


Information Security Policies in Nigerian Institutions: Evaluation and Readiness

Adeyemi Abel Ajibesin, American University of Nigeria, Nigeria*

 <https://orcid.org/0000-0001-6518-0231>

Kasim Maharazu, American University of Nigeria, Nigeria

Olusegun Ogundapo, American University of Nigeria, Nigeria

ABSTRACT

Information systems have become part and parcel of today's business operations, with competition on its rise. The security challenges related to information systems could have a severe impact on the overall business objectives of an institution if not handled at the right time. A well-meaning institution must take a full-blown step towards information security management to achieve information security. Information security management has been seen as any management system to address the security issues affecting an institution and align security needs to the overall business objectives. Conversely, information security policy is the foundation upon which institutions base their entire information security management. This study looks at the uptake of information security policy among Nigerian institutions. The survey result created a clear picture of the uptake of information security policy among Nigerian institutions.

KEYWORDS

Evaluation, Information Security, Institutional Readiness, Management, Policy Development, Security Policy, Security Threats, Vulnerabilities

INTRODUCTION

Information security is one of the crucial aspects that cannot and should not be neglected in any well-meaning institution. As institutions gradually realize the importance of information systems to their business progress, the need for the security of the products has become necessary. Therefore, it can be asserted that institutions neglect security at their peril. Recent research studies have shown great concern on the importance of information systems security and its policies in an institution (Boss, Kitsch, Angermeier, Shingler, and Boss, 2009; D'Arcy and Hovav, 2009; and Posey, Roberts, Lowry, Bennett, and Courtney, 2013). Meanwhile, related research has emphasized the importance of the human and process variables in ensuring the effectiveness of information security policy. It is believed that information systems security policy is the foundation upon which every institution's security is based (Parker, 1998). On this basis, we can easily discern the importance of having a formal policy for institutions' information security. Besides, information security policy describes how institutions achieve their security objectives alongside their institutional goals (Nasir and Vajjhala, 2020).

DOI: 10.4018/IJRCM.303103

*Corresponding Author

One big problem attached to an information security breach is that even those innocent employees are liable to be affected by the damage done (Hsu, Shih, Hung, and Lowry, 2015). In other words, damage caused by a single employee can significantly impact the entire staff of the institution. This might result in low patronage, low revenue, and a bankrupting level of a business. The above statement strengthens the importance of having an information security policy, complying with it, enforcing it, and emphasizing the penalties for its breach. However, many institutions have been implementing security measures for many years, yet they have not minimized or possibly done away with their security challenge (Al-Awadi, 2009). They are still striving hard to achieve sound information security. Thus, institutions need to devise mechanisms to fight against the ever-growing number of security breaches to their information systems. Furthermore, one of such protection mechanisms is formulating and complying with documented security policy (Doherty, Anastasaki, and Fulford, 2009). This study tends to fill this gap by using an empirical method to assess the readiness of Nigerian institutions towards the adoption and implementation of information security policy.

Many institutions today are striving hard to achieve security in their institutions. Many have engaged security experts to do away with threats and vulnerabilities to their information assets. These measures include technical, processes, and human actions (Adamu, and Aliyu, 2021). However, many institutions have been experiencing security breaches. This tends to raise the question: why are institutions still striving to achieve a substantive level of security after working with security for so many years? There are various reports concerning cyber threats and the urgent need to intensify efforts to provide information technology infrastructure and adequate internal and external controls to achieve security solutions in Nigeria. In a conference held by Cyber Security Experts Association of Nigeria (CSEAN) (2018), it was reported that “In Nigeria, business institutions, ministries, departments, and government agencies (MDAs), are said to lose over N127 billion annually, translating to about 0.08 percent loss in the country’s annual Gross Domestic Product (GDP) (Vanguard Newspaper, 2018)”. Equally, according to Price Waterhouse Coopers (PWC)’s Nigeria Cyber Security Outlook (2015), several allegations of hacking attempts at various public institutions and political organizations’ websites during the year. Prominent examples are “...the reported hack and de-facing of the Independent National Electoral Commission (INEC) website in March 2015 and that of Lagos State Government in December 2015 (Mondaq Report, 2017).” In this regard, inadequate or ineffective countermeasures can serve as the means to incurring security breaches in an institution (Wang, 2015).

While there have been so many concerns on the need to mitigate external risks, it is also paramount to understand that insiders posed more severe threats. An employee’s error or malicious intent can significantly impact the security of information resources and may persist (Johnston, Warkentin, McBride & Carter, 2016). This has created a clear picture of how institutions have suffered from various forms of attacks both globally and locally. The increased number of risks to information security has heightened the thirst of managers to intensify efforts towards awareness on the need for substantial information security management. In addition, information security policy has been noted as a critical component in pursuing a good information security environment (AlShaikh, Maynard, Ahmad, & Chang, 2015; Fulford & Doherty, 2003). However, there has been an under uptake of information security policy among institutions. Research is conducted in the UK at regular intervals to examine the “uptake, dissemination and the impact of information security policies” among some UK institutions. However, there is no evidence of a similar empirical study in Nigeria to the best of the researcher’s knowledge. So, this study intends to fill this gap by empirically investigating the uptake, content, implementation, and roles of information security policy in Nigeria’s institutions (Makeri, 2019). While there is a body of literature in policy implementation, formulation, and compliance, few studies have been conducted on the content and structure of information security policy. The aims were formulated into the following research questions:

Research Question1: What specific areas have the Nigerian institutions covered in their information security policies?

20 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/article/information-security-policies-in-nigerian-institutions/303103

Related Content

Breaking Barriers to Promote Sustainable Development in the Wine Industry: A Theoretical Study on the Role of the Entrepreneurial Ecosystem Approach

Eloi Jorge, Carlos Herves-Belosoand Antonio Monteiro Oliveira (2021). *Financial Management and Risk Analysis Strategies for Business Sustainability* (pp. 124-145). www.irma-international.org/chapter/breaking-barriers-to-promote-sustainable-development-in-the-wine-industry/274725

Risks in Supply Chain Logistics: Constraints and Opportunities in North-Eastern Nigeria

Edna Mngusughun Dengaand Sandip Rakshit (2022). *International Journal of Risk and Contingency Management* (pp. 1-18). www.irma-international.org/article/risks-in-supply-chain-logistics/295957

Ethics, Risk, and Media Intervention: Women's Breast Cancer in Venezuela

Mahmoud Eidand Isaac Nahon-Serfaty (2015). *International Journal of Risk and Contingency Management* (pp. 49-69). www.irma-international.org/article/ethics-risk-and-media-intervention/133547

Homeowner Behavioral Intent to Evacuate After Flood Risk Warnings

Kenneth David Strang (2013). *International Journal of Risk and Contingency Management* (pp. 1-22). www.irma-international.org/article/homeowner-behavioral-intent-to-evacuate-after-flood-risk-warnings/80017

Estimating and Managing Enterprise Project Risk Using Certainty

Scheljert Denas (2017). *International Journal of Risk and Contingency Management* (pp. 47-59). www.irma-international.org/article/estimating-and-managing-enterprise-project-risk-using-certainty/177840