World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

Managing organization information security systems, conflicts, and integrity for sustainable Africa transformation

Felix Chukwuma Aguboshim [1,*], Joy Ebere Ezeife [1] and Ifeyinwa Nkemdilim Obiokafor [2]

[1] *Department of Computer Science, Federal Polytechnic, Oko, Nigeria.*
[2] *Department of Computer Science Technology, Anambra State Polytechnic, Mgbakwu, Nigeria.*

World Journal of Advanced Research and Reviews, 2022, 14(02), 080–085

Publication history: Received on 04 April 2022; revised on 04 May 2022; accepted on 06 May 2022

Article DOI: https://doi.org/10.30574/wjarr.2022.14.2.0425

Abstract

The ubiquitous reliance on technological innovations by enterprise organizations for electronic file-sharing networks across all business transactions has further exposed organization system enterprises to security threats and risks. Globally, a positive relationship exists between employees' adherence to security policy enforcement, enterprise definitions, and effective management of organization security systems. Security measures required to handle threats to the organizations' data: confidentiality, integrity, and availability are becoming complex, dynamic, psychological, but largely undeveloped, outdated, and non-sustainable in Africa despite the huge cyber-security innovations. This study highlights the gaps created by poor employees' adherence to security policies and enforcement in managing organization information security systems, conflicts, and integrity, and strategies to close them. The authors explored a narrative review of prior research that revealed significant information on strategies for managing organization information security systems. Peer-reviewed articles within the last five years were extracted from electronic databases, using relevant search keywords Results show that organizational security issues can be prevented or mitigated through effective adherence to security policies, control over policy enforcement, and enterprise definitions. Findings from this study may extend proper security management practices and prevention strategies for Africa's transformation.

Keywords: 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 [34] because what contributes to information insecurity has proven to be complex, dynamic, and more psychological in nature [4], [10], and [22]. The activities required to handle threats to the organizations' data confidentiality, integrity, and availability are also complex, dynamic, and psychological. Perimeter defenses, control over devices, employee 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 [35]. Attackers are personalizing their attacks, but defenses are not been personalized [35]. Information security has been defined from multiple perspectives [20] and with a holistic approach that expands beyond the specialized security [23], to comprise the terrain, the technology, and the people [32] and [34]. A significant quantum of empirical inquiries points to the fact that humans appear to be the most important links to the information security of any association, and always constitute the loftiest threat to the information security measures and information integrity of any association [32]. This is because of the differences in adventures or exploits regarding the intent to apply security measures or executive crimes [17]. [34]

* Corresponding author: Felix Chukwuma Aguboshim
Chief Lecturer, Department of Computer Science, Federal Polytechnic, Oko, Nigeria.

reported a security incident where members of a Financial Institution's credit card numbers and information were stolen. Investigations carried out involved the three components of information security systems as identified by [32] and [34]: the environment, the technology, and the people. In this case, the security breach did not come from the technical nor the environment or external but from the apparently overlooking 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 dust bin outside. This gave hackers the information cheaply to attack the bank. The breach points to a lapse in information system security, which is not the same as technology security [34]. 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 [31]. Today's information system consists of the environment, technology, and the people. [32] and [34]. Therefore delivering Security Education Training and Awareness (SETA) should reflect the principles of Information security that aim 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 understanding of security policies and implementation that has some technical solutions [1]. However, modifying human behavior through training is hard; some battle-worn security executives might even dismiss it as impossible [35]. 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 [35].

2. Literature Review

Managing organization information security systems, conflicts, and integrity for sustainable Africa transformation requires the study of the information security specialized controls, analysis, and conflation of previous inquiries, successes, failures, and how best-advanced generalities and ways can be used to minimize information security pitfalls and failures. Information systems security is of high precedence in all situations of association or government, especially in Africa. In Africa, information systems are vulnerable to numerous pitfalls that can beget significant damage and losses, ranging from crimes distorting database integrity to fires destroying, maybe, the centers of the entire system. Losses can come from the conduct of apparently trusted workers defrauding a system, from hackers, or from careless data entry. Generally, security breaches can creep in when data integrity situations, systems- trustability situations, aren't harmonious with the perceptivity of the information reused; when there are failures or discontinuity in enforcing and maintaining functional plans harmonious with the criticality of stoner information processing conditions, or neglect of information system security programs and program.

