MANAGING ORGANISATION INFORMATION SECURITY SYSTEMS, CONFLICTS, AND INTEGRITY FOR SUSTAINABLE AFRICA TRANSFORMATION

IfeyinwaNkemdilim, Obiokafor [1]; Dr Felix. C. Aguboshim [2] and Chukwuka Sunday Nwajikwa[3]

[1] Lecturer, Department of Computer Science Technology, Anambra State Polytechnic, Mgbakwu. Nigeria ifykems@gmail.com; +2348038843496.

[2] Chief Lecturer, Department of Computer Science, Federal Polytechnic, Oko Nigeria

[3]Programme Analyst, Anambra State Polytechnic, Mgbakwu Nigeria

Abstract

The widespread dependence of business organisations on technological advancements for digital file-sharing networks across all business transactions puts organisation system companies to additional security dangers. In all countries, staff devotion to security rules compliance, organisation clarifications and efficient administration of organisation security systems are directly related. Despite massive cyber-security advancements, the security measures necessary to tackle threats to organisations' data which are confidentiality, integrity, and availability are becoming sophisticated, fluid, psychological but mainly underdeveloped, outmoded, and non-sustainable in Africa. This study reveals gaps in organisational information security system management, issues and authenticity resulting from insufficient personnel compliance with security laws and regulations, as well as strategies to remedy them. The researchers did an in-depth review of current research, which yielded valuable information on approaches for controlling organisational information security systems. Peer-reviewed publications over the past five years were retrieved from electronic databases using relevant search terms. According to the findings, effective compliance with security standards, responsibility over policy execution, and enterprise definitions can prevent or reduce organisational security risks. The outcomes of the study might be utilised to enhance excellent security management practices and preventative approaches for Africa's growth.

Keyword: *Security enterprise definition, Security threats, Confidentiality, Integrity and availability, Identity theft solution, enterprise security policies*

1. Introduction

Human failings can undermine even the strongest security countermeasures (Taylor & Robinson, 2015) because what contributes to information insecurity has proven to be complex, dynamic and even more of psychological (Cottrell, 2016) in nature (Fenz, et al., 2014; Olusegun &Ithnin, 2013). The activities required handling threats to the organisations' data confidentiality, integrity and availability are also complex, dynamic, and psychological. Perimeter defences, control over devices, employees' adherence to

policies, control over policy enforcement, and enterprise definitions are no longer reliable as the reality is that there are no perimeter boundaries, but all security platforms are complex, dynamic, and psychological (Thompson, 2013). Attackers are personalizing their attacks, but defences are not being personalized (Thompson, 2013).

Information security has been defined from multiple perspectives (Narain, et al., 2014) and with a holistic approach that expands beyond the specialized security (Perez, et al., 2014), to comprise the terrain, the technology, and the people (Stallings & Brown, 2012; Taylor & Robinson, 2015). Major empirical research indicates that individuals seem to be the most significant contributors to any organization's information security, and they always pose the greatest risk to any organization's information security measures and information integrity (Stallings & Brown, 2012). This is because exploits differ in their goal to deploy security measures or commit executive crimes (Komatsu et al., 2013).
Taylor and Robinson (2015) reported a security concern involving employees of a financial institution's credit card numbers and information which were stolen. Investigations carried out involved the three components of information security systems as identified by Stallings and Brown (2012), and Taylor and Robinson (2015): the environment, the technology, and the people. There was no technical or environmental breach in this case but rather, it was the apparent neglect of the important and critical role that people play in maintaining system security. Customers' credit card details and information that had been left scattered on the floor had been tossed away to the dust bin outside by the cleaners. This provided hackers with a low-cost means of attacking the bank. 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, et al., 2014).

The information system of today includes technology, the environment, and people (Stallings & Brown, 2012; Taylor & Robinson, 2015). Therefore, delivering Security Education Training and Awareness (SETA) should reflect the principles of Information security that aims to protect the business function of the organization, the information, and knowledge of the organization irrespective of where it may be stored and transmitted, and essentially reflect a people's understanding of security policies and implementation that has some technical solutions (Ahmad & Maynard, 2014). However, modifying human behaviour through training is hard; some battle-worn security executives might even dismiss it as impossible (Thompson, 2013). SETA will be effective to correct breaches that could result from unintentional errors. Effectiveness can be measured through regular auditing and implementation of corrective checks, analytics tool, to

prevent the enterprise's fate from ever coming down to a click/no-click decision (Thompson, 2013).

