ZIBELINE INTERNATIONAL PUBLISHING

Malaysian E Commerce Journal (MECJ)

Journal Homepage: http://myecommerecejournal.com/

DOI: http://doi.org/10.26480/mecj.02.2019.22.26

ISSN: 2521-0505 (online)
CODEN: MECJBU

RESEARCH ARTICLE

THE IMPACT OF INFORMATION SECURITY IN CORPORATE GOVERNANCES IN NIGERIA

Yakubu Ajiji Makeri*

Kampala International University School of Computing and Information Technology.
Corresponding Author Email: yakubu.makeri@kiu.ac.ug

ARTICLE DETAILS

Article History:

Received 01 June 2019
Accepted 11 July 2018
Available online 15 July 2019

ABSTRACT

The conceptualization of information security culture to develop an information security culture measurement model, to do so, comprehensive literature analysis of current information security culture models and frameworks were examined. Organizations in the developing countries need to protect their information assets (IA) optimally. This paper is based upon the argument that achieves the fully effective information security management (ISM) strategy; is essential to look at information security in a socio-technical context, i.e., the cultural, ethical, moral, legal dimensions, techniques devices, and. Tools An information security culture is defined as the attitudes, assumptions, values, beliefs, and The knowledge that employees/stakeholders use to interact within the organization's systems and procedures at any point in time. This paper is to addresses whether the current reference documents on corporate governance pay sufficient attention to information security within their organization or whether reference documents on security management and baseline controls sufficiently recognize the relationship with internal control systems and framework, governance pay attention among and the responsibilities of the corporate board with respect to information security and training, and executive accountability. The Information Systems (IS) in organizations already ubiquitous in developed countries – are being deployed in developing countries more Information Security Governance with services such as registration of death. Birth, issue of passport, registration of marriage, collection of tax, registration of voters, payroll, and public finance amongst others have been computerized or are under active considerations for automation consists of these services and framework has become a vital function within the information system and governance. With increased dependence on the IS connected over open data networks, efficient information security governance has become a vital success feature for organizations in developing countries. Among the Developing countries are going through processes that developed countries went through many years ago. To achieve information security in an organization, it is essential to create and implement effective information security in a corporate organization. The focus of this paper is to enhance information security in non-profit organizations in the context of developing counties. According to the United Nations, developed countries are United States, Canada, the Japan, Australia, New Zealand, and European countries, while the remainder is developing countries like Nigeria. The adoption and This goal concentrates of information systems faces many challenges in many developing countries such as lack of skilled personnel and Musa, 2010; Karokola and Yngström, 2009; Kimwele, Mwangi and, financial constraint, national culture, and inferior infrastructures security awareness among others. The studies have indicated social issues are at least as vital as technical issues in implementing information security governance. The information system is defined as "A discrete set of information resources organized for the such threats may continue to increase unless strong information security frameworks are implemented throughout company management chains. Collection, maintenance, processing, The use, of sharing, dissemination, or disposition of information". It also includes industrial/process controls equipment, the telephone switching, exchange; and equipment for environmental control.

KEYWORDS

socio-technical context, information security management, information security culture

1. AT OVERVIEW RESEARCH PROBLEMS

The discipline of information security is concerned with the confidentiality, integrity, and availability of information assets. There are several unsolved issues related to efficient information security governance in the developing countries such as voter registration, passport, voting, national identity, education records, financial records, and. The information security governance studies seek to tackle some of these issues; most of these studies argue within a culture of western societies [1]. These studies may not apply to nations outside. This research is concerned with improving information security in a corporate organization that resides in a culture outside the Western civilization, specifically Nigeria. The main research question is:

1.1 Purpose of Research

1.1.1 The purpose of the research

To develop a useful, integrated, theoretically robust framework that will support non- profit organizations to succeed in the challenging the most improving quality information security governance within the context of Nigeria.

