International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 2 Feb 2021, pp: 37-43 www.ijaem.net ISSN: 2395-5252

Strategies for Enhancing ICT Innovations System Security in Nigeria

Dr. Felix. C. Aguboshim
Principal Lecturer, Department of Computer Science, Federal Polytechnic, Oko Nigeria.

Submitted: 25-01-2021 Revised: 05-02-2021 Accepted: 10-02-2021

ABSTRACT: Information and Communication Technology (ICT) innovations are becoming ubiquitous and pervasive, being applied rapidly in all facets of life. Achieving secure enterprise information systems have become more complex and have further made the CIA triad: confidentiality, integrity, and availability of organizations' data become insecure, and prone to breaches and fraudulent activities. For this study, the Enterprise Information Systems (EIS) security conceptual framework was adopted that comprised: security policy, security awareness, access control, and top level management support. The author explored a narrative review of vast works of literature that revealed significant information on conceptual framework and existing systems that enhance ICT innovations security, analysis and synthesis of prior research. Findings of the study show that breaches and fraudulent activities exist that may be perpetrated against ICTs, such as Skimming attacks, phishing/vishing attack, hacking, and physical attack, etc. Also, systems strategies that enhance ICT security exist within the implementation of procedures, policies, resources, and operations to mitigate certain security threats, vulnerabilities, and risks. Result from this study may bring trust and increase ICT adoption rate, new innovation and influence that may advance ICT technology innovations.

Keyword: ICT innovations, CIA triad, ICT security function, security threats, vulnerabilities and risks

I. INTRODUCTION

Globally, the use of internet-enabled devices, and the availability of high speed ICT systems and large datasets have facilitated productivity, efficiencies, and capabilities across all major industries and organizations. ICT is increasingly recognized as enablers of modern technology-dependent innovations to improve the lives of people everywhere (Cotter, 2018), for productivity, empowerment, and economic development in any society.Technology, though complex and modern, has become enablers of enablers (Silic & Back, 2014), enabled in a complex interconnectivity platform that makes people rely extensively on technology(Fenz, Heurix, Neubauer, & Pechstein, 2014), but seemingly opened up avenues for theft, fraud and other forms of security threats by offenders who might even come from within the organization (Nasir, Wu, Yago, & Li, 2015).ICT innovations are becoming ubiquitous and pervasive, being applied rapidly in all facets of life. This ubiquitous and pervasive use of internet-enabled devices have brought with it new cyber security challenges and significant security risks (Nasir, et al., 2015). The rapid IT impacts on ICT systems and of internet-enabled devices are being accompanied by a corresponding rise in network security breaches resulting in big losses to the industry, bringing with it fierce security challenges (Nasir, et al., 2015).

It is estimated that more than 20 billion devices are expected to be connected to the Internet by 2020 (Allassani, 2014). The risks introduced by the growing number and variety of such devices are substantial.Innovations systems securities have been identified as important strategies for sustainable productivity and empowerment of any organization that is ICT dependent (Oladimeji & Foltyn, 2018). As a result of these complex security risks, the need for information security to protect organizations' network and data becomes more relevant (Allassani, 2014). Information security can provide technical solutions such as Multi-Sensor Cameras systems that are now integrated with mobile devices, apps, and networked interfaces to be viewed remotely from any location, with an ability to see 360 degrees around an area and pinpoint where potential intrusions are located. Other security solutions include Drones, which provide great way to survey a large area or a dangerous facility, and a Two-Factor Authentication that provides the way for companies to keep their networks secure in addition to intrusion detection system, anti-virus software, firewall systems, and cryptology (Allassani, 2014)

In addition, the behavior and activities of their employees are influenced and manage through information security policies on the use of ICTs and computer systems. Organizations can make information security more effective through regular training of their employees. Information Technology is, therefore, encompassing, involving its access, storage, processing, and transmission (Allassani, 2014).

