International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 1 Jan-Feb 2021, pp: 826-832 www.ijaem.net ISSN: 2395-5252

Strategies for Identity Theft Prevention and Countermeasures in Nigeria:A Narrative Study

Theresa Chioma Nwabineli[1], & Dr. Felix Chukwuma Aguboshim[2]

[1]*Lecturer, Department of Computer Science, Federal Polytechnic, Oko Nigeria.*
[2]*Principal Lecturer, Department of Computer Science, Federal Polytechnic, Oko Nigeria.*

Submitted: 25-01-2021 Revised: 05-02-2021 Accepted: 08-02-2021

ABSTRACT: The growing and ubiquitous reliance of technological innovations for electronic file-sharing networks across all business transactions over the internet has increased the magnitude of identity theft. In Nigeria, this is more pronounced by lack of agile learning processes, poor knowledge sharing practices, and high illiteracy rate of 40.33% for adults aged 15 years and older. A positive relationship exists between high internet access, poor knowledge sharing practices, illiteracy, and increased identity theft. Knowledge sharing practices and technology awareness strategies required for identity theft prevention in Nigeria are still largely undeveloped, outdated, and non-sustainable despite the huge cyber-security innovations. This study highlights the gaps created by high illiteracy rate, poor knowledge sharing practices, and identity theft prevention awareness, in curbing identity theft, and strategies to close them. A narrative review methodology was adopted in this study that reviewed prior research works of literature that revealed significant information on identity theft prevention in Nigeria. Also, peer-reviewed articles within the last five years were extracted from electronic databases, using some keywords such as “Identity theft”, “Identity theft prevention”, “consequences of identity theft”, etc. Results show that identity theft in Nigeria can be prevented through improved literacy level, agile learning processes, good knowledge sharing practices, and excellent adherence to cyber-security policies. Findings from this study may extend proper knowledge sharing practices and proper identity theft prevention strategies in Nigeria.

Keyword: Identity theft prevention, Consequences of identity theft, knowledge sharing practices, Identity theft solution, cyber-security policies.

I. INTRODUCTION

Identity theft is defined as the intentional, unauthorized use of unwitting individual’s identifying information or credentials for unlawful purposes or financial transactions (Burnes, DeLiema, & Langton, 2020; Federal Trade Commission, 1998; Koops & Leenes, 2006). Identity theft is the act of stealing or obtaining the personal or financial information, or credentials of unsuspected persons in order to pose as them for unauthorized purchases or financial transactions (Golladay & Holtfreter, 2017; Thomas, 2018). Identity theft can be seen as the deceitful act or fraudulent intentional, unauthorized use of a person’s identifying information for unlawful purposes or criminal purposes without their consent (Reyns, 2013). Similarly, it is an online fraud that encompasses the cloning or duplication of someone’s digital information or online accounts with the intention of committing identity fraud against individuals or organizations (Wall, 2013). Simply put, it is using trickery to gain a dishonest advantage over or steal someone’s personal information to perform unlawful transactions on your behalf without your knowledge or permission.

Identity theft is not only a personal matter. Big organizations also experience data breaches, involving customer or consumer data being leaked or stolen, thereby leading to occurrence of identity theft using information gained from one of these breaches. Identity theft has become ubiquitous and therefore is affecting individuals all over the world (Reyns & Henson, 2016). Globally, the rise of new digital technologies and the growing reliance on the electronic file-sharing networks and storage of personal information across all forms of banking transactions, entertainment, and business services over the internet has intensified the magnitude of identity theft. The need for identity theft prevention in an ever-rising incidence of cybercrime has become increasingly evident and significantly important in developing countries, especially in Nigeria, where internet services, electronic file-sharing, and storage of personal information play critical roles among predominantly illiterate Nigerians. The existing technological innovations in Nigeria have failed to provide easy-to-use system for the high populated illiterates or semiliterate Nigerians, and the many literate ones with illiterate-mind-sets (Aguboshim & Miles, 2018). United Nations Educational, Scientific, and Cultural Organization (UNESCO) 2015 Statistic Report placed the Nigeria literacy rate for adults aged 15 years and older at 59.67% (UNESCO, 2015), meaning that 40.33% of Nigerians are illiterates.