2.1. Analysis and Conflation of Previous Exploration

Over time there have been enormous advances in the field of specialized information security controls with complex and progressed specialized controls similar to Asanti-virus, customer-grounded firewalls, and real-time doctoring [33]. Some socio-specialized trends that are likely to shape the cybersecurity terrain in the coming decade have been linked. [8], and their possibility to produce great effect in the information security specialized controls observed [15]. In the last decades, the IEEE Security & Sequestration has concentrated on a wide variety of important programs that have not only contributed to the understanding of security but also to the innovative and effective results of information specialized security problems [25]. These trends, according to [8], are pall computing; big data [13]; the Internet of Effects; the mobile internet or mobile computing; brain-computer interfaces, and mobile robots; amount computing, and the demilitarization of the internet. These trends come with their grueling requirements and conditions for further data, further connections, further movement, and flows. As a result of this massive data storehouse and interconnectivity, organizational data and information are exposed to further openings for vicious exploitation and pitfalls, lower security, and lower control [19]. The circumstance of disasters, operation crimes, and oversights, further increase the pitfalls placed on information systems. Important previous exploration has also concentrated on individual fraud types identity theft, intellectual property fraud, and insurance fraud. Still, Scholarly exploration in the area of fraud is delicate [11]. Studies of fiscal fraud are hampered because it's delicate, if not insolvable, to pierce malefactors. Enterprises may be reticent to admit passing security or fraud problems within their operations, while directors may repel inquiry or analysis from outside groups, including academic experimenters to study their enterprises for fear of exposing their character to the public. It's also delicate for external experimenters to gain access to the association's original, unsanitized data. This is one of the reasons why determining what contributes to information instability has proven to be complex in nature [10], because similar conditioning is needed to handle pitfalls to the associations' data confidentiality, integrity, and vacuity is also complex. Despite the perpetration of advanced security specialized controls, information systems have remained vulnerable. This is because there are attestations that suggest that mortal vulnerabilities are decreasingly exploiting information systems [33]. Some experimenters have noted a number of

reasons for this, such as problems with the usability of information systems [5], [13], and [21], compromised opinions by druggies [12] and limited capability to misbehave with Knowledge Management Systems or instructions [6], and [29]. Still, [9] epitomized and distributed these miscalculations into four orders processes (operation process and specialized design operation methodologies), people involved in a design, product design size, and urgency, including its pretensions, performance, robustness, and trustability), and technology (IS failures performing from the use and abuse of ultramodern technology). Nonetheless, Study by [16] has handed enhanced strategies to manage the Information Security Management (ISMS) of the association by proposing three core control particulars of the Information Security Management (ISMS) videlicet security policy, access control, and mortal resource security.

3. Methodology

Significant research pieces of evidence and findings based on the study conceptual framework and existing challenges that plagued organization information security systems for Sustainable Africa Transformation were reviewed, analyzed, and synthesized by the researchers. Researchers adopted a narrative review methodology was adopted where the study may be described as descriptive or explanatory [3], and [26], and where analysis and synthesis of various and related research findings are required to draw holistic interpretations or conclusions supported by the reviewers' own experience, existing theories, and models [14], and [27]. With narrative studies, researchers can capture and comprehend diverse and numerous insights around scholarly research topics, with great abilities, capabilities, and opportunities to extract from vast literature, reflective practices, shared views, and knowledge [18]. Within the context of this narrative study, the researchers reviewed an enormous of peer-reviewed articles in line with the identified keywords, term identification, article identification, quality assessment, data extraction, and data synthesis.

4. Data Collection

Data collection came from reviewed research findings that are related and associated with our study. The ProQuest databases, ScienceDirect, Google scholar, Walden University international library databases, and other related peer-reviewed texts were our major sources of data collection. We used phrases and terms as key search words within the databases for related literature on strategies for managing organization information security systems with a stress on preventing or mitigating through effective adherence to security policies, control over policy enforcement, and enterprise definitions in Africa. Phrases and terms engaged included "Managing organization information security systems", "conflicts, and integrity for sustainable Africa transformation", "leveraging Africa information security systems", and lots of others. Our reviews incorporated 36 references. Thirty-three (92%) of the entire references within the study are peer-reviewed.

5. Discussion

[2] cited some eloquent numbers from InfoWatch Analytical Center, within the half of the year two thousand and fourteen, which recorded 654 cases of leakage of nonpublic information, which was 32 further than what it absolutely was within the previous year, while 71 of these who blurted information were workers of companies. In Africa, workers are more vulnerable to falling victim to social engineering attacks because of rapacity, tone-interest, guilt, liability to trust others, ignorance or neglect of association policies, ethics, and programs [12]. The inflexibility of these pitfalls and the degree to which they're effectively eased aren't effective [30]. This is because top directors, middle directors, and workers likewise, have continued to neglect information security principles, which in turn, redounded in far further frequent security breaches than are necessary [36]. Utmost IT inspection reports have indicated that the root cause of utmost security breaches is failure to misbehave with specialized, functional, and operation programs. Utmost reports show that the physical security and environmental controls for the multitudinous IT apartments are frequently deficient with no vittles for spare data telecommunications lines to give service in case of failure of serving lines. In some cases, there is no attestation of the IT means or interconnections relating to the Security Technology Integrated Program (STIP). In summary, these scarcities or neglects of information security principles or programs frequently place at threat the confidentiality, integrity, and vacuity of the data stored, transmitted, and reused. The authors have purposely discussed failures before successes, because measuring security technical control successes is hard [25], and so that like many disciplines, we can learn from our mistakes. Understanding what causes failures and avoiding them can be a good way to understand how to measure successes in security. The entire security technical control is hard, complex, multidimensional, emergent, irreducible, and resident in abstraction, and context affects the environment [25]. Information security success should be dependent on interrelated variables such as System Quality, User Satisfaction, Information Quality, Individual Impact, and Organizational Impact, to define information success [9], and the service quality dimension of information technology (IT) departments [24].