The objectives of the research are to:

• Understand the existing strategies of information security

• To understand the current state of information security in non-profit organizations in Nigeria

• To understand the cultural factors which may impact the development and implementation of information security in a non-profit organization

• The framework is to improving information security culture in the Nigeria context

1.1.2 Research Motivation

This researcher work has experienced the deployment of IS at various organizations in Nigeria, how to adopt have transformed IS the way services provided by this paper has no doubt the sustainability of IS usage in Nigeria to develop the country. More countries are connected through open networks, and the usage increases, so do criminal activities on information systems [2]. Many developing countries ensure management implements a useful cyber-risk framework have experienced information security breaches. Some public institutions in Nigeria have been victims of cyber-attacks, including Nigeria. Another incident occurred when two nationals were caught stealing at Automatic Teller Machine (ATM) Since the introduction of multi-party democracy in Nigeria in 2015; elections have been marred with claims of ballot rigging. Nigeria is not the only developing country to face information security breaches [3]. This includes understanding the risks associated. In Nigeria, the majority of employees work in the non-profit sector. The former employee of this sector did observe that computer users in this sector have only fear of losing their data. The researcher, as a cybersecurity professional, would like to see this trend in security vulnerability for organizations in developing countries to be professional. The current research is to help by identifying the cultural factors that influence the governance of approach information security and create a framework that will enhance the management of information security in the non- profit organizations [4].

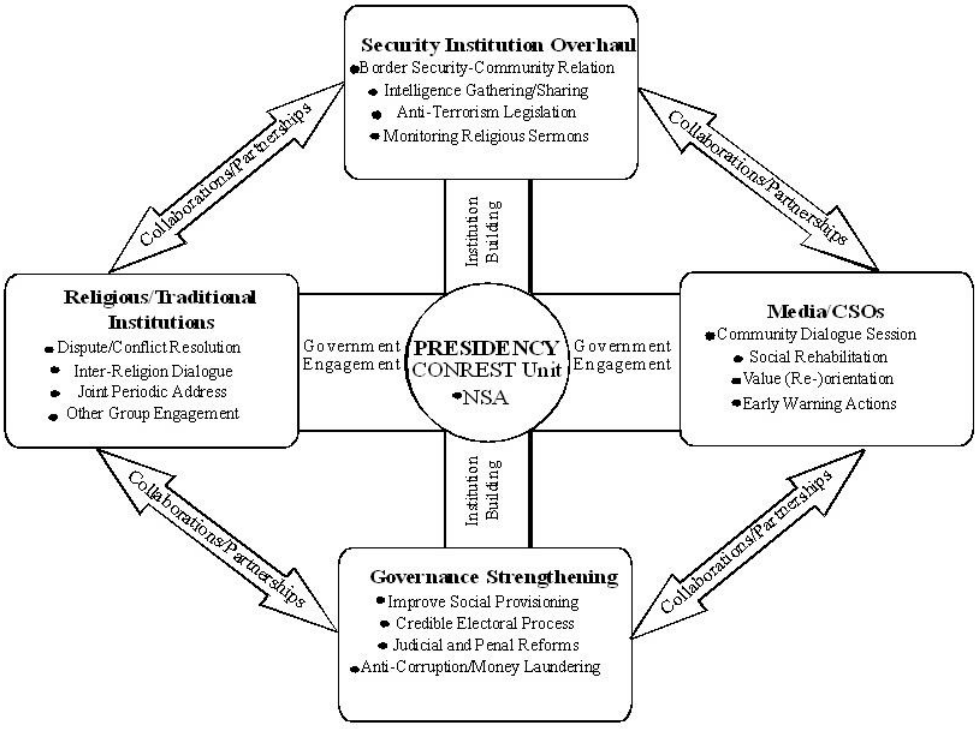

Figure 1: Counter Religious Extremism and Terrorism (CONREST) Strategy for Nigeria (Source: Author Elaboration)

This approach of mixed research methods consisting of qualitative, quantitative approaches will be employed in this research work to address the questions of the research [5]. This will, in turn, to achieve the research objectives, realize research purpose, and bring a better understanding of the study.

1.1.3 The research process and Overview

The investigation went through a series of operations as described in the exploratory case study was performed, consisting of several organizations [6]. They Data collection and analysis was conducted using a mixed methods approach.

1.1.4 Research Benefits

This research will be relevant to non-profit organizations such as public sector organizations in Nigeria. The benefits of this research are:

• This model is to Ensure information security governance grounded by the theory of semiotics for organizations in Nigeria.