In Nigeria, identity theft prevention has become significantly difficult due to the level of illiteracy, among others, which is put by the United Nations Educational, Scientific, and Cultural Organization (UNESCO) 2015 Statistic Report as 40.33% for adults aged 15 years. Specifically, positive and significant statistical relationships exist between high illiteracy rate, high internet access, poor knowledge sharing practices, poor learning processes, poor adherence to cyber-security policies, high corruption practices, and increased identity theft (Anyaehie & Areji, 2015; Bennett, 2017). There is no uniformity in the application of strategies for user-centered system interface and improved literacy level (Aguboshim & Miles, 2018), agile learning processes and good knowledge sharing practices (Shah, et al., 2019), and excellent adherence to cyber-security policies designed to prevent identity theft especially in Nigeria (Aguboshim, et al., 2019; Olise, 2010). Nigeria is ranked among countries in Africa where identity theft is prevalent. Strategies Policies and technology required for the operation of identity theft prevention and solutions in Nigeria are still largely undeveloped, outdated, and non-sustainable despite the huge human resources and technological innovations

1.1 Problem Statement

Agile learning processes and good knowledge sharing practices coupled with good system usage literacy required to prevent identity theft are crippled by outdated, non-sustainable, or virtually non-existent practices, awareness, and literacy campaign systems in Nigeria. Our purpose in this study was to identify major forms of social engineering techniques to perpetrate identity theft and the loopholes or sequence of communication adopted typically in Nigeria by cybercriminals, and strategies of effective prevention and countermeasures or recovery. The general IT problem postulated in this study was the high incidence of identity theft in Nigeria due to high illiteracy rate and lack of agile learning processes, good knowledge sharing practices, and excellent adherence to cyber-security policies to prevent identity theft. The specific IT problem is that some managers and stakeholders of organizations lack strategies, practices, policies, and value systems for identity theft prevention and countermeasures or recovery.

1.2 Research Question

What are learning processes and knowledge sharing practices and strategies used by stakeholders to effectively prevent and counter identity theft?

II. LITERATURE REVIEW

Identity theft is significantly prevalent in Nigeria. However, all sectors (government, industry, organizations, and individuals) have a role and responsibility in preventing it. Anti-fraud education awareness ought to be put in place to raise awareness of this issue. This section provides a review of professional and academic literature relevant to identity theft prevention and countermeasure strategies. Identity theft prevention and countermeasure are basically to secure the individuals' identity or financial documents: credit card, bank or loan accounts, etc., against being deceived or defrauded by other persons or a third person. Identity theft prevention and countermeasure are also implemented to secure organization system resources: hardware, software, data, and communication lines and networks and preserve the integrity, availability, and confidentiality of system resources. According to Golladay and Holtfreter (2017), users fall, victim to identity theft, when they disclose security details, such as their PIN or password, assume an email request or caller is genuine, allow them to be rushed into action, or fail to stay in control. There are several forms of identity theft usage: open bank accounts, get credit cards, loans, take over existing accounts, order goods in the victim's name, get passports, driving licenses and personal documents, etc.,