5.1. Developing More Effective Information Security Technical Controls in Africa

Technology alone cannot solve our information security systems problems, conflicts, and integrity for Sustainable Africa Transformation until we understand the technology and the problems [32]. Security problems, like IoT problems, are about psychology, not technology [4]. Computer security is more of a social and organizational problem, rather than a technical problem [7]. This is because the technical systems are managed and used by people. Despite the advancement in technology, security breaches have been on the increase involving both small and large organizations [10]. In the past, attacks on a company's sensitive data and information were fairly straightforward to identify and easy to capture the attention of virus attacks, network intrusion attempts, and blocks same just at the perimeter. With the rise of multi-functional malware, these easy mitigation approaches could no longer help. Today an attacker may try to compromise organizational data with a phishing attempt. Recently, the increasing dependency on data and electronic services, and complex connectivity, originally intended to secure confidentiality, integrity, and availability of data, have now made devices with software-defined behavior or network connectivity to be susceptible of being compromised by an external party [10]. These are dangerous trends in information security. However good practices exist such as computer and network installations, good system development, and critical business applications, that provide high-level techniques of information security. Other good practices included methodologies that impact the assessment of crucial elements and applications that identifies and criticality examines the business processes in relation to confidentiality, availability, and integrity of data. In a social network site (SNS) for instance, some of the technical controls implemented are customization of access controls based on the users' groups and information type, setting privacy in a user-friendly way to make for flexibility, integrating with a user-friendly interface that is easily understood by any typical SNS user; and customized search implemented to further enhance the preservation of the user's privacy [21].

Information security control is therefore a complicated task that involves the implementation and observing numerous security controls [19]. The result from the analysis of three widely used information security standards and best practice guidelines according to [19], showed that about 30% of the security controls included in ISO 27001 and NIST SP 800-53 can be automated by existing tools. It is, therefore, necessary to automate as many controls as possible in order to achieve greater efficiency in information security management. Also, regular auditing of information security management systems is extremely necessary to ensure the confidentiality, integrity, and availability of organization data.

The past can be studied and analyzed to predict the future no matter how random past events have been. Inviting statisticians into the security control room to help examine not just the data being collected but also the models being used to capture our assumptions. According to [25], a Bayesian approach can help check any assumptions made about the parameters of prior distribution models, and it will also help choose among competing models, so that the feedback on model performance, married with improved data quality, can help change our focus from certainty about what happened in the past to confidence in understanding what is likely to happen in the future. Exact and achievable solutions are possible by using the dynamic programming algorithm approach in the proposed model that can result in an optimal security control subset based on its implementation cost, its effectiveness, and the limited budget [28].

6. Conclusion

The analysis and synthesis of prior research have revealed and identified the interdisciplinary nature of the problem of the assessment of the human factor, and ways of reducing the risk to the information security of an organization. Security automation can decrease human intervention, costs, and the complexity of security activities. Combinations of different security control automation tools are required because no single tool can exploit the full security control automation potential. Security technical control is a knowledgebase affair. Security professionals should begin to think differently by separating epistemic risk from aleatory risk. By contrast, epistemic risk reflects the incomplete state of our knowledge about a process, while aleatory risk represents the inherent randomness in a process. Therefore epistemic risk can be reduced by continuously collecting and compiling more and better evidence from various activities conducted during the system development life cycle. This will increase our knowledge and understanding of all facets of security platforms, to improve the process of building our systems, establishing assurance, enhancing preventive measures, and more.

Compliance with ethical standards

Acknowledgments

Our sincere appreciation and thanks to Dr. Felix. Chukwuma. Aguboshim for his wonderful contributions.

Disclosure of conflict of interest

There are no conflicts of interest.

References

[1] Ahmad A, Maynard S. Teaching information security management: reflections and experiences. Information Management & Computer Security. 2014; 22(5): 536-513.

[2] Astakhova LV. Information security: Risks related to the cultural capital of personnel (Review). Scientific and Technical Information Processing. 2015; 42(2): 41-52.

[3] Bell EE. A Narrative Inquiry: A Black Male Looking to Teach. The Qualitative Report. 2017; 22(4): 1137-1150.

[4] Cottrell L. IoT problems are about psychology, not technology. 2016.

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

[6] 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 institutos de pesquisa p'blicos. Journal of Information Systems and Technology Management : JISTEM, 12(2) 289-315. https://doi.org/10.4301/S1807-17752015000200006

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

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

[9] 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

[10] 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

[11] 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.

[12] 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

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

[14] 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

[15] 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

[16] 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

[17] 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

[18] 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

[19] 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.

[20] 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

[21] 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

[22] 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.

[23] 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.

[24] 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

[25] 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.

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

[27] 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

[28] 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

[29] 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

[30] 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

[31] 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.

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

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

[34] 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.

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

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