• The framework for information security culture for organizations in the developing countries in the world.

• Contribution to the knowledge of non-profit organizations concerning their state of information security governance Nigeria.

• Due to the experience concerning integrating social and technical issues in developing counties like Nigeria. A model for information security governance.

• A contribution to the knowledge concerning cultural factors, on information security which will influence management in the Nigeria.

1.1.5 Focus Research

The focus of this research work is on the factors relevant to the management of information security in non-profit organizations in developing countries like Nigeria. The issues that are considered to be the focus of this research:

• The activities and factors associated with information security governance within organizations in a developing country environment.

• Issues related to information security culture in organizations in the context of a developing country.

2. INTRODUCTION

The research paper is on information security management practices, ICT

in the developing countries, culture, organizational semiotics, and related features of Nigeria [7,8]. The literature review aims to highlight gaps in the literature concerning information security management in non- profit organizations in the developing countries and provide background information on the documentation that is used to form the research and theoretical framework.

2.1 Background of Information Security

2.1.1 What is information security

According to CNSS (2010, p.37), information security is "the protection of information and information systems from unauthorized access, use, disclosure, modification, disruption or destruction to provide confidentiality, integrity, and availability." While, in this research, information security is defined as "preservation of confidentiality, integrity, and availability of information; also, other properties, such as non-repudiation, authenticity, accountability, and reliability can also be involved in cybersecurity."

The properties of information security are defined below:

• Confidentiality means that information is disclosed to an authorized user.

• Integrity means an unauthorized user does not modify information.

• Availability means data is available when required to an authorized user.

• The authenticity means a user attempting to access the information is, in fact, the user to whom the level of access belongs. To

• The accountability implies the user is responsible to the safeguarding of the information the user accesses.

• The Non-repudiation intends a sender of information cannot deny having to send the information.

• Reliability means data is being consistently processed according to its design.

2.1.2 Threats on information systems

To provide the protection, we need to provide direct measures according to a threat that the information system and cybersecurity are facing. A warning is a cause of harm to an organization [9]. Risks could be caused by cyber risk and external or internal sources including but not limited to employees' actions, the act of nature, malicious codes, technical failures, deliberate attacks and competitors. The attacks could be in the form of automated attacks or a combination of computerized attacks and social engineering.

Threats target and implementation of the vulnerabilities in on the system to cause damage. Vulnerability includes weakness of an information system that can be exploited by a threat Vulnerabilities could be unsecured ICT equipment, weak password, untrained employees, and inadequate physical security immature, software, and others.

A social engineering attack is a technique where an attacker employs tactics to leverage human trust in the targeted system to acquire confidential information. To starts operations with an attempt in which an attacker sends an email to an individual to come from a trusted source, is called social engineering and with free email provider such as Yahoo, Hotmail [10]. Most email requests that the user reply with the user's account password and account information is from the trusted source can verify the correct functioning of the report.

2.1.3 Countermeasures against threats

To provide protection and countermeasures must be implemented according to threats that organizations are facing. Measures that are performed to guarantee the security of confidentiality, integrity, and availability of information systems are called information assurances. Some examples of countermeasures that are used to protect against threats are:

• Training and awareness administered to employees to limit employees' actions that could jeopardize the security of information systems.

• Use of strong passwords in authentication scenarios.

• Use of backup systems to protect against an act of nature.

• Use of anti-virus, anti-malware, anti-spam software to protect against the virus, malware, and spam attacks.

• Use of information security management standards to benchmark the security activities in an organization.

• Image verification, mod rewrite, black hole, request limitation, hidden field trap, and spider trap, among others, can be used to protect from automated attacks.

2.2 Information security in developing countries

Developing countries are those countries which are in the process of industrialization but have limited resources. According to developed countries are Canada, the United States, Japan, Australia, New Zealand, and European countries, while the remainder is developing countries (which indeed classifies apparently wealthy countries such as Saudi Arabia as developing countries).

Many developing countries are in an early stage of adopting information systems in their government institutions. The adoption of information systems faces many challenges in many developing countries such as lack of skilled personnel, financial constraint, national culture, and inferior infrastructures among others.