Identity theft is not a new crime. Despite the fact that many researchers have devoted much attention to identifying the factors that increase the risk of identity theft, little is known about the aftermath of victims. A few researches on identity theft have focused on predictors of victimization, reporting behaviors of the victims, and their health and mental outcomes. However, little remains known about the individuals who choose to take any identity-theft measures despite concerns over this fast-growing breed of crime (Ylang, 2020). Results from studies conducted by Golladay and Holtfreter (2017), indicated that among financial losses and loss of time, victims of identity theft also experience emotional (e.g., depression) and physical (e.g., poor health) symptoms, and withdrawal from certain transactions especially those one involving their bank accounts. In addition to the rising incidence of identity theft, there is growing recognition of the negative emotional and physical health consequences of financial crimes (Li, et al., 2019; Randa & Reyns, 2019). One in 10 identity theft victims, roughly 2.6 million people, reported experiencing severe emotional distress following victimization (Randa & Reyns, 2019). According to Golladay and Holtfreter (2017), the majority of identity theft victims experienced sleep problems, anxiety, and irritation six months after the crime, while older adults and minorities experience more severe emotional consequences including depression, anger, worry, and a sense of vulnerability.

Financial services in a Nigeria 2014 Survey report by Enhancing Financial Innovation and Access (EFInA) revealed that only 7.9% of Nigerians use ATMs and 53% of adults who are bank customers use their ATM cards. According to EFInA (2014), Nigerians are likely to be among the top population that stores money in their houses, rather than aligning to the ongoing cashless move (EFInA, 2014).

It is estimated that about 65% of the cash in circulation in the Nigerian economy is outside of the banking system (Emengini & Alio, 2014; Ezeamama, et al., 2014). One of the major reasons for this might be ignorance, illiteracy, and lack of trust in technology resulting from identity theft. If most people in the country understand and can use available technological innovations by themselves because it is easy-to-use, and trust them, this will be leveraging economic development and social change. Likewise, the knowledge of identity theft statistics and understanding of the threat and what measure is required for prevention and protection, is invaluable, especially in Nigeria where identity theft is high.

III. METHODOLOGY

In line with Hill and Burrows (2017), where analysis and synthesis of different and related research findings are required to draw holistic interpretations or conclusions based on the reviewers' own experience, existing theories and narrative review methodology is usually recommended and adopted. Also, a narrative study approach is best suited for studies described as qualitative rather than quantitative, and descriptive or explanatory in nature (Happel-Parkins & Azim, 2017). In this study, therefore, we adopted a narrative review methodology, where we reviewed, analyzed, and synthesized prior research findings. Narrative studies exhibit substantial strengths and acceptability in that they have the ability to provide platforms for comprehension of diverse and numerous understanding around scholarly research findings, and the opportunity to make reflective practice and acknowledgment of researchers' views and knowledge (Scarnato, 2017). Furthermore, reviews are done comparatively using multiple sources to gain multiple perspectives, maximize reliability and validation of data, and build coherent justification for interpretation and conclusion that relates to the study. This approach ensures reliability and validity of data, and justification of interpretations from the reviews.

IV. DATA COLLECTION

We reviewed vast professional and academic research findings that are relevant and related to identity theft prevention and recovery. Many of such research findings came from the Google Scholar and ScienceDirect databases and peer-reviewed journals, and other related texts. We as well used phrases such as "Identity theft", "Identity theft prevention", "consequences of identity theft", etc., as key search words in the databases for related literature. Reviews incorporated 44 references. Forty-two (95%) of total references incorporated in the study are peer-reviewed, while (61%) are peer-reviewed journals that are within the last 5 years.

V. ANALYSIS AND SYNTHESIS OF PRIOR RESEARCH

Cybersecurity security and some socio-technical trends that are likely to shape identity theft prevention and countermeasures have been identified (Computer Fraud & Security, 2016). Also identified are possibilities of these security measures to produce significant effects in the information security technical controls (Hinduja & Kooi, 2013). There have been enormous advances in the past, in the field of technical information security controls involving some complex and matured technical controls systems such as anti-virus, client-based firewalls, and real-time patching (Stewart & Lacey, 2012). There are also researches that have focused on individual fraud types: identity theft, intellectual property fraud, or insurance fraud. However Scholarly research in the area of identity fraud is difficult (Goode & Lacey, 2011). Studies of identity theft or fraud are hampered because it is difficult, if not impossible, to access offenders. Firms may be reluctant to admit experiencing security or fraud problem within their operations, while managers may resist inquiry or analysis from outside groups, including academic researchers to study their firms for fear of exposing their reputation to the public. This makes it difficult for external researchers to gain access to the organization's original, unsanitized data. This is a major reason why determining what contributes to information insecurity has proven to be complex in nature because such activities required to handle threats to the organizations' data: confidentiality, integrity, and availability are also complex (Fenz, et al., 2014).

