The International Journal Of Engineering And Science (IJES)
|| Volume || 4 || Issue || 12 || Pages || PP -49-53|| 2015 ||
ISSN (e): 2319 – 1813 ISSN (p): 2319 – 1805

An Analysis of the Information Security Governance in the State Owned Enterprises (Soe) In Zimbabwe.

Joseph Sigauke[1], Paul Mupfiga[2] , Theo Tsokota[2]

----------**ABSTRACT**----------
This study examined the existence and implementation of information security governance (ISG) in the state-owned-enterprises (SOE) in Zimbabwe. The study examined the implementation of information security governance in SOEs in Zimbabwe. This exploratory study was conducted using semi-structured interviews to collect data from a simple random sample. Interviews were also carried out with a composition of 13 Board members, 18 Executive management and 26 IT Executives. The data was then arranged into tables and for simple interpretation. The results of the study revealed that information security governance in SOE in Zimbabwe is still lagging behind. Despite the majority of Zimbabwe SOE recognizing the importance of ISG, most of them have no clear information security strategies or written information security policy statements. The study recommends that the state-owned-enterprises use IT governance frameworks such as COBIT, ITIL and BS17009.
Keywords *- Information security governance, State Owned Enterprise, Zimbabwe.*

Date of Submission: 01 June 2015 Date of Accepted: 15 December 2015

I. INTRODUCTION

Information security refers to protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, (USC-3542, 2011). This entails guarding against improper information modification or destruction, and includes ensuring information non repudiation and authenticity of the information. This extends to preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information, and availability, which means ensuring timely and reliable access to and use of information. A secure system must satisfy some importance features: confidentiality, integrity, availability and accountability (Kumar, 1995). The level of satisfaction, or the confidence the system transmits, is defined by a security policy which creates rules of what area what are not allowed in the system. Security policies are important to the security management strategy. An SOE's electronic information assets are amongst its most important and crucial assets. These electronic information assets are constantly exposed to threats during storage, processing and transmission, that is, unauthorized access, unauthorized changes and loss, which, if they materialize, can result in risks that can damage the electronic information assets and have serious consequences for the SOE, (Tarantino et al, 2008). Information that is processed in almost all SOEs in Zimbabwe is either processed manually or electronically (involving the use of information technology (IT) equipment). At times the information is exchanged electronically using facilities such as the internet for file transfer or e-mails. These facilities provide fast exchange of information; they also possess great danger of divulging the information to the unintended recipients. Information about the organization may be compromised to the extent that it may be regarded as information espionage.

II. INFORMATION SECURITY GOVERNANCE (ISG)

ISG is defined as the organization's management responsibilities and practices that provide strategic vision ensure objectives are achieved, manage risks appropriately, use organizational resources responsibly, and monitor the success or failure of the information security programs (IBM Global Business Services, 2006). According to IBM (2006), ISG relates to the protection of valuable assets against loss, misuse, disclosure, or damage. In this context, valuable assets are the information recorded on, processed by, stored in, shared by, transmitted from, or retrieved from an electronic medium. The information must be protected against harm from threats leading to different types of impacts such as loss, inaccessibility, alteration, or wrongful disclosure. While there are many characteristics to IT security governance, an all-inclusive definition is difficult to contextualise. Leading practice dictates that IT security governance defines the core IT security principles, the accountabilities and actions of an organisation, to ensure that its objectives are achieved. IT governance provides outcomes specifically focused on aligning IT with the business while security governance provides

outcomes specifically focused on aligning security with the business, including both physical and IT security. As depicted, IT governance and security governance contain a number of similar attributes which is IT security governance.
The different focus of IT governance and security governance results in an overlap of activities, with this distinction ensuring that the IT security governance framework is not solely driven from an IT point of view, (CIO, CISO and Practitioner Guidance, 2009).

III. RESEARCH DESIGN METHODOLOGY

The study was targeted at examining the implementation of information security governance in SOEs in Zimbabwe. An exploratory study was conducted using semi-structured interviews to collect data from a simple random sample. The data was classified according to quantitative and qualitative structures. The data was arranged into tables and for simple interpretation. Classification of data took the form such as agree, strongly agree, disagree, true, false, not sure. This study was based on SOEs in Zimbabwe.