Achieving secure ICT systems is complex in nature because it demands a well-designed and well-developed structure that enables reliable physical and logical connection between different systems. ICT system involves software, hardware, and concepts such as data protocols that control the interactions between systems. Technology alone, therefore, cannot solve ICT security problems until we understand technology and the problems (Stallings & Brown, 2012). This is because the man appears to be the most important links to the information security of any organization, and invariably constitutes the highest risk to the information security measures and information integrity of any organization (Stallings & Brown, 2012). The user is often the weakest link in the security of a system. Many security breaches are caused by weak passwords, unencrypted files left on unprotected systems. This is why security breaches have been on the increase, involving both small and large organizations, despite the advancement in technology (Fenz, et al., 2014).For instance, Astakhova (2015) cited some eloquent figures from InfoWatch Analytical Center, in the first half of the year that recorded 654 cases of leakage of confidential information, which was 32% more than what it was in the previous year, while 71% of them were employees of companies. Additionally, these threats are not effectively and efficiently mitigated (Silic & Back, 2014).

Therefore, determining what contributes to information insecurity and secure ICT system is of paramount importance to in this study, particularly in the implementation of activities that mitigate threats to the organizations' data: confidentiality, integrity, and availability (Fenz, et al., 2014).Secure ICT system must be within the conceptual frameworks that leverage confidentiality, integrity, and authentication (Stallings & Brown, 2012). A conceptual framework for secure ICT system is considered for computer security that included among others: availability, access control, and privacy. According to Fenz, et al. (2014), these can be viewed from its five distinct functional areas: prevention, deterrence, risk avoidance, detection, and recovery; and defined in terms of several interdependent domains: physical and personnel security, system security, operational or procedural security, and network.

In this paper, the author established some strategies for implementing a secured ICT Innovations system that may impact data trustworthiness, accountability and compliance especially with users (Bertino, et al., 2014). Strategies do not seek to address all of these risks. They are focused on the availability, integrity and confidentiality of organization's ICT. However, it is essential that it works in harmony with other related policies and programs, including cyber safety, identity security and privacy.This study seeks to implement the activities that can handle threats to the ICT Innovations organizations' data: confidentiality, integrity, and availability within the operations of the ICT secure system (Fenz, et al., 2014). It also seeks to implement secure ICT system that will present a functional ICT system operation, that is clear, safe, concise, familiar, responsive, consistent, attractive, enjoyable, efficient, and forgiving, and reliable to handle every ICT service delivery to customers. Secure ICT system will attract more customer to use ICTs which in turn, will cause organizations to enjoy additional revenue, high levels of customer satisfaction, investment opportunities, cost savings, effective service delivery, and competitiveness (Jegede, 2014).

It is anticipated that findings from this study may encourage social change as more ICT systems are likely to be secured to leverage ICT Innovations customers' confidence, improve user morale, preference, attraction, and productivity, and also increase the use of ICT in companies and organizations globally. Additionally, a successful ICT system use though will attract diverse security breaches. Offense informs defense, therefore the knowledge of the flaws or intending flaws and the workaround can inform and constitute part of the intelligent countermeasures constructed to build effective and persistent defenses. Also continuous measurement to test, audit, and validate the effectiveness of the ongoing security measures can form significant mitigations or countermeasures against intending attacks. This will no doubt create new innovation and influence that will impact more researches on ICT Innovations secure systems and advance the use of ICT technology.

1.1 Problem Statement

Security breaches among ICT Innovations have been on the increase despite the advancement in technology (Fenz, et al., 2014). Astakhova (2015) cited some eloquent figures from InfoWatch

Analytical Center, in the first half of the year that recorded 654 cases of leakage of confidential information, which was 32% more than what it was in the previous year, while 71% of them were employees of companies. These threats are not effectively mitigated to efficient handle threats to the organizations' data: confidentiality, integrity, and availability (Fenz, et al., 2014; Silic & Back, 2014).ICT Innovations security functions should include policies, resources, activities, operations and implementation procedures defined to mitigate most security threats, vulnerabilities, and risks. The general IT problem is the implementation of procedures, policies, resources, activities, and operations to mitigate most security threats, vulnerabilities, and risks. The specific IT problem is that some IT managers of ICT Innovations security function lack strategies to mitigate most security threats, vulnerabilities, and risks of ICT Innovations systems.