Findings identified identity theft as the signature crime of the Information Technology age (Thomas, & Galligher, 2018; Zaeem, et al., 2017), with malicious programs, as one of the most preferred and effective vectors by phishers (Farina, K. (2015; Zaeem, et al., 2017). According to Nagunwa (2014), phishing provides a good platform for identity theft. Malware, empowered through spear-phishing techniques (Hille, et al., 2015), are being used by hackers to enable other malware, spy and stealing of identity information of their host users' data and possibly reconfigure and deny users access to the operating system (OS) or to some applications (Govindaraj, et al., 2018). It is therefore important that more research and information be engaged to help combat spear-phishing attacks and the resultant negative consequences such as ransomware and identity theft (Thomas, & Galligher, 2018). As stated by Thomas and Galligher (2018), one method to help combat identity theft that merits exploration is empowering users with preventive and countermeasure strategies to resist spear phishing attacks. Spear phishing is one of the highest challenges faced by IT departments in combatting identity theft (Goel, et al., 2017). Spear phishing is viewed as the entry point for many intrusions and hacking activities such as ransomware and identity theft, which are the two most damaging effects of spear-phishing injection (Collier, 2017). Although phishing attacks enable many different types of intrusion beyond identity theft, researchers have identified end-users and employee stakeholders as the most vulnerable point of entry for these attacks and have called for additional research to address these insurgents and growing problems (Hille, et al., 2015; Thomas & Galligher, 2018).

In spite of the vast adoption and implementation of advanced identity theft security technical controls, e-commerce users' payment information systems have remained vulnerable. This is because there is evidence that suggests that human vulnerabilities are increasingly exploiting users and organization information systems and increased identity theft (Stewart & Lacey, 2012). Some researchers have noted a number of reasons for this, ranging from problems with the usability of information systems (Cristian & Volkamer, 2013; Hartzog & Stutzman, 2013; Okesola & Grobler, 2014), compromised decisions by users (Greavu-Serban & Serban, 2014) and limited ability to comply with knowledge management systems or instructions (de Albuquerque & dos Santos, 2015; Shehata, 2015), poor knowledge sharing practices and learning processes, poor adherence to cyber-security policies, and high corruption practices (Anyaehie & Areji, 2015; Bennett, 2017). There is no uniformity in the implementation of strategies for user-centered system interface and improved literacy level (Aguboshim & Miles, 2018), agile learning processes and good knowledge sharing practices (Shah, et al., 2019), and excellent adherence to cyber-security policies designed to prevent identity theft especially in Nigeria (Aguboshim, et al., 2019; Olise, 2010). Nevertheless, strategies for prevention of identity theft can be achieved through brilliant security policies that mitigate spear phishing platforms, access control, and agile learning processes and good knowledge sharing practices that are proven core control method that empowers users to resist spear-phishing attacks help combat identity theft especially in Nigeria.

VI. CONCLUSION

There's no way to protect oneself against identity theft completely. Preventing identity theft and recovering from such theft justifies the ability to implement agile learning processes, good knowledge sharing practices (Shah, et al., 2019), and other cybercrime mitigation innovative activities and policies without which the ever-rising incidence of identity theft (Holt & Turner, 2012), will become excessively outrageous, and might diminish public confidence in government, organizations, and corporate entities, prompting increasingly restrictive access to government databases (Burnes, et al., 2020).