Currently there are approximately 66 governmental organizations in Zimbabwe. Some of the SOEs include, Environmental Management Authority (EMA), Zimbabwe Tourism Authority (ZTA), Zimbabwe National Road Administration (ZINARA), National Oil Company of Zimbabwe (NOCZIM), Minerals Marketing Corporation of Zimbabwe (MMCZ), Zimbabwe Revenue Authority (ZIMRA), Tobacco Industry and Marketing Board (TIMB). Using a non-probability, convenience sample technique, a cross-section of ten (10) SOEs were chosen for this study. Interviews were also carried out with a composition of 13 Board members, 18 Executive management and 26 IT Executives. A semi-structured interview questionnaire was developed for the Board members and the IT support staff to respond to. The interview questions were developed based on ISG guidelines for boards of directors and executive management issued by ITGI (2006). The interview questions were divided into three main sections. The first section collects general information about the characteristics of research sample and respondents' profiles. The second section of the interview questions collects information regarding the importance and implementation of ISG in SOE organizations, while the last section of the interview questions includes a self-assessment checklist of the implemented ISG practices in SOE organizations. The questions were of an open ended type to encourage respondents to explore their own experiences, perceived success factors and measures undertaken to secure information. The reality as perceived by the respondents had to be described in terms of the meaning respondents attach to the elements of the field of study they were questioned about. The data was then arranged into tables and for simple interpretation.

Multiple sources of the data and knowledge was required since the study wanted to understand the respondents insights, experiences, cultures and the ways they interpret and understand information security governance. The small selective sample is related to the in depth nature of the qualitative approach (Carr, 1994). The advantage on non-probability technique was that the population elements are selected on a basis of their availability. This was the case when most of the sampled elements volunteered to take part. Also the researchers used their personal judgment to select the elements during the research. The researchers also visited SOEs identifying elements to be used in the research. During the research it was very difficult to interview some Board members and other senior executive members of most SOEs due to the nature of their duties. The issue of multiple sitting by some Board members was cited as factor that made it difficult to arrange interviews with some Board members. This resulted in a small number of Board members being interviewed during this research. Most Board members were engaged in business meetings and travelling. Appointments for interviews with some Board members were done but some of the Board members did not fulfill the arranged appointments. This made the research difficult as required input from the Board members were only obtained from 13 Board members.

IV. DATA COLLECTION AND ANALYSIS

The interview questions posed during the semi-structured interviews were validated through the approval of the method by three experienced people in the field of social science research, and one information security expert. The interviews were arranged and conducted with all of the participants at the convenience of the interviewee and took place in the interviewees' offices. Confidentiality of the data was guaranteed by use of pseudo names by the participants during interviews. All participants requested that anonymity be guaranteed this was done by the researchers by not publishing any data specific to one organization.

V. RESEARCH FINDINGS

The views collected from the overview interviews of IT support staff have been used in the discussions of the related responses. Different success factors were derived from the findings. In this study, an empirical survey, using a self-administered questionnaire, was conducted to explore and evaluate the current status and the main

features of ISG in the Zimbabwe environment. Most Board members complained of tight business schedules. In light of these reasons, the researchers believes that the collected questionnaires were enough for data analysis and adequate to achieve the purpose of this exploratory study.

IT security awareness

Not even one of the SOEs in the study had a formal security awareness program for the staff and the various departments. The IT departments were more likely to have such programs than other departments but only a pocket of knowledge was available from the IT departments.

IT security policy

The SOEs indicated that they had no formal policies covering IT Security, most SOEs had interim policies or policies in progress. Another interesting finding of the study was the importance of the active engagement of SOEs senior management in the policy development. The gap between security as a top issue and as a priority in the government organizations is particularly worrisome, given the challenges of ensuring adequate IT security. The security policy is expected to be a high-level document, describing the security goals the organization is expecting to achieve and not the procedures involved therein (Barman, 2001). The policy document is thus an indication of management's commitment towards information security and due diligence. At the same time people to implement controls and initiate procedures for achieving the stated security goals. The task of breaking up the high-level security policy into actionable, implementable components is thus the responsibility at the middle-level.

Information security management in SOEs

It is important to keep in mind that each SOE must implement the system that works best in their specific situation – there is no one-size-fits-all system. Security management is a business-like approach to security. As with any business plan, goals are set, levels of authority are established and so on. Ultimately, security management becomes knitted into the fabric of the organization and becomes part of its culture. In SOEs this has to be improved by allowing the qualified personnel to be responsible for issues encompassing security management as this a key component of most organizations. As with most SOEs concentration has been on physical security only but failure to define information security, its generation, delivery and safe keeping. In order to have an effective security management system, it should include the following key elements and sub-elements.

