 2016.

[53] V. Venkatesh, M. Morris, G. Davis, and D. Davis, User Acceptance of Information Technology: Toward a Unified View, 2003). MIS Quarterly, 27(3), 425–478. https://doi.org/10.2307/30036540