2.3 Information security management

There are various practices to manage information security in organizations. The training includes the implementation of information security management systems (ISMS) in the organizations. Information security management systems emphasize the purpose to formalize responsibilities and control prescribed processes. In the next sections, a review of information security management systems found in the literature is demonstrated.

2.3.1 ISO/EIC 27001:2005 Standard

This is an international standard for information security based on British Standard BS 7799. The measure has adopted a process approach that establishes; implements operate, monitors, reviews, maintains and improves an organization's information security management system (ISMS). The standard implements the Plan-Do-Check-Act (PDCA) model to all its processes [11-13]. "Plan" means execute the ISMS; "Do" means run and manage the ISMS; "Check" means scrutinize and reassess the ISMS; and "Act" means preserve and enhance the ISMS. Compliance with ISO/IEC 27001:2005 guarantees that an organization has achieved a certain level of compliance level for each of the eleven clauses addressed. The limitations covered are:

• "Information security policy."

• "Organisation of information security."

• "Asset management."

• "Physical and environmental security."

• "Human resources security."

• "Communications and operations management."

• "Access control."

• "Information systems acquisition, development, and maintenance."

• "Information security incident management."

• "Business continuity management."

• "Compliance"

2.3.2 ISO/IEC 27002:2005

This is an internationally accepted best practice for information security based on British Standard BS 7799-1. It is a code of practice for information security management. It provides guidelines for implementing the ISO/IEC 27001:2005 standard.

2.3.3 ISO/IEC 27005:2008

This is an internationally accepted standard for information security risk management. The standard defines a process to manage risk including establishing the context, assessment of risk, treatment of risk, acceptance of risk, communication of risk and monitoring and reviewing of risk. The process follows the PDCA model. To understand ISO/IEC 27005:2008, one has to be aware of ISO/IEC 27001 and ISO/IEC 27002 standards. According the rule is unable to prioritize controls and to measure the impact of security enhancements.

2.3.4 NIST 800-14

It is a United States of America special publication on generally recognized standards and customs for the security of information technology systems based on OECD's guidelines for information security. The paper elaborates eight standards to be met by the information security program, which are:

- To support the mission of the organization
- To be a vital ingredient of robust administration
- To be financially sustainable
- To share security responsibilities to external users
- To make clear security responsibilities and accountability of users
- To use a comprehensive and integrated approach in the design of a security program
- To be reviewed regularly
- To consider social issues

Also, the publication elaborates fourteen customs to be met by the information security program, which are:

- Security policy
- Organization of the program
- Organization of Risk
- Planning of security
- Employee/User factors
- Planning for incidents and disasters
- Information security incident management
- User education and awareness
- Computer security, support, and operations

2.3.5 The Control Objectives for Information and related Technology (COBIT)

It is a risk-based IT governance framework developed by the Information Systems Audit and Control Association (ISACA). It is based on the scrutiny and integration of existing IT standards and best practices. According to ITGI, the framework guarantees IT is aligned with the business; IT permits the company and maximizes benefits; IT resources are utilized sensibly, and IT risks are adequately controlled. COBIT refers to many processes, to the information security process. The COBIT framework enables administrators to bridge the gap between control requirements, technical challenges, and operational risks.

2.3.6 The Control Objectives for Information and related Technology (COBIT)

It is a risk-based IT governance framework developed by the Information Systems Audit and Control Association (ISACA). It is based on the scrutiny and integration of existing IT standards and best practices. According to ITGI, the framework guarantees IT is aligned with the business; IT permits the company and maximizes benefits; IT resources are utilized sensibly, and IT risks are adequately controlled. COBIT refers to many processes, to the information security process. The COBIT framework enables administrators to bridge the gap between control requirements, technical challenges, and operational risks.

2.3.7 Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE)

OCTAVE is a risk-based approach for managing information security that is inclusive, systematic, driven by the situation, and self-directed. It was developed at Carnegie Mellon University. The procedure is organized in three phases which are (i) build asset-based threat profile; (ii) identify infrastructure vulnerabilities, and (iii) develop security strategy and planning. The pillar of OCTAVE is structured interviews at various levels of an organization to identify critical assets, risks on those assets, and design mitigation strategies for the assets. OCTAVE approach employs a PDCA cycle.