SOEs may choose to group or break down these elements and sub-elements in different ways, in accordance with their own security management system structures, but the each objective of the elements should include senior management commitment, resource management, threat assessment and risk management, management of emergency and incidents, quality control and quality assurance and relevant security program suitable in that particular SOE. A clear organizational chart of the security department should be drafted where all necessary responsibilities have a dedicated point of contact. The organizational chart should be proportionate to the size of the SOE. This is the missing link in many SOEs as security management issues are either engrossed as make shift and not accorded its rightful position with the SOEs. Communication of security information is a very important part of the senior management commitment.

The role of board and management

As boards of directors and corporate executives wrestle with regulatory and legal requirements and the need to maintain the integrity and continuity of business processes, the concept of information security governance takes on added meaning and importance. Governance, as defined by the IT Governance Institute (ITGI) (2006), refers to the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly. Since information is a vital resource for organizations, it is important to ensure that information security activities are integrated into the corporate governance structure. Organizations need to understand the importance of security as a component of as a component of corporate governance. Zimbabwean SOEs implements new technologies prior proper planning on information security. Senior management at most SOEs seem not to be sure of what exactly the IT personnel do to ensure sound security. The Board needs to be aware of a proper information security governance framework. Also the Board and senior management at SOEs are supposed to lead in the crafting of security policies and policy development and ensuring that individual roles and responsibilities are clearly communicated and understood at all levels.

After a policy has been approved by the governing body of the organization and related roles and responsibilities have been assigned, there is need to develop a security and control framework that consists of standards, measures, practices and procedures (Nolan and McFarlan, 2005). Most board members frequently lack the fundamental knowledge needed to ask intelligent questions about IT risks and expense. This leaves the CIOs, who manage critical corporate information assets, pretty much on their own. A lack of board oversight by the Board concerning IT activities is dangerous; it puts the firm(s) at risk the same way that failing to audit its does.

In Zimbabwe a few SOEs are battling to implement these security standards. This is due to the fact that senior management and the Board at times are not aware of what exactly needs to be done on IT information security governance issues. As alluded by Dale Vile, Freeform Dynamics Ltd, October 2011 "In our environment, some senior executives and some associates will insist on what they want the company to provide in the way of communications devices". "Senior management will change or overrule the rules as needed". This possess a great danger to issues of security management within organization the CIO is left alone because he is not able to argue with his or her bosses, resulting in the CIO bending the elbow to the senior management demands.

VI. DISCUSSION

This study has provided evidence of a major security problem in Zimbabwe SOEs and this may lead to them experiencing security problems as a result of not implementing basic and necessary countermeasures. Despite the fact that an IT security policy is a basic IT security tool, Zimbabwe SOEs appear to be lagging behind in this aspect. From the survey it is evident that some SOEs do not have IT security policies. The length of time an SOE has been in operation and how long it has been using computers in its operations are key determining factors to how widely acceptable information security framework are implemented. Zimbabwean SOEs are struggling to provide a sound IT infrastructure for information processing efficiency and quickening of business turn-around processes.

The practice at most SOEs organizations is that hardware and software acquisition is done without reference to a well-defined operational and procedural security framework. The main reasons to what causes this practice is that at several SOEs the matters of information security governance is not documented enough especially in areas where it supposed to clearly state the information security concerns of the organization. The top management is supposed to craft the operational and procedural frameworks within their organizations and if they are not aware of what should be done concerning the information security governance framework, it makes it difficult to address issues on information security. So how can the issues of information security addressed with or given a notice when the head of any organization is not aware of what should be done concerning information security governance. The SOEs top management should be the ones crafting the operational and procedural frame works within their organization. According to ITGI (2006), "it is a fundamental responsibility of senior management to protect the interests of the organisation's stakeholders. This includes understanding risks to the business to ensure that they are adequately addressed from a governance perspective, to effectively manage the risks including information security risks by integrating information security governance in the overall enterprise governance framework of the organization." In the SOEs successful implementation of information security governance should start from the senior management of the organization. They should show commitment to Information Security initiatives, when this is done dove-tailing with business components would be easy. This has been a complicated component in Zimbabwe SOEs because of several reasons such as failure by the senior management to understand and coordinate IT security issues.

The management should understand the information security issues and use it as one of their key component for business continuity success factor. This may entail an organization has to establish key personnel such as IT security personnel, in their traditional organizational structures. The duty of the IT security person would be overseeing all IT security threats and maintaining business continuity. The Zimbabwe SOEs, this concept of incorporating IT security personnel has not yet been implemented in most of the known SOEs. It was observed that at most SOEs; there was no establishment for a post for IT Security personnel. This illustration means that the senior management does not understand the information security governance issues.