II. LITERATURE REVIEW

ICT system users are driven to use the system based on their perceived trust level, which determines their use of the system (Cottrell, 2016). Human failings also can undermine even the strongest security countermeasures (Taylor & Robinson, 2015), because what contributes to information insecurity has proven to be complex, dynamic and more of psychological in nature (Cottrell, 2016; Fenz, et al., 2014). Security measures required to handle threats to the organizations' data: confidentiality, integrity, and availability are also 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 in reality there are no perimeter boundaries, but all security platforms are complex, dynamic and psychological (Allassani, 2014). Attackers are personalizing their attacks, but defenses are not been personalized (Allassani, 2014). Information security has been defined from a multiple perspective (Narain, Gupta, & Ojha, 2014) and with a holistic approach that expands beyond the technical security (Perez, Branch, & Kuofie, 2014), to comprise the environment, the technology, and the people (Stallings & Brown, 2012; Taylor & Robinson, 2015).

A significant number of empirical researches point to the fact that humans appear to be the most important links to the information security of any organization, and invariably constitute the highest risk to the information security measures and information integrity of any organization (Stallings & Brown, 2012). This is because of the differences in behavior regarding the intent to implement security measures or administrative errors.Taylor and Robinson (2015) reported a security incident where members of a financialInstitution's credit card numbers and information were stolen. Investigations carried out involved the three components of information security system as identified by Stallings and Brown (2012), and Taylor and Robinson (2015): the environment, the technology, and the people. In this case, security breach did not come from the technical nor the environment or external but from the apparently overlook of the important and critical role that people play in maintaining system security. The cleaner staff had thrown away customers' credit card numbers and information that was left littered on the floor to the dustbin outside. This gave hackers the information cheaply to attack the organization. The breach points to a lapse in information system security, which is not the same as technology security (Taylor & Robinson, 2015). Violations of established security safeguards by insiders led to information system security incidents. Management putting in place good policies coupled with good formulation and communication of same, information security policies intentions, principles, rules and guidelines which should be adhered could have averted the security breach (Sommestad, Hallberg, Lundholm, & Bengtsson, 2014).

2.1 Conceptual Framework

For this study, the Enterprise Information Systems (EIS) security was adopted as the conceptual framework that comprised: security policy, security awareness, access control, and top level management support.Information security policies are set of rules, standards, practices, and procedures set up by an organization to maintain a secure IT system. The credibility of the entire information security program of an organization depends upon a well-defined information security policy (ISP) to actualize work-related groups that influence individuals' decision-making (Sommestad, 2018). Policy gaps are the foundation of most security failures (Aguboshim & Udobi, 2019). Researchers believe that developing a well-defined information security policy is one of the most practical ways to preserve protected systems (Choi, 2019; Kajtazi, Cavusoglu, Benbasat, &Haftor, 2018), and the first step toward preparing an organization against attacks from internal and external sources. Ineffective implementation of security policy may lead to weaknesses in enterprise information systems security.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 2 Feb 2021, pp: 37-43 www.ijaem.net ISSN: 2395-5252

However, the focus should shift more toward organization-specific information security needs, because there is still lacking contributions that would show how contextual factors could be successfully integrated into ISP development (Paananen, Lapke, &Siponen, 2019). Supportive organizational factors such as culture and end-user involvement significantly influence employees' attitudes towards compliance with ISP (Amankwa, Loock, &Kritzinger, 2018). However, leadership appears to exhibit the weakest influence on attitudes towards compliance with ISP (Alshare, Lane, & Lane, 2018). Overall, employees' attitudes and behavioural intentions towards ISP compliance together influenced the establishment of information security compliance in organizations. While security policies, procedures, and controls are the most implemented security measures, Allassani (2014) claimed that they are not the most effective in information security

