Global Journal of Computer Science and Technology: G Interdisciplinary
Volume 18 Issue 3 Version 1.0 Year 2018
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Cyber Forensic and Data Collection Challenges in Nigeria

By Whyte Stella Tonye

Abstract- The importance of structural investigation to obtain a reliable chain of evidence on cyber-attacks organizations or individual data for application of legal presentation in court in computer forensics. Where ever there is a discovery of evidence or proofs of illegal misuse of organization data it leads to the prosecution of the culprits. Today the technology in cyber forensic is utilizing the application of scientific methods and technics to recover data from electronic and digital media. This scientific method requires expertise that goes beyond regular forensic data collection, techniques, and practices which must conform to universal standards. Increase in the use of computer and the internet has resulted in the change in human behaviors and ways in which they communicate, this growth in technology has given rise to cybercrimes which have caused the insecurity of the cyberspace in general. The increase in the growth of computer and the Internet use has changed the human behavior and ways of communication, this growth in technology has given rise to the rise in cybercrime which is now sophisticated and difficult to trace, investigate, and prosecution of criminals without reliable and accurate data collection.

GJCST-G Classification: H.2.7

Strictly as per the compliance and regulations of:

Cyber Forensic and Data Collection Challenges in Nigeria

Whyte Stella Tonye

Abstract- The importance of structural investigation to obtain a reliable chain of evidence on cyber-attacks organizations or individual data for application of legal presentation in court in computer forensics. Where ever there is a discovery of evidence or proofs of illegal misuse of organization data it leads to the prosecution of the culprits. Today the technology in cyber forensic is utilizing the application of scientific methods and technics to recover data from electronic and digital media. This scientific method requires expertise that goes beyond regular forensic data collection, techniques, and practices which must conform to universal standards. Increase in the use of computer and the internet has resulted in the change in human behaviors and ways in which they communicate, this growth in technology has given rise to cybercrimes which have caused the insecurity of the cyberspace in general. The increase in the growth of computer and the Internet use has changed the human behavior and ways of communication, this growth in technology has given rise to the rise in cybercrime which is now sophisticated and difficult to trace, investigate, and prosecution of criminals without reliable and accurate data collection.

I. Introduction

The emergence of the world wide web and the development of the information technology have necessitated the rise in a cyber investigation, as cybercrime is growing so fast and maturing into a more challenging issue and need to be confronted (Kumarri and Mohapatra, 2016). A gap is seen with regards to analysis of large and disparate datasets and data collection strategies as the existing forensic software solutions developed from the first generation of tools addressed mainly scalability issues. As the volume of data increases it affects the capability of processor speed and the rate forensic tools can manage (Darren and Kim-Kwang, 2014).

Harichandran, Breitinger, and Baggili (2016) stated that the increase in the number of successful cyber-attacks is threatening financial and personal security worldwide. Currently, there is a shift from the usual hobby hacking to a well-organized cybercrime. These attacks are now typically carried out for personal and commercial purposes in a more sophisticated and targeted manner in the bid to circumvent common security measures. (Skopik, Settanni, and Fiedler, 2016). Several cyber forensic techniques are used to Investigate these increasing cybercrimes. These techniques assist in tracking down internal and external network attacks by focusing on inherent network vulnerabilities and communication mechanisms (Suleman et al. 2015).

Cyber Forensic is a field that is new and emerging with the introduction of new technologies readily accessible, available, affordable, and heavily dependent on individuals and businesses. As technology grows, new criminal techniques and activities known as cybercrimes emerge, posing challenges to law enforcers (Hamid & Amin, 2014). According to Zhou and Ziang (2012), cyber forensic is a brand new technology in the law of information security, with two procedures; first, searching for evidence and secondly taking out the evidence. It is therefore essential to protect data from targeted system attack. Very important is to prevent hackers from attacking and stealing away organization data and electronic evidence. Organizations could prevent these attacks by collecting related data and analyzing security policies/procedures and knowing the security status of the entire system and securing personnel awareness level.

A reliable data collection is the beginning of successful operations of an analysis system as the accuracy of data is directly affected by strategies of data collection (Zhou and Ziang, 2012). According toSesan, Soremi, and Oluwafemi (2015), the recentincidents of ATM fraud, identity theft, email hijacking of email accounts, and phishing on individuals and the financial institutions has increased the rate ofcybercrime in Nigerian. This has resulted to a hype in the economic cost of cybercrime to Nigeria which was before now unknown. Sesan et.al's work shows thathigher incidence of cybercrime is seen morein the Western and Eastern parts of the country although a small sample size was used. The general IT problem is that most developing countries like Nigeria do not have strategies to ensure reliable forensic data collection to carry out forensic investigations. The specific IT problem is that IT managers lack strategies to ensure the reliability of cyber forensic data collection for forensic investigations. Again most studies on cyber forensic are done outside of the shores of the country. Hence this paper examines the challenges of cyber forensic data collection in Nigeria.