For the successful implementation of information security governance, planning on information security prior to implementation of new technologies needs to be observed; in most SOEs this area is still grey. No proper planning is being done prior to adoption a new technology. The SOEs are rushing to adopt the new technologies without exactly understand the security issues which needs to be setup prior to usage of the new technology. Taking for example other organizations have installed wireless access point without security key or with very weak key that may lead to hacking of company vital important information. The integration between business

and information security is another issue that can bring successful implementation of information security governance. Business components need to be incorporated together and monitored. Information generation including its upstream and downstream movement has to be integrated together as well. Information security mechanisms put in place should allow a steady flow of information not to completely restrict movement of information.

Alignment of information security with the organization's objectives is a very important factor that leads to a successful implementation of information security governance. Security mechanism and countermeasures should be aligned with to the organization's objectives. The Executive and line management should be aware and be involved in the information security governance issues such as ownership and accountability for implementing, monitoring and reporting on information security for there to be success. In most SOEs the management hierarchy is not involved in the information security and they seem not to be aware of dangers associated with information security threats and risks.

Consequently, this study recommends that IT governance should be put on the agenda and the Information Systems Auditors (IS Auditors) can ensure that organization adhere to the recommendation. When the IT governance is on the agenda chances are that the senior management would discuss issues of IT security governance. SOEs are depending more on their IT infrastructure but they lack the means to secure it appropriately due to inadequate know-how. SOEs can be made adequately aware of IT security issues through regular education and training.

VII. CONCLUSION

The area of IT security governance in SOEs in Zimbabwe is still at its infants stage due to several reasons such as the spear heading ministry was only instituted less than five years ago. The national ICT Policy framework was drafted and adopted recently. This on its own possesses a great challenge to the implementation of IT security governance in SOEs. This means issues of information security governance in Zimbabwe SOEs still remain at the foundation stage but in roads in the area of information security governance are being pursued. Further research can look at ways of assisting SOEs particularly in Zimbabwe come up with comprehensive IT information security governance policies and sensitizing SOEs management about proper IT information security governance frameworks including well-articulated IT security standards. All SOEs in Zimbabwe are encouraged to practice good information security practices by safe guarding all information procedures and cycles. It is recommended that the SOEs use IT governance frameworks such as COBIT, ITIL and BS17009. There is need for further research to also address issues related to the evolution of ICT usage and their implication to IT information security governance in SOEs in Zimbabwe.

REFERENCES

[1] Bailey, I, 2013. Chief Information Security Officer-Information Security Program for the BC Government, Washington: UWC Press

[2] Benson V & Davis K, 2009. Business Information Management, Denmark:Ventus Publishing

[3] Brisebois, R, 2009. IT Governance - What is IT Governance & why is it importance for the IS Auditor

[4] Carr, L.T. 1994. The Strengths and Weaknesses of Quantitative and Qualitative Research: What Method for Nursing? Journal of Advanced Nursing

[5] Caruso, J.B, 2003. Information Technology Security: Governance, Strategy & Practice in Higher Education, New York: [Educause Center for Applied Research (ECAR)]

[6] Colin B, 2005. Guideline For IT Management – Aligning IT with Business Strategy, Washington: WUC Press

[7] Dos Santos Moreira, E, Luciana, A, Fondazzi, M, 2002. Ontologies for Information Security Management & Governance, Brazil: Rio Press

[8] Gottschalk, P, 2010. Policing Cyber Crime, Denmark:Ventus Publishing

[9] IBM Global Business Services, 2006. USA: IBM

[10] ITGI, 2000. COBIT (Control Objectives for Information and related Technology) 3rd Edition, 2000, www.ITgovernance.org andwww.isaca.org

[11] ITGI, 2006. Guidance for Boards of Directors and Executive Management, 2nd Edition, available from www.isaca.org

[12] ITGI, 2006. Information Security Governance – Guidance for Board of Directors and Executive Management , 2nd Edition, Available from www.isaca.org

[13] John, P, 2006. Information Security Governance: Motivations, Benefits and Outcomes. USA: Information Systems Control Journal

[14] Nolan, R, Richard N, 2005. Information Technology and the Board of Directors, USA: Harvard Business Review

[15] Scot, P, 2012. Security Policies for Next Generation IT , USA: Tech Target

[16] Vinod, P, Rajendra, S, 2004. Identifying Linkages between statements in information security policy, procedures & controls, SJM School of Management, Mumbai: IIT Bombay