III. METHODOLOGY

A narrative review approach was adopted in this study to review significant information on the conceptual framework, existing systems that enhance ICT system security, analysis, and synthesis of prior research. A narrative study approach is best suited to a study that can be described as descriptive or explanatory (Bell, 2017; Privizzini, 2017), and where summaries of different primary studies from which conclusions may be drawn into a holistic interpretation contributed by the reviewers' own experience, existing theories and models are needed. Results from narrative studies are of a qualitative rather than a quantitative meaning (Scarnato, 2017). The strengths of narrative study are in its ability to comprehend the diverse and numerous understanding around scholarly research topics and the opportunity to speak with self-knowledge, reflective practice and acknowledgement of shared views and knowledge (Malcolm, 2017). In this paper, I lay out more clearly the methodological commitments of narrative inquiry. Within narrative inquiry, I have made the search criteria and the criteria for inclusion explicit. This study'sreview process included key words and term identification, article identification, quality assessment, data extraction, and data synthesis. Methodological triangulation is the use of multiple sources of data that pertains to a case or phenomenon, to gain multiple perspectives, maximize reliability and validation of data and build coherent justification of data interpretation (Durif-Bruckert, et al., 2014). I adopted methodological triangulation to ensure the reliability and validity of data, and justification of interpretations from the reviews.

IV. DATA COLLECTION

This review was based on a literature search of online information obtained from the following international library databases: the ProQuest databases, ScienceDirect, Walden University collection of scholarly and peer-reviewed journals, and other related texts. A combination of phrases and terms were used as key search words in the databases for related literature on strategies for enhancing ICT system security in Nigeria. Such phrases and terms included informationsystem security, ICT security function, ICTsecurity threats, cyber-attacks and security, major determinants of EIS, and many others. We conducted a thorough review of the literature and incorporated 33 references into this study. Thirty one (94%) of total references incorporated in the study arepeer-reviewed, while (91%) are peer-reviewed journals that are within the last 5 years.

V. ANALYSIS AND SYNTHESIS OF PRIOR RESEARCH

Over the years there have been enormous advances in the field of technical information security controls with complex and matured technical controls such as anti-virus, client-based firewalls, and real-time patching. Some socio-technical trends that are likely to shape the cyber security environment in the next decade have been identified (Dupont, 2013), and their possibility to produce a great effect in the information security technical controls observed. These trends, according to Dupont (2013), are cloud computing; big data (Hartzog & Stutzman, 2013); the Internet of Things; the mobile internet or mobile computing; brain-computer interfaces, mobile robots; quantum computing, and the militarization of the internet. These trends come with their challenging needs and requirements for more data, more connections, more movement, and flows. As a result of this massive data storage and interconnectivity, organizational data and information are exposed to more opportunities for malicious exploitation and threats, less security, and less control. The occurrence of disasters, operation errors, and oversights, further increase the risks placed on information systems.

Much prior research has also focused on individual fraud types: identity theft, intellectual property fraud or insurance fraud. However Scholarly research in the area of fraud is difficult. Studies of financial 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 is one of the reasons 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).

Despite the implementation of advanced security technical controls, information systems have remained vulnerable. This is because there is evidence that suggests that human vulnerabilities are increasingly exploiting information systems . Some researchers have noted a number of reasons for this, ranging from problems with the usability of information systems (Hartzog & Stutzman, 2013), compromised decisions by users (Greavu-Serban & Serban, 2014) and limited ability to comply with Knowledge Management Systems or instructions (de Albuquerque & dos Santos, 2015). However, Dwivedi, et al. (2015) summarized and categorized these mistakes into four categories: process (management process and technical project management methodologies), people involved in a project, product (project size and urgency, including its goals, performance, robustness, and reliability), and technology (IS failures resulting from the use and misuse of modern technology). Nevertheless, Study by Ho, Hsu, and Yen (2015) has provided an improvement strategy to manage the Information Security Management (ISMS) of the organization by proposing three core control items of the Information Security Management (ISMS) namely security policy, access control, and human resource security.