It is believed that no single strategic preventive tool can exploit the full security control and countermeasure for identity theft. Instead, a combination of different tools is required. Strategy for identity theft prevention and recovery technical control is a knowledgebase affair. What contributes to information insecurity has proven to be complex, dynamic, and more psychological in nature. Security measures need to be dynamic and versatile in order to handle complex security threats. Organizations' and users' data confidentiality, integrity, and availability are becoming complex, dynamic, and psychological. Perimeter defenses, control over devices, employee's adherence to policies, control over policy enforcement, and enterprise definitions are no longer reliable as all security platforms are complex, dynamic, and psychological. Attackers are personalizing their attacks. Security defenses must be personalized as well, with a holistic approach that expands beyond the technical security to include all arms of enterprise information systems security that comprised: agile learning processes, excellent knowledge sharing practices, and high, security policy and awareness, access control, and top-level management support, including the environment, the technology, and the people that could avert all forms of security breaches.

REFERENCES

[1]. Aguboshim, F. C., Ezeasomba, I. N., & Ezeife, J. E. (2019). Sustainable Information and Communication Technology (ICT) for Sustainable Data Governance in Nigeria: A Narrative Review. Journal of Information Engineering and Application (JIEA), 9(5), 15-20. https://doi.org/10.7176/jiea/9-5-02

[2]. Aguboshim, F. C., & Miles, G. S. (2018). Engaging pictorial images and voice prompts interface design strategy to create easy to use banking ATM system interfaces in Nigeria. International Organization of Scientific Research (IOSR-JMCA), 5(5), 11-22. https://doi.org/10.9790/0050-05051122

[3]. Anyaehie, M. C., & Areji, A. C. (2015).Economic Diversification for Sustainable Development in Nigeria. Open Journal of Political Science, 5(1), 87-94. https://doi.org/10.4236/ojps.2015.52010

[4]. Bennett, S. (2017). What is information governance and how does it differ from data governance? Governance Directions, 69(8), 462–467.

[5]. Burnes, D., DeLiema, M., & Langton, L. (2020). Risk and Protective Factors of Identity Theft Victimization in the United States. Preventive Medicine Reports, 5(2), 1-26 https://doi.org/10.1016/j.pmedr.2020.101058

[6]. Collier, R. (2017). NHS ransomware attack spreads worldwide. CMAJ, 189(22), 786-787. https://doi.org/10.1503/cmaj.1095434

[7]. Computer Fraud & Security. (2016). Identity theft rises sharply as fraudsters target social media. Computer Fraud & Security, 7, 1-3. https://doi.org/10.1016/S1361-3723(16)30048-3

[8]. Cristian, T. M., & Volkamer, M. (2013). Usable secure email communications: criteria and evaluation of existing approaches. Information Management & Computer Security, 21(1), 41-52.

[9]. de Albuquerque, A. j., & dos Santos, E. (2015). Adoption of information security measures in public research institutes/adoç'o de medidas de segurança da informaç'o em institutosde pesquisa p'blicos. Journal of Information Systems and Technology Management : JISTEM, 12(2) 289-315. https://doi.org/10.4301/S1807-17752015000200006

[10]. EFInA. (2014). EFInA access to financial services in Nigeria 2014 survey. http:// www.efina.org.ng/ assets/ResearchDocuments/2014-Documenst/EFInA-Access-to-Financial-Services-in-Nigeria-2014-Survey-Key-Findings.pdf

[11]. Emengini, S. E., & Alio, F. C. (2014). Cashless economy and financial statement reporting in Nigeria. European Journal of Accounting Auditing and Finance Research, 2(3), 1-9.