Author: *Rivers State Ministry of Health, Port Harcourt, Nigeria.*
e-mail: *stellawhyte@outlook.com*

II. Literature

This study used the disruptive innovation theory as a framework. Clayton Christensen coined the theory and analyzed the phenomenon in 1995. Disruptive innovation theory describes a process where product or service takes its root from simple applications at the bottom of the market and rigorously moves up the market, eventually displacing established competitors. (Christensen, 2016). The author developed the disruptive innovation theory for evaluation and clarification of business strategies to respond to technological change. Disruption theory helps the development of new technology to make a strategic choice between taking a sustainable path and taking a disruptive one. Identification of the technology industries has resisted the forces of disruption, at least until very recently. Cyber forensic globally is one of such. Over more than 100 years, new kinds of technology with diverse initial charters created helped to address the problems of various population segments. The use of this disruptive theory in this study makes collection of reliable forensic data measurable and significantly more accurate as predictions of which cyber forensic investigations will succeed (Christensen et al., 2015). The theory is also used to explore cyber forensic investigations as the type of destructive innovations which requires a fundamental shift in ways data collection for investigation is carried out by investigators.

III. Concept of Cyber Forensic

According to Losavio, Pavel, & Polyakova (2015), cyber forensic is the search to reliable evidence within electronic information. Computer forensics is the practice of collection, analyzing and reporting on digital data in a legally admissible manner. It is used in the detection and prevention of crime and in any dispute when evidence is stored digitally (Forensic control, 2016). The practice follows a similar process to other forensic disciplines and faces related issues. Aziz (2014) defined a digital forensic tool called data acquisition as a more reliable tool to measure correctness, accuracy, and completeness for the course of justice and discovery of facts. The objective of this study is to explore strategies used by IT managers and investigators to ensure the reliability of cyber forensic data collection for forensic investigations of cyber-crimes. According to the Cyber Shield (2016. 9 August), more than 58% organization in the world still lack appropriate controls to prevent insider attack, with just 44% unaware that their organization ever had experience of an insider attack at all. The literature review aligns with the purpose of the study to explore best strategies employed by cyber forensic investigators, which successful cyber forensic investigation managers may use to ensure the reliability of data collection. An extensive review of books and journal articles provided insight concerning the issue of data collection for cyber forensic investigations in Nigeria. According to Nte Ngoboawaji (2012), lack of forensic skills and equipment has negatively affected forensic investigation capabilities in Nigeria which have resulted in the high increase in unresolved murder cases. Oladele (2006) opined that the Nigeria police force which is charged with the responsibility of maintaining law and order, unfortunately, is inadequate thereby adding to the mystery of absence of justice as experts have linked criminal justice system to lack of absence of forensic evidence rendering justice ineffective.

This paper intends to identify the gaps observed in the previous research literature. In doing so, series of different topics associated with the issue of cyber forensic and data collection emerged including anti-forensic attacks, forensic investigations, digital forensic, computer forensic, and computer security. Books and journal articles were extensively reviewed to provide insight on the issue of data collection in cyber forensic investigations and challenges. The process yielded several different topics related to the subject of the study. The increase in the size of data to be presented for analysis has resulted in a significant challenge in computer forensic analysis. Materials published in the past five years (2011–2016), have been located by searching various academic databases including EBSCO, ACM digital lib, Google Scholar, and IEEExplore to mention a few. The author checked keywords like computer forensics, data collection, computer forensic challenges, and forensic data on computer forensic on the internet. According to Daren & Kim (2014), there is a serious gap about cyber forensic data volume challenge about the acquisition of data and models used in the database. Issues in integration process of forensic cases have been raised on data acquisition and the modules used (Quentin et al. 2014). Gou, Jim, and Quim (2013), opined that email is one of the written form naturally used as documentary evidence and as a potential carrier of criminal evidence. The email header provides detailed technical information, such as the sender, software used by the composer and the email server. Technical digital forensic identifies, collects, preserves and analyses data in a way that preserves the integrity of the evidence gathered so that it can be used effectively in a legal case. Nickson and Venter, (2013) present a step by step framework in an attempt to propose a high-level procedure for enhancing the potential digital evidence presentation in any legal proceedings. Kumari and Mohapatra,(2016) iterated that cyber investigations and crime is growing and maturing into a more challenging issue which needs to be confronted early. They also declared that lack of digital forensic tools and techniques had hindered forensic investigations. Nickson and Venter (2015) in their paper also stated that cyber forensic methods assist in