2. Literature Review

Organisational information security systems, conflicts, and integrity management for long-term Africa change requires the study of the information security specialized controls, analysis, and conflation of previous inquiries, successes, problems, as well as how improved generalisations and methods may be leveraged to reduce information security hazards and failings. Security of information systems is a top priority in any organisation or government, particularly in Africa. In Africa, information systems are subject to a variety of problems that can result in significant harm and losses such as frauds that alter database integrity to explosions that destroy, perhaps, the entire system's centres. Losses might occur as a result of seemingly trustworthy employees scamming a system, hackers or sloppy data input. In broad terms, security breaches can occur if data integrity circumstances, systems-trustability scenarios are not in sync with the sensitivity of the information reused; when there are errors or disruption in implementing and sustaining operational strategies in sync with the importance of stoner information processing terms; or when information system security programmes and programme management are neglected.

2.1 Analysis and Conflation of Previous Exploration

Over the years, there have been great developments in the field of specialised information security measures, such as anti-virus, customer-grounded firewalls, and real-time doctoring (Stewart & Lacey, 2012). According to Dupont (2013), some socio-specialized patterns that are expected to affect the cyber security landscape in the following years have been identified. In addition to that, their abilities to produce great impact relating to specialized controls in information security have also been found (Hinduja &Kooi, 2013). In the past few years, the IEEE Security and Sequestration Society has focused on a wide range of essential programmes which have not only led to improved knowledge of security but has also brought about creative and successful outcomes of information specialized security problems (Pfleeger, et al., 2010). These trends, according to Dupont (2013) and Hartzog& Stutzman, (2013), are pall computing, big data the internet of effects, the mobile internet or mobile computing, brain-computer interfaces, mobile robots, amount computing and the demilitarization of the internet. These developments come with arduous prerequisites and circumstances for additional data, connections, mobility and fluxes. A consequence of this vast data repository and interconnectedness is that organisational data and information become vulnerable to additional opportunities for vicious misuse and hazards, as well as reduced security and control (Montesino & Fenz, 2011). The occurrence of catastrophes, operational crimes, and mistakes increases the risks posed to information systems.

Previous research has also focused on particular fraud types such as identity theft, intellectual property fraud, and insurance fraud. Nonetheless, scholarly investigation of fraud is sensitive (Goode & Lacey, 2011). Studies of fiscal fraud are impeded since piercing malefactors is difficult, if not impossible. Companies may be hesitant to disclose passing security or fraud issues within their business operations, while executives may resist outside investigation or analysis, including academic experimenters to examine their companies for the dread of revealing their inner workings to the general. It is also delicate for external experimenters to gain access to the association's original, un-sanitized data. This explains why understanding the reasons behind information instability has proven to be complicated (Fenz et al., 2014), because comparable training is required to deal with hazards to the associations' data secrecy, integrity and vacuity.

Information systems have remained susceptible despite the implementation of modern security specialised measures. This is because evidence suggests that deadly vulnerabilities are being exploited less frequently in information systems (Stewart & Lacey, 2012). Some researchers have identified a variety of causes for this, including issues with information system usability (Cristian &Volkamer, 2013; Hartzog& Stutzman, 2013; Okesola & Grobler, 2014), compromised opinions by druggies (Greavu-Serban & Serban, 2014) and limited capability to misbehave with Knowledge Management Systems or instructions (de Albuquerque & dos Santos, 2015; Shehata, 2015). Still, Dwivedi, et al (2015) note that these errors were encapsulated and dispersed into four categories which are operation process and specialised design operation techniques, individuals involved in a design, product (design size and urgency, including its assertions, efficiency, stability, and trustworthiness), and technology (its faults caused by the exploitation and abuse of cutting-edge technology). However, a study conducted by Ho et al. (2015) provided enhanced approaches for managing the association's Information Security Management (ISMS) by recommending three core control details of the Information Security Management (ISMS) videlicet security policy, access control, and mortal resource security.

3. Methodology

Significant evidence and conclusions on organisational information security systems for sustainable Africa transformation were evaluated, analysed and synthesised by researchers. The study is both descriptive and explanatory, using a narrative review technique (Bell, 2017; Privizzini, 2017). The method entails analysing and synthesising varied studies and reaching comprehensive conclusions based on the researchers' expertise, current theories, and models (Hill & Burrows, 2017; Scarnato, 2017). Researchers may capture and grasp different and many insights about scholarly study themes using story studies, with considerable abilities, capacities, and possibilities to extract from substantial literature, reflective practices, shared viewpoints and expertise (Malcolm, 2017). Within the framework of this narrative study, the researchers analysed

a large number of peer-reviewed publications based on the selected keywords, identifying terms, identifying articles, assessing quality, extracting data and synthesising data.

4. Data Collection

This study collected data from peer-reviewed papers that were relevant to the present research as ProQuest databases, Science Direct, Google Scholar, Walden University foreign library databases, and other relevant peer-reviewed sources were used in the study. Key phrases and terms related literature on techniques for controlling organisation information security systems in Africa, with a focus on avoiding or minimising through efficient compliance to security policies, control over implementation of policies and enterprise meanings. "Managing organisation information security systems," "conflicts and integrity for sustainable Africa transformation," "leveraging Africa information security systems," and many more phrases and words were used. 36 references were used in the evaluations. At least, 90% of the articles included in the study were peer-reviewed.