[12]. Ezeamama, M. C., Ndubuisi, N. J., Marire, M. I., & Mgbodile, C. C. (2014). The Impact of Central Bank of Nigeria Cashless Policy in Nigeria Economy. IOSR Journal of Business and Management (IOSR-JBM), 16(12), 84-95. https://doi.org/10.9790/487x-161218495

[13]. Farina, K. (2015). Cyber crime: Identity theft. International Encyclopedia of the Social and Behavioral Sciences, 633-637. https://doi.org/10.1016/B978-0-08-097086-8.45054-3

[14]. Federal Trade Commission. (1998). Identity Theft and Assumption Deterrence Act. Washington, DC: Federal Trade Commission; 1998. https://www.ftc.gov/node/119459

[15]. Fenz, S., Heurix, J., Neubauer, T., & Pechstein, F. (2014). Current challenges in information security risk management. Information Management & Computer Security, 22(5), 430-410. https://doi.org/10.1108/IMCS-07-2013-0053

[16]. Goel, S., Williams, K., & Dincelli, E. (2017). Got phished? Internet security and human vulnerability. Journal of the Association of Information Systems, 18(1), 22-44.

[17]. Golladay, K., &Holtfreter, K. (2017). The Consequences of Identity Theft Victimization: An Examination of Emotional and Physical Health Outcomes.Victims & Offenders, 12(5), 741-

760. https://doi.org/10.1080/15564886.2016.1177766

[18]. Goode, S., & Lacey, D. (2011). Detecting complex account fraud in the enterprise: The role of technical and non-technical controls. Decision Support Systems, 50(4), 702-714. ISSN 0167-9236.

[19]. Govindaraj, M., Prashant, R., & Pratheeksha, B. (2018). Behind Identity Theft and Fraud in Cyberspace: The Current Landscape of Phishing Vectors. International Journal of Recent Trends in Engineering and Research, 4(3), 585-597. doi:10.23883/ijrter.2018.4169.tpgpo

[20]. Greavu-Serban, V., & Serban, O. (2014). Social Engineering a General Approach. Informatica Economica, 18(2), 5-14. https://doi.org/10.12948/issn14531305/18.2.2014.01

[21]. Happel-Parkins, A., & Azim, K. A. (2017). She Said, She Said: Interruptive Narratives of Pregnancy and Childbirth. Forum: Qualitative Social Research, 18(2), 16-21.

[22]. Hartzog, W., & Stutzman, F. (2013). Obscurity by design. Washington Law Review, 88(2), 385-418.

[23]. Hill, C., & Burrows, G. (2017). New voices: The usefulness of a narrative approach to social work research. Qualitative Social Work: Research and Practice, 16(2), 273-288. https://doi.org/10.1177/1473325017689966

[24]. Hille, P., Walsh, G., & Cleveland, M. (2015). Consumer fear of online identity theft: Scale development and validation. Journal of Interactive Marketing, 30(1), 1-19. doi:10.1016/j.intmar.2014.10.001

[25]. Hinduja, S., & Kooi, B. (2013). Curtailing cyber and information security vulnerabilities through situational crime prevention. Security Journal, suppl. Special Issue: Security in a digital world: Understanding, 26(4), 383-402. https://doi.org/10.1057/sj.2013.25

[26]. Holt, T. J., &Turner, M. G. (2012).Examining Risks and Protective Factors of On-Line Identity Theft. Deviant Behavior, 22(4), 308-323. https://doi.org/10.1080/01639625.2011.584050

[27]. Koops, B. J., & Leenes, R. (2006). Identity theft, identity fraud and/or identity-related crime. Datenschutz und Datensicherheit-DuD, 30(9), 553-556. https://doi.org/10.1007/s11623-006-0141-2.

[28]. Li, Y., Yazdanmehr, A., Wang, J., & Rao, H. R. (2019). Responding to identity theft: A victimization perspective. Decision Support Systems, 121(1), 13-24. https://doi.org/10.1016/j.dss.2019.04.002

[29]. Nagunwa, T. (2014).Behind Identity Theft and Fraud in Cyberspace: The Current Landscape of Phishing Vectors. International Journal of Cyber-Security and Digital Forensics (IJCSDF) 3(1), 72-83.