tracking down internal and external network attacks by focusing on the inherent network vulnerabilities and communication mechanics. Losavio et al., (2015) in their study states that cyber forensic is the search for reliable evidence within electronic information which may result in infringing on users privacy. Slim and Noureddine (2013), describes techniques used in digital forensic investigations to be theoretical and scientific. The theoretical techniques are characterized by anti-forensic while the scientific techniques as the preparation of systems for forensic analysis. The theory of hierarchical visibility was proposed to investigate security incidents conducted over complex systems and to be used in the anti-forensic attack to investigate and provide or prove occurrences from uncomplicated evidence. Kumarri and Mohapatra, (2016) have also stated that lack of digital forensic tools and techniques has hindered forensic investigations.

IV. Material Method

This paper used the qualitative exploratory case study research method for this study. The author used the qualitative method for this study to establish exploratory actions to understanding the meaning behind actions and behaviors in employing strategies by IT managers in a cyber forensic investigation to ensure reliability in data collection. The research method is also used for conducting interviews is to obtain unique and comprehensive information from the participants undergoing the interview (Tuominen, Tuominen & Jussila, 2013). The justification for selecting qualitative rather than quantitative or mixed methods was by the preference to collect multiple sources of data. From the description of Malina, Hanne, and Selto (2011), mixed method researchers employ emphases on both qualitative and quantitative approaches to create a research outcome stronger than either method individually. The preferred method of the study was the qualitative method not quantitative or mixed method because researchers use the qualitative method as a means to involve directly with the participants (Toloie-Eshlaghy et al., 2011). The author used a qualitative method to seek an in-depth understanding of IT managers based on an insider's experience and perception of the phenomenon.

V. Research Design

This paper uses the case study research design for the study. A case study design is an increasingly popular approach among qualitative researchers (Hyett, Kenny, & Dickson, 2014). Using a case study design has a level of flexibility that researchers may not have with other research methods such as phenomenology, narrative, and ethnography design (Hyett et al., 2014). The qualitative research method was used to establish exploratory actions by researchers to understand the meaning behind actions and behaviors and to see the phenomenon from the perspective of the participants (Sinkovics & Alfoldi, 2012). The method allows the use of an in-depth exploration of the phenomenon by actively engaging with participants who have experiences with the phenomenon and expresses their perceptions in their understanding (Coenen, Stamm, Stucki, & Cieza, 2012). This paper uses the qualitative method to explore actions to understand the meaning behind actions and behaviors and to see the phenomenon from the perspective of the IT managers which both quantitative and mixed method which cannot of providing (Sinkovics & Alfoldi, 2012).Quantitative research method, on the contrary, is used by researchers to represent the generalization of a population with the use of numerical data to prove or disapprove a hypothesis (Hoare & Hoe, 2013). This paper would also give the author opportunity to interact with participants in day-to-day practice to explore issues in the context of work which is the intent of this study (Moll, 2012).

VI. Social Implication

Cyber forensic is the search to reliable evidence within the electronic information; this may result to infringing on personal privacy and challenging fundamental legal principles to protect forensic data. The investigations undergo legal and policy development to interconnectivity. Cybersecurity protects systems and networks against unauthorized access, data manipulation, and defense against any hacker or intruder (Olayemi 2014). Hence IT managers and business outfit and government agencies should ensure overall system integrity and sustainability of their network infrastructure. Also, organizations should increase its defense –in- depth approach to network and computer security with the adoption of appropriate cybersecurity wares.

More so, given that collecting evidence the digital media is properly examined and checked to identify, preserve recover and analyze facts and opinions about the information gathered. The evidence is usually difficult to collect as the right tools are not available to collect them or they are of low quality or as revealing the identity of the criminal is difficult.

VII. Conclusion

The number of successful cyber-attacks has risen significantly in the global world and continues to threaten financial and personal security. Cyber forensics has undergone a shift where evidence is massive in size and may be insufficient to convict cybercriminals and financial loss is recently a big worry in the globe with major concerns in standardization. These cyber forensic challenges can be reduced by researching new methods to improve reliable forensic data collection and

speed up evidence recovery and analysis for investigations. The government and organizations need to get better forensic tools and techniques to support a wider variety for investigative purposes. The objective of this study was to enlighten IT managers in government and private organizations in Nigeria with strategies to ensure the reliability of cyber forensic collection of data for forensic investigations to reduce cybercrimes and vulnerability in the society. The adoption of the information from this study may contribute to building a sustainable and less vulnerable society in Nigeria and other sub-Saharan African countries. Digital forensic investigation process models have provided guidelines to identify and preserve potential digital evidence captured from a crime scene, but the process for this forensic evidence to be admissible in court is a significant challenge to investigations as there are currently no standardized guidelines to present the standard collection and representations of digital forensic evidence. This paper, therefore, recommends that methodologies and expertise are needed in a country to enhance the potential cyber forensic digital collection, presentation, and interpretations in any legal proceedings.

