The Strategy Detection on Information Security in Corporate Organizations on Crucial Asset

Yakubu Ajiji Makeri#

*School of Computing and Information Technology, Kampala International University, Uganda
E-mail: yakubu.makeri@kiu.ac.ug

Abstract—Information Security is a crucial asset within an organization, and it needs to be protected. Information System (IS) Security is still a significant concern for many organizations. It is profoundly crucial for any organization to preserve Information System (IS) Security and computer resources, hardware, software, and networks, etc. The Information System (IS) assets against malicious attacks such as unauthorized access and improper use. This research, we developed a theoretical model for the adoption process of IS Security innovations in organizations, are numerous measures available that provide protection for organization IS assets, including (hardware, software, networks, etc.) and antivirus, firewall, filters, Intrusion Detection System (IDS), encryption tools, authorization mechanisms, authentication systems, and proxy devices. The model is to derive by the four combining theoretical models of innovation adoption, namely, the Theory of Planned Behaviour (TPB, Diffusion of Innovation theory (DOI), the Technology Acceptance Model (TAM),) and the Technology-Organisation-Environment (TOE) framework. The Computer security education needs to consider as a means of combating threats (Arachchilage and Arachchilage et al., 2016). While the process of innovation assimilation is as a result of the user acceptance of innovation within the organization. This model depicts security innovation adoption in organizations, as a two decision proceeding for any organization. The stage until its acquisition of innovation and adoption process from the initiation is considered as a decision made any organization. The The model also introduces several factors that influence the different stages of information Security and the innovation adoption process. Adoption of IS security measures by the individuals and organizations.

Keywords—Information Security.

I. INTRODUCTION

In many nations across the Africa and globe, cybersecurity is accepted as a national priority (Center for Strategic and International Studies, 2011). According to Sharma (2012), lack of cybersecurity can cripple the economy and safety of an entire nation. This is owing to the apparent dependence on cyberspace to perform functions deemed critical to the wellbeing of individuals, organizations, and countries. Such reliance on cyberspace is speedily shifting Internet access from being a 'luxury' for a few to becoming a 'basic human right' for all (Zeldin, 2012). Although the ever-increasing reliance on cyberspace should solidify the need for cybersecurity, nations like South Africa (SA) still lag behind.

State of information security In Africa

The state of computer crime in different from other countries all over the world, where the rule of information technology security in Africa and all is affected organization by many factors such as IT infrastructure, growth of IT end-user and responsibilities for maintaining security in the organization. The management and most technical people, employees, vendors, and contractors have different parts of developing and implementing an effective security process. For this paper will look at the roles and responsibilities of management, Information Security Department, and professional and users in achieving and maintaining information security management system (ISMS) in the organization.

Technology Infrastructure Security.

Top Management Support

Information security in today's organizations, be understood as a domain of professionals who install and configure equipment and software. According to many presidents and directors, their companies are well protected by firewalls, antivirus, data encryption, and password systems. However, as practice shows, the technical security will never be sufficient to deter those interested in gaining organization assets. A recurring, organizational factor studied by IS researchers is top management support top management support is one of the consistently found and highly critical factors that
influence IS implementation. They responsibilities of Management’s goes beyond the basics of support they must set the tone for the entire program. The comprehensive range of security measures in the form of physical controls, procedural controls, and technical controls would thwart almost all kinds of security breaches. Were examined to keep secure the sensitive company information, with the corporate security policies (e.g., restricting access to confidential personal information). They Password policies (e.g., all system-level passwords must be changed on at least a quarterly basis) and disciplinary procedures. Just to bless the program a Management must own up to the program by becoming a part of the process. It’s the responsibility for implementation, development, maintenance. This is defining the information security objectives of the organization, how to allocate an amount of money to be invested in information security within the organization, and ensuring the compliance and enforcement of implementation.

Organisational IS Readiness

Determinants of Security Innovation Adoption

The IS security adoption model, we considered technology, organization, environment, and user acceptance attributes that were examined in the past IS innovation adoption literature. Also, each of the factors included in the proposed model has been reviewed found to have a significant influence on IS security innovation adoption research.

The Management should also ensure that the security controls the organization by performing the following:

(i) To ensure the security process by organizational policies and practices that are consistently applied,
(ii) They Require any information with similar criticality and sensitivity characteristics be always protected regardless of where in the organization it resides,
(iii) The Enforce and compliance with the security program in a balanced and consistent manner across the organization and Coordinate information security with physical security.