[30]. Okesola, J. O., & Grobler, M. (2014). Developing a secured social networking site using information security awareness techniques. South African Journal of Information Management, 16(1), 1-6. https://doi.org/10.4102/sajim.v16i1.607

[31]. Olise, F. P. (2010). Information and Communication Technologies (ICTs) and Sustainable Development in Africa: Mainstreaming the Millennium Development Goals (MDGs) into Nigeria's Development Agenda. Journal of Social Sciences, 24(3), 155-167.

[32]. Randa, R., & Reyns, B. W. (2019). The Physical and Emotional Toll of Identity Theft Victimization: A Situational and Demographic Analysis of the National Crime Victimization Survey. Deviant Behavior, 1-15. https://doi.org/10.1080/01639625.2019.1612980

[33]. Reyns, B. W. (2013). Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses. Journal of Research in Crime and Delinquency, 50(2), 216–238. https://doi.org/10.1177/0022427811425539

[34]. Reyns, B. W., & Henson, B. (2016). The thief with a thousand faces and the victim with none: Identifying determinants for online identity theft victimization with routine activity theory. International journal of offender therapy and comparative criminology, 60(10), 1119–1139. https://doi.org/1177/0306624X15572861

[35]. Scarnato, J. M. (2017). The value of digital video data for qualitative social work research: A narrative review.Qualitative Social Work: Research andPractice,https://doi.org/10.1177/1473325017735885

[36]. Shah, M., Maitlo, A., Jones, P., & Yusuf, Y. (2019). An investigation into agile learning processes and knowledge sharing practices

to prevent identity theft in the online retail organisations. Journal of Knowledge Management, 23(9), 1857-1884. https://doi.org/10.1108/jkm-06-2018-0370

[37]. Shehata, G. M. (2015). Leveraging organizational performance via knowledge management systems platforms in emerging economies: Evidence from the Egyptian Information and Communication Technology (ICT) industry. VINE, 45(2), 278-239. https://doi.org/10.1108/vine-06-2014-0045

[38]. Stewart, G., & Lacey, D. (2012). "Death by a thousand facts", Information Management & Computer Security, 20(1), 29-38. doi:10.1108/09685221211219182

[39]. Thomas, J. E. (2018). Individual Cyber Security: Empowering Employees to Resist Spear Phishing to Prevent Identity Theft and Ransomware Attacks. International Journal of Business and Management, 13(6), 1-14.https://doi.org/10.5539/ijbm.v13n6p1

[40]. Thomas, J. E., & Galligher, G. C. (2018). Improving backup system evaluations in information security risk assessments to combat ransomware. Computer and Information Science, 11(1), 14-25. https://doi.org/10.5539/cis.v11n1p14

[41]. UNESCO. (2015). Data center. Retrieved from http://www.uis.unesco.org/DataCentre/Pages/country-profile.aspx?regioncode=40540&code=NGA

[42]. Wall, D. S. (2013). Policing identity crimes. Policing and Society, 23(4), 437?460. https://doi.org/10.1080/10439463.2013.780224

[43]. Ylang, N. (2020). Capable guardianship against identity theft: Demographic insights based on a national sample of US adults. Journal of Financial Crime, 9(1), https://doi.org/10.1108/JFC-12-2018-0140

[44]. Zaeem, R., Mnaoharan, M., Yang, Y., & Barber, K. (2017). Modeling and analysis of identity threat behaviors through text mining of identity theft stories. Computers & Security, 65, 50-63. https://doi.org/10/1016/j.cose.2016.11.02

International Journal of Advances in Engineering and Management
ISSN: 2395-5252

IJAEM

Volume: 03 Issue: 01 DOI: 10.35629/5252

www.ijaem.net

Email id: ijaem.paper@gmail.com