References Références Referencias

1. Christensen, Michael E. RaynorRory McDonald (2015). What Is Disruptive Innovation?. Harvard Business Review, 44–53. Retrieved from https://hbr.org/2015/12/what-is-disruptive-innovation
2. Darren, Q. & Kim-Kwang, R. C.(2014). Impacts of increasing volume of digital forensic data: A survey and future research challenges. Digital Investigation, 11, 273-294. http://dx.doi.org/10.1016/j.diin.2014.09.002
3. Guo, H., Jin, B., & Qian, W.(2013). Analysis of email header for forensic purpose. International conference on communication sysem and network technologies. doi:10.11.09/CSNT.2013.78.
4. Harichandran, S.V., Breitinger, F., Baggili, I., & Marrington, A. (2015). A cyber forensics needs analysis survey: Revisiting the domain's needs a decade later. Computers & security, 57, 1–13. doi.org/10.1016/j.cose.2015.10.007
5. Hyett, N., Kenny, A., & Dickson, V. (2014). Methodology or method? A critical review of qualitative case study reports. International Journal of Qualitative Studies on Health and Well-Being, 9, n/a. doi:10.3402/qhw.v9.23606
6. Krajcovic, P. (2015). Strategies in media planning. Communication Today, 6(2), 20-31. Retrieved from http://www.communicationtoday.
7. Kumari, N. & Mohapatra, A. K (2016). An insight into digital forensics branches and tools. International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT), 243-250. doi.org/10.1109/icctict.2016.7514586
8. Losavio, M. P., Pavel, P., & Polyakova, S.(2015). Cyber black box/event data recorder: legal and ethical perspectives and challenges with digital forensics. The Journal of Digital Forensics, Security, and Law. 10(4), 43-57. Retrieved from http://ojs.jdfsl.org/index.php/jdfsl/article/view/352/257
9. Kumari, N. & Mohapatra, A. K (2016). An insight into digital forensics branches and tools. International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT), 243-250. doi.org/10.1109/icctict.2016.7514586
10. Malina, M., Hanne, N., & Selto, F. (2011). Lessons learned: Advantages and disadvantages of mixed method research. Qualitative Research in Accounting and Management, 8(1), 59-71. doi:10.1108/11766091111124702
11. Nte, Ngboawaji Daniel. (2012). An Evaluation of the Challenges of Forensic Investigation and Unsolved Murders in Nigeria.. African Journal of Criminology and Justice Studies. African Journal of Criminology and Justice Studies: AJCJS, 6(1&2), 143-162.
12. Olayemi, J. O. (2014). A socio-technological analysis of cybercrime and cyber security in Nigeria. International Journal of Sociology and Anthropology, 6(3), 116-125. doi:10.5897/IJSA2013.0510
13. Sesan,G., Soremi, B., and Olufemi, B. (2015). Retrieved from https://www.pinigeria.org/download/cybercrimecost.pdf
14. Skopik, Settanni, & Fiedler (2016). A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. Computers & Security, 60, 154–176. doi.org/10.1016/j.cose.2016.04.003
15. Slim, R. & Noureddine, B. (2012). A Hierarchical Visibility theory for formal digital investigation of anti-forensic attacks. Computers & Security, 31(8), 967–982. doi.org/10.1016/j.cose.2012.06.009
16. Suleman, K., Abdulla, G., Ainuddin, W. A W., Mohamed, S., & Lftikhar, A.(2015). Cyber Forensic Techniques. Journal of Network and Computer Application, 66, 214-235. Doi:10.1016/j.jnca.2016.03.005
17. Toloie-Eshlaghy, A., Chitsaz, S., Karimian, L., & Charkhchi, R. (2011). A classification of qualitative research methods. Research Journal of International Studies, 20,106-123. Retrieved from http://www.eurojournals.com.
18. Tuominen, T., Tuominen, P., & Jussila, I. (2013). A tool to be used deliberately: Investigating the role of profit in consumer co-operatives. International Business Research, 6, 122-133. doi:10.5539/ibr.v6n11p1