II. DIRECTION AND STRATEGY

The ICTs, use, in particular, the Internet has become a matter of strategic importance. Meanwhile, free, secure and open Internet is an engine for the economic growth of any organization and social development that facilitates communication, innovation, and business transformation. The challenges in our societies become interconnected and dependent on the Internet and ICTs, we become more vulnerable to the misuse of these, and we need to ensure that internet security of our ICT infrastructure is improved. To maintain its integrity as well as users’ trust in its reliability to any organization, National cyber-security technologies, in line with international strategies, and technologies practices, and it’s taking into account the Cyber Security and Personal Data Protection law;

i. Support the creation of national governance on defining roles and responsibilities of the stakeholders on Cyber-security;
ii. Develop legislation Legal and Regulatory frameworks and specific provisions related to cybersecurity;
iii. Enhance technical capabilities to monitor and defend national networks;

Evaluation of cybersecurity strategies

Objectives in NCSS the objectives of cybersecurity strategies reflect the differences in national contexts. However, there are some similarities between the European approaches. Cybersecurity strategies often have goals to articulated around the clusters, which are reflected in the purposes of the Cybersecurity Strategy of Africa

(i) To achieve cyber resilience: develop capabilities and cooperating efficiently within the public and private sector
(ii) To secure critical information infrastructures
(iii) To reduce cybercrime
(iv) To develop the industrial and technological resources for cybersecurity; and
(v) To contribute to the establishment of an international cyberspace policy

Contingency theory

Contingency theory states that the best way to structure and manage organizations. According to their research based on the management of innovation, Burns, and Stalker (1968), found out that organizational systems should vary based on the level of stability in the environment. Contingency approach is to recognize and respond to situational variables to attain corporate objectives effectively (Drazin and VandeVen, 1985). Contingency management is to manage the interaction between a set of environmental variables and another set of technological and managerial variables, and the goal is to strive for the attainment of organizational objectives (Lee et al., 1982; Luthans, 1976). Therefore, to take on policy-oriented managerial activities or risk management activities is dependent upon an organization's contingency strategy. This theory informs the study since the contingency approach has been applied to information security management. For example, Solms et al. (1994) proposed an information security model (ISM, which consists of five information security levels: ideal; prescribed; baseline; current; and survival. Except for the perfect level, all the other four levels are dynamic and contingent upon environmental variables such as information security threats, vulnerabilities, and impact for an organization. The procedures for coping with organizational information security problems are most undefined since the processes are
dependent upon several situational variables. Therefore, to take on policy-oriented managerial activities or risk management activities is dependent upon an organization's contingency strategy.

**Coercive Pressures**

They Coercive pressures force organizations to adopt specific traditional rules and practices in managing the organization for information security. The government laws and regulations; Such pressures force organizations to act in compliance with particular standards and practices for information security to receive legitimacy with the laws and rules Existing. According to Dhillon and Buckhouse (2000), there is a critical need to protect information and to manage the security of Information and Communication Technologies (ICT) systems within organizations. The laws and regulations are made for the protection of data in an organization to satisfy the requirements of various stakeholders for information security in organizations have to gain legitimacy. Also, organizations have to adopt multiple information security practices to provide the foundation for building a robust response to regulatory requirements. Existing laws Such legislation may cover not only privacy/data and regulations influence the commitment of organizational management towards information security compliance. Such an impact is reflected by the change of the attitudes and behaviors of management towards information security in organizations. Usually, the administration is responsible for ensuring that their organizations comply with applicable laws and includes regulations for information security. Failures to incorporate specific legal requirements in their information security practices for meeting the legal obligations for information security as a result of concerning information security in organizations (Hu et al., 2006; Liang et al., 2007).

**Normative Pressures**

The Normative pressures come from the community expectation that organizations are compelled to honor as responsible citizens in a specific circumstance and the decision to adopt new practices is often influenced by how organizational stakeholders take actions concerning the latest methods. The pressures are raised from the values and norms that are embedded in the organization for information security. Organizations are likely to adjust their behaviors on what is viewed as appropriate among members of their social networks and consequently adopt techniques and methods that reflect the current standards of those networks, this implies that organizations are subjected to specific pressures exerted by the expectations of stakeholders within a particular time. The privacy and quality of services, for example, are desirable social needs in today’s dynamic environment that must be adequately addressed in organizations. These desirable social needs put organizations and their management in the spotlight; In many cases, organizations will implement useful capabilities only if those capabilities will reduce their capital and operational expenses.

There is abundant of literature supporting the use of normative pressures for enhancing information security compliance (Appari et al., 2009). Demonstrate the different community pressures have an impact on information security compliance in public organizations in developing countries. The stakeholders’ expectations of information security generate specific loads in organizations strengthen their information security practices based on the above discussion, the study argues that normative forces are exerted mainly through social forces that influence information security compliance in organizations and strengthen management commitments towards information security compliance.

**Mimetic Pressures**

Mimetic pressures refer to the acquiescence by imitating peers to gain organizational legitimacy (DiMaggio & Powell, 1983). Such demands are present when an organization adopts the same actions, structure, and behaviors of similar organizations within their environments for gaining legitimacy. Understanding of the Mimetic pressures causes to imitate success action, and practices took by such as competitors and business partners along the supply chain within their industry successes serve as the basis of the desirable imitation, especially when organizations face similar needs and hoping for same success within.