VI. CONCLUSION

The main objective of this study was to inform IT, managers of information security function, the strategies to withstand most security threats, vulnerabilities, and risks of ICT systems. What contributes to information insecurity has proven to be complex, dynamic and more of psychological in nature. Security measures need to be complex in order to handle the complex security threats. Organizations' 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 the environment, the technology, and the people There are differences in behavior intent towards implementation of security measures.

IT managers of ICT security systems must put in place good policies coupled with good formulation and communication of same, EIS securitypolicy, security awareness, access control, and top level management support which should be adhered that could avert all forms of security breaches.

REFERENCES

[1]. Aguboshim, F. C., & Udobi, J. I. (2019).Security issues with mobile IT: A Narrative Review of Bring -Your-Own-Device (BYOD). Journal of Information Engineering and Application (JIEA), 9(1), 56-66. doi:10.7176/jiea/8-1-070

[2]. Allassani, W. (2014).Determining factors of bank employee reading habits of information security policies.Journal of Information Systems and Technology Management, 11(3), 533-548. doi:10.4301/S1807-17752014000300002

[3]. Alshare, K. A., Lane, P. L., &Lane, M. R. (2018).Information security policy compliance: a higher education case study. Information and Computer Security, 26(1), 91-108doi:10.1108/ics-09-2016-0073

[4]. Amankwa, E., Loock, M., &Kritzinger, E. (2018).Establishing information security policy compliance culture in organizations.Information and Computer Security, 26(4), 420-436. doi:10.1108/ics-09-2017-0063

[5]. Astakhova, L. V. (2015). Information security: Risks related to the cultural capital ofpersonnel (Review). Scientific and Technical Information Processing, 42(2), 41-52.doi:10.3103/S0147688215020021

[6]. Bell, E. E. (2017). A Narrative Inquiry: A Black Male Looking to Teach. The Qualitative Report, 22(4), 1137-1150.Retrieved from http://nsuworks.nova.edu/tqr/vol22/iss4/12

[7]. Bertino, E., Ghinita, G., Kantarcioglu, M., Nguyen, D., Park, J., Sandhu, R., …Xu, S. (2014). A roadmap for privacy-enhanced secure dataprovenance.Journal of Intelligent Information Systems, 43(3), 481-501.doi:10.1007/s10844-014-0322-7

[8]. Choi, Y. (2019). Organizational Control Policy, Information Security Deviance, and Moderating Effect of Power Distance Orientation.International Journal of Cyber Behavior, Psychology and , 9(3), 48-60. doi:10.4018/ijcbpl.2019070104

[9]. Cotter, C. (2018).ICTs as an Antidote to Hardship and Inequality implications for New Zealand Policy Quarterly, 14(2), 80-87

[10]. Cottrell, L. (2016). IoT problems are about psychology, not technology. Retrieved fromhttp://www.tripwire.com/state-of-security/security-data-protection/iot/iot-problems are-about-psychology-not-technology/

[11]. de Albuquerque, A. j., & dos Santos, E. (2015). Adoption of information security measures inpublic 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. doi:10.4301/S1807-17752015000200006

[12]. Dupont, B. (2013). Cybersecurity Futures: How Can We Regulate Emergent Risks?Technology Innovation Management Review, 3(7), 6-11.