Discussion and Findings

Astakhova (2015) cited some impressive figures from InfoWatch Analytical Center, in the first half of 2014 that at least 650 examples of non-public information leaking were documented which increased slightly than what it was in 2013, while 71 of those who leaked information out information were among employees of corporations. In Africa, workers are more prone to fall victim of social engineering assaults as a result of self-interest, feeling guilty, inability to have confidence in others, or ignorance or disregard for association policies, ethics, and programs (Greavu-Serban & Serban, 2014). The rigidity of these problems, as well as the extent to which they are successfully alleviated is ineffective (Silic & Back, 2014). This is due to the fact that senior executives, middle executives and employees constantly disregard information security standards, resulting in significantly more recurrent security breaches than is required (Whitman, 2003). According to most IT inspection reports, the primary driver of most security breaches is failing to misbehave with specialised, effective, and operational programmes. According to the most recent reports, physical safety and environmental regulations for the numerous IT residences are typically poor, with no provisions for backup data telecommunications links to provide service in the event that supplying lines fail. In some cases, there is no attestation of the IT means or interconnections relating to the Security Technology Integrated Program (STIP). In a nutshell, these gaps or omissions in information security concepts or programmes commonly jeopardise the security, reliability, and accessibility of data saved, communicated and reused.

The authors purposefully presented failures before achievements since assessing security technological management accomplishments is difficult (Pfleeger et al., 2010), and

one can gain insight from mistakes made, as in many other fields. Knowing the reasons for breaches and how to prevent them will help one comprehend how to quantify security performance. The complete security technological control is difficult, complicated, multifaceted, emerging, indestructible, and based in the realm of abstraction, and contextual influences of the surroundings (Pfleeger et al., 2010). Information security success should be dependent on interrelated variables such as system quality, user satisfaction, information quality, individual impact, and organizational impact as to define information success (Dwivedi et al., 2015) and the service quality dimension of information technology (IT) departments (Petter, et al., 2013).

Developing More Effective Information Security Technical Controls in Africa

It is not possible to tackle information security system difficulties, issues, and integrity for Sustainable Africa Transformation without first understanding technology and its challenges (Stallings & Brown, 2012). Security issues, like IoT issues, are about the mindset rather than technology (Cottrell, 2016). Computer security is a societal and organisational issue, not basically a technological one (Dhillon & Backhouse, 2000). This is due to the fact individuals supervise and utilise technical systems. Despite the advancement in technology, security breaches have been on the increase involving both small and large organisations (Fenz, et al., 2014). In the past, attacks against a company's sensitive data and information were relatively simple to spot, with virus attacks and network intrusion attempts easily captured and blocked at the boundary. With the rise of multi-functional malware, these easy mitigation approaches were no longer helpful.

Nowadays, a phishing effort may be used by a hacker to compromise organisational data. In recent years, the increased reliance on data and digital services, as well as complicated connection settings, which was initially meant to protect data privacy, reliability, and accessibility, have made gadgets with software-defined behaviour or network access vulnerable to breach by outside parties (Fenz et al., 2014). These are dangerous trends in information security. However, there are effective practices that provide high-level protective measures, such as computer and network installations, good system development, and essential business applications. Other best practices include approaches that effect an essential component evaluation and apps that identify and critically review corporate procedures in respect to data security, availability, and reliability. Some of the technical measures put in place in a Social Network Site (SNS) include customization of access controls based on the users' groups and information type, setting privacy in a user-friendly way to allow for adaptability, incorporating with an interactive interface that can be readily understood by any usual SNS user, and customised search to additionally improve the safeguarding of the user's privacy (Okesola & Grobler, 2014).

As a result, information security control is a difficult undertaking that necessitates the deployment and monitoring of over 130 security measures (Montesino & Fenz, 2011). The outcome of an examination of three commonly used information security standards as well as best practice recommendations by Montesino and Fenz (2011) showed that existing solutions can automate around 30% of the security controls listed in ISO 27001 and NIST SP 800-53. To improve the effectiveness of information security management, it is vital to automate as many processes as feasible. Furthermore, continuous monitoring of information security management systems is critical to ensuring the privacy, reliability and accessibility of organisational data.

Regardless of how arbitrary previous occurrences were, the past may be examined and analysed to forecast the future. Bringing statisticians inside the security control room to assist in the examination of not only the data being gathered, but also the simulations being employed for recording presumptions might be helpful. According to Pfleeger et al. (2010), a Bayesian strategy may assist to verify any presumptions made about the variables of before delivery simulations, as well as select among alternative models, so that feedback on the effectiveness of the models, combined with enhanced data quality, may assist in shifting the attention from assurance about what took place previously to trust in predicting what is probably bound to take place in the years to come. Precise and practical options are attainable by employing the adaptive programming algorithm technique in the suggested model, which can result in the ideal security control subset based on deployment price, efficiency, and financial limitations (Shahpasand et al., 2015).