A better approach often is to analyze the impact of not being compliant or becoming only partially compliant and implement and operate information security practices in terms of minimizing risks and threats, increasing stakeholder’s confidence, trust, and improving employees’ performance, and reducing the negative impacts on organizations. The organizations publicize their perceived benefits; they create pressures on other organizations to take actions concerning their information security practices. The perceived benefits may exhibit individual personality characteristics to imitate their successful peers to behave. Similarly, organizations with adequate information security practices influence employees’ behaviors to conform to industry norms.

**Management Commitment**

Management commitment is a reflection of the efforts of senior management to promote information security compliance in organizations. It is related to the decisions, investments, and actions are taken for enforcing information security standards and policies across the organization. The Commitment from top management is significant for information security compliance in organizations since their decisions usually drive the operational practices across the organization. The understand information security as a core competency in organizations could have direct implications for business survivability. Senior management should provide visible support and a real commitment to information security compliance in their organizations.

Management commitment is an internalized organizational pressure that affects the behaviors of employees in complying with information security standards and policies. The participation, communication, and championing of senior management stimulate employees’ intentions towards information security compliance and encourage the adherence to ensure information security standards and policies (Kolkskwska & Dhillon, 2012). Management commitment has a strong effect on employees’ information security compliance within. Such conceptual model hypotheses that institutional pressures have a positive impact on information security compliance in organizations.
It further assumes that institutional constraints affect senior management commitments towards information security compliance the conceptual model with the identified constructs and their associated attributes.

A Structural Model

The significance of the structure model is tested using the paths coefficient and the explanatory power for each dependent variable (R²) (Byrne, 2013). The hypothesized model contains five constructs, as shown in Figure 1. The hypothesized model, with the path coefficient and the explanatory power (R²) for each dependent construct, is displayed in. All factors on hypothesized paths except for the path coefficient from social pressures to management commitment are found to differ from zero significantly (p<0.05 or p<0.01), as shown by the dotted lines.

III. THE RESULTS

The results of the model indicate strong support for H1, H2, H3, H4, H6 and H7 with path coefficient values ranged from 0.42 to 0.74 respectively (p <0.05 or p <0.01). The results are to be reject H5implying that social pressures have an insignificant effect on management commitment for information security in organizations. The terms of the explanatory power, the model accounts for 76% of the variance in coercive pressures, 60% of the variation and normative pressures, 67% of the variance in mimetic pressures, and 70% of the difference in management commitment. With this result, the study can conclude that all hypotheses except H5 are supported to reduce theirs.

This confirms the significance of institutional pressures on information security compliance in organizations with to gain legitimacy from all the stakeholders. The study has stressed the importance of coercive pressures and mimetic pressures for influencing management commitment towards information security compliance. The insignificant effect of social pressures on management commitment towards information security compliance suggests that management commitment towards information security compliance is not dependent on the presence of social tensions in the external environment. Ensure the availability and capability of permanent staff for the strategy execution. It reinforces the assumption that the higher impact of coercive pressures exerted by regulatory agencies and the mimetic that is through the influences of security benefits among partners, the higher the commitment of the management is towards information security compliance in the organization. The implementation phase and operation includes taking global considerations into account. (Porter, 1990). Defined strategy implementation as the process of allocating resources to support the chosen strategies. In practice, how institutional constraints affect the information security compliance process in organizations, the various management activities that are necessary to put the policy to the implementation such findings to organizations with valuable suggestions on how organizations can improve their information security compliance.

IV. CONCLUSION

This study proposes and validates a hypothesized conceptual model in evaluating the impact of institutional pressures on information security compliance in organizations. It shows that there is strong support for six hypotheses and no support for one of the seven hypothesized relationships in the proposed conceptual model. Specifically, this study demonstrates that institutional pressures have a positive impact on information security compliance in organizations. It clearly indicates that law and regulation and security benefits have a direct effect on management commitments towards information security compliance in organizations. Such findings underscore the importance of having institutional pressures for effective information security compliance. There are several limitations in this study, which can be addressed in the future; ultimately, objective measures of information security compliance should be considered. The second, the research findings remain limited since these findings have been validated in a single organization in one country. Further studies should consider incorporating psychological, technological, and factors for enforcing information security compliance in organizations.

REFERENCES

[1] Posthumus, S., and von Solms, R. 2004. "A Framework for the Governance of Information Security," Computers & Security (23), pp 638-646.
[2] Posthumus, S., and von Solms, R. 2006. "A Responsibility Framework for Information Security," Security Management, Integrity, and Internal Control in Information Systems (193), pp 205-221.