2.3.8 Information Technology Infrastructure Library (ITIL)

This is a framework that provides best practices for information technology. It provides guidelines on managing IT security using Control, Plan, Implements, Evaluates, and Maintain steps. ITIL can be adapted to the needs of an organization. It is used in association with other best practices such as ISO/IEC 27002.

3. DISCUSSION

Some of the above approaches for information security management are country or industry specific such as NIST 800-14 and HIPAA. According to Anttila and Kajava, the PDCA model adopted in some of the standards is applied in the standards rather unsystematically, vaguely, and meagrely for the overall aims of information security management. The major limitation of the COBIT framework is the reality that it does not offer continuous process improvement. Standards and other recognized references for information security management underline the significance of senior executives' commitment to information security management. But, according senior executives of large and small companies are not interested in information security in their management practices and do not understand their managing role for information security. Also, information security management emphasizes the information security policy. Finally, information security standards and best practices provide guidance and framework for best practice but not solutions. They need to be tailored to the requirement of the organization. Also, they need to be tailored for institutions in the developed countries. In Principle (5) of the OECD stresses the implementation of information security to cate to the needs of a democratic society. However, in many developing countries, democracy is in confusion or not on the same level as developed countries.

4. CONCLUSION

This paper has provided an essential understanding of information security governance of non-profit organizations in the context of a developing country. A framework for information security culture has been recommended for effective information security governance in the non-profit organizations. The chapter discussed the contributions of the research to the body of knowledge, implications of research, and future works. By reading this work organization in the developing countries could have an initial point of reference for their security requirements.

REFERENCES

[1] Cameron, K.S., Quinn, R.E. 2006. Diagnosing and Changing Organizational Culture: Based on the Competing Values Framework. San Francisco, USA: Jossey-Bass.

[2] Carl, D., Gupta, V., Javidan, M. 2004. Power distance' in House, R., Hanges, P. Javidan, M., Dorfman, P., and G. Vipin. London: Sage Publications Ltd., pp.513-563.

[3] Casmir, R., Yngstrom, L. 2003. IT Security Readiness in Developing Countries: Tanzania Case Study' in Irvine, C., and Armstrong, H. (eds.) Security education and critical infrastructures. Norwell, Mass: Kluwer Academic Publisher. Pp. 117-127.

[4] CERT. 2010. Cybersecurity watch survey: Cybercrime increasing faster than some company defenses. Software Engineering Institute, Carnegie Mellow. Available at: http://www.cert.org/archive/pdf/ecrimesummary10.pdf. (Accessed: 28

November 2013)

[5] Chaula, A., Yngstrm, L., Kowalski, S. 2006. Technology as a tool for fighting poverty: How culture in the developing world affect the security of information systems. Proceedings of the 4th IEEE International Workshop on Technology for Education in Developing Countries (TEDC06). Iringa, Tanzania, 10-12 July.

[6] Cheang, S. 2009. Conceptual Model for Cybersecurity Readiness Assessment For Public Institutions in Developing Country: Cambodia', 2009 Fourth International Conference on Computer Science and Convergence Information Technology, Seoul, South Korea, November 24-26.

[7] Cheang, S., Sang, S. 2009. State of Cybersecurity and the Roadmap to Secure Cyber Community in Cambodia,' 2009 International Conference on Availability, Reliability, and Security, Fukuoka, Japan.

[8] CISCO. 2010. The impact of global security threats trends on the enterprise. Cisco Systems.

[9] CLUSIF. 2008. Information systems threats and security practices in France. CLUSIF.Available at http://www.clusif.asso.fr/fr/production/sinistralite/docs/CLUSIF-rapport-2008-en.pdf (Accessed: 02 November 2010)

[10] CNSS. 2010. National Information Assurance Glossary. Available at: http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf. (Accessed: 04 July 2010)

[11] CS. 2010. Report of the Commonwealth observer group: Tanzania general elections. Available at: http://www.thecommonwealth.org/files/232431/FileName/FinalReport- TanzaniaCOG.pdf. (Accessed on 19 November 2012)

[12] CSI. 2011. Computer Crime and Security Survey. Computer Security Institute.

[13] Coyle, B. 2004. Risk awareness and corporate governance, 2nd ed. Canterbury: Financial World Publishing.