Conclusion

Prior study review and summary have shown and recognised the multidisciplinary character of the issue of human factor evaluation, as well as approaches to reduce the threat to an organisation's information security. Human interaction, expenses, and the intricate nature of security procedures may all be reduced with security automation. Since no one instrument can fully harness the security control automation capacity, an integration of several security control automation technologies is necessary. Technical security control is a matter of knowledge. Security experts should learn to approach issues imaginatively by distinguishing between epistemic and aleatory or random risk. On the contrary, epistemic risk shows our inadequate understanding of a procedure, whereas aleatory risk reveals the intrinsic unpredictability of an operation. As a result, epistemic risk may be lowered by gathering and synthesising higher quality evidence from diverse actions carried out throughout the system's development cycle. This will strengthen the expertise and awareness of all aspects of security systems, allowing one to better the process of designing systems, creating confidence, and improving preventative measures, among other things.

References

Ahmad, A., & Maynard, S. (2014). Teaching information security management: reflections and experiences. Information Management & Computer Security, 22(5), 536-513. https://doi.org/10.1108/IMCS-08-2013-0058

Astakhova, L. V. (2015). Information security: Risks related to the cultural capital of personnel (Review). *Scientific and Technical Information Processing, 42*(2), 41-52. https://doi.org/10.3103/S0147688215020021

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

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

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

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'oeminstitutos de pesquisap'blicos. *Journal of Information Systems and Technology Management: JISTEM, 12*(2) 289-315. https://doi.org/10.4301/S1807-17752015000200006

Dhillon, G., & Backhouse, J. (2000). Information system security management in the new Millennium. *Communications of the ACM 43* (7)

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

Dwivedi, Y., Wastell, D., Laumer, S., Henriksen, H. Z., Myers, M. D., Bunker, D., Elbanna, A., Ravishankar, M. N., & Srivastava, S. C. (2015). Research on information systems failures and successes: Status update and future directions. *Information Systems Frontiers, 17*(1), 143-157. https://doi.org/10.1007/s10796-014-9500-y

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

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.

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

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

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

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

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. https://doi.org/10.1108/ics-04-2014-0026

Komatsu, A., Takagi, D., &Takemura, T. (2013). Human aspects of information security. Information Management & Computer Security, 21(1), 5-15. https://doi.org/10.1108/09685221311314383

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. https://doi.org/10.21608/ejsw.2017.8725

Montesino, R., &Fenz, S. (2011). Information Security Automation: How far can we go? Availability, Reliability and Security (ARES), 2011 Sixth International Conference on. https://doi.org/10.1109/ares.2011.48.

Narain, S. A., Gupta, M. P., & Ojha, A. (2014). Identifying factors of "organizational information security management. Journal of Enterprise Information Management, 27(5), 667-644. https://doi.org/10.1108/JEIM-07-2013-0052

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

Olusegun, O. J., & Ithnin, N. B. (2013). Enhancing the Conventional Information Security Management Maturity Model in Resolving Human Factors in Organization Information Sharing. International Journal of Computer Science and Information Security, 11(8), 65-76.

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.

Petter, S., DeLone, W., & McLean, E. R. (2013). Information systems success: the quest for the independent variables. *Journal of Management Information Systems, 29*(4), 7?62

Pfleeger, S. L., Predd, J. B., Hunker, J., & Bulford, C. (2010). Insiders Behaving Badly: Addressing Bad Actors and Their Actions. *Information Forensics and Security, IEEE Transactions on, 5*(1), 169-179. https://doi.org/10.1109/TIFS.2009.2039591.

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

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

Shahpasand, M., Shajari, M., Hashemi-Golpaygani, S. A., & Ghavamipoor, H. (2015). comprehensive security control selection model for inter-dependent organizational assets structure. *Information and Computer Security, 23*(2), 218-242. https://doi.org/10.1108/ICS-12-2013-0090

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

Silic, M., & Back, A. (2014). Information security: Critical review and future directions for research. *Information Management & Computer Security*, *22*(3), 308-279. https://doi.org/10.1108/IMCS-05-2013-0041

Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. (2014). Variables influencing information security policy compliance: A systematic review of quantitative studiesInformation Management & Computer Security, 22(1), 42-75.

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

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

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

Thompson, H. (2013). The human element of information security. Security & Privacy, IEEE, 11(1), 32-35.

Whitman, M. E. (2003). Enemy at the gate: Threats to information security. *Communications of the ACM, 46*(8), 91-95.

.