[13]. Durif-Bruckert, C., Roux, P., Morelle, M., Mignotte, H., Faure, C., &Moumjid-Ferdjaoui, N. (2014).Shared decision-making in medical encounters regarding breast cancer treatment: the contribution of methodological triangulation.European Journal of Cancer Care, 24(4), 461-472. doi:10.1111/ecc.12214

[14]. Dwivedi, Y., Wastell, D., Laumer, S., Henriksen, H. Z., Myers, M. D., Bunker, D., …Srivastava, S. C. (2015). Research on information systemsfailures and successes: Status update and future directions. Information SystemsFrontiers, 17(1), 143-157. doi:10.1007/s10796-014-9500-y

[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.doi:10.1108/imcs-07-2013-0053

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

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

[18]. Ho, L., Hsu, M., & Yen, T. (2015). Identifying core control items of information security management and improvement strategies by applying fuzzy DEMATEL.Information and Computer Security, 23(2), 161-177. doi:10.1108/ics-04-2014-0026

[19]. Jegede, C. A. (2014). Effects of automated teller machine on the performance of Nigerian banks. American Journal of Applied Mathematics and Statistics, 2(1), 40-46.doi:10.12691/ajams-2-1-7

[20]. Kajtazi, M., Cavusoglu, H., Benbasat, I., &Haftor, D. (2018).Escalation of commitment as an antecedent to noncompliance with information security policy.Information and Computer Security, 26(2), 171-193doi:10.1108/ics-09-2017-0066

[21]. Malcolm, P. M. (2017). Peer support in mental health: a narrative Review of its relevance to social work. Egyptian Journal of Social Work, 4(1).19-40. doi:10.21608/ejsw.2017.8725

[22]. Narain, S. A., Gupta, M. P., & Ojha, A. (2014). Identifying factors of "organizationalinformation security management. Journal of Enterprise Information Management, 27(5), 667-644.doi:10.1108/jeim-07-2013-0052

[23]. Nasir, M. A., Wu, J., Yago, M., & Li, H. (2015). Influence of Psychographics and Risk Perception on Internet Banking Adoption: Current State of Affairs in Britain. International Journal of Economics and Financial Issues, 5(2), 461-468.

[24]. Oladimeji, T. T., & Foltyn, G. B. (2018). ICT and Its Impact on National Development In Nigeria: An Overview. Research & Reviews: Journal of Engineering and Technology, 7(1), 1-10.

[25]. Paananen, H., Lapke, M., &Siponen, M. (2019).State of the Art in Information Security Policy Development.Computers & Security, 10(1), 10-16. doi:.1016/j.cose.2019.101608

[26]. Perez, R. G., Branch, R., & Kuofie, M. (2014).EOFISI Model as a Predictive Tool to Favor Smaller Gaps on the Information Security Implementations.Journal of Information Technology and Economic Development, 5(1), 1-20.

[27]. Privizzini, A. (2017).The Child Attachment Interview: A Narrative Review. Frontiers in Psychology,8(1),doi:10.3389/fpsyg.2017.00384

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

[29]. Silic, M., & Back, A. (2014). Information security.Information Management & Computer Security, 22(3), 279-308. doi:10.1108/IMCS-05-2013-0041

[30]. Sommestad, T. (2018).Work-related groups and information security policy compliance.Information and Computer Security, 26(5), 533-550. doi:10.1108/ics-08-2017-0054

[31]. Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. (2014). Variables influencinginformation security policy compliance: A systematic review of quantitative studies. Information Management & Computer Security, 22(1), 42-75. doi:10.1108/imcs-08-2012-0045

[32]. Stallings, W., & Brown, L. (2012). Computer security: Principles and practice (2nd ed.).Upper Saddle River, NJ: Prentice Hall.

[33]. Taylor, R. G., & Robinson, S. L. (2015). An information system security breach at FirstFreedom Credit Union 1: what goes in must come out. Journal of the InternationalAcademy for Case Studies, 21(1), 131-138.

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

IJAEM

Volume: 03 Issue: 02 DOI: 10.35629/5252

www.ijaem.net
Email id: ijaem.paper@gmail.com