An Evaluation of Security Governance Model in Organizational Information Technology or Information Systems Security Implementation

Dayang Hanani Abang Ibrahim, Nadianatra Musa, Chiew Kang Leng
Faculty of Computer Science and Information Technology
Universiti Malaysia Sarawak
hananii@unimas.my

***Abstract*—The study was aimed to investigate the security governance model in organizational IT security implementation. A triangulate design has been applied to data collection from three sources websites, interviews, and survey. Automatic security measures controls have been adopted to minimize and control the human actions and the correspondence with the system. Important elements depicted from the findings include directing and monitoring actions within the IS/IT security. The IS/IT security governance model of the inter relationship among the three components of the Formal, Technical and the Informal are important to achieve the good practices of IS/IT security. The educational concept may also increase the organisational and the employee values. The study has affirmed positive prevalence of the trend that most of the companies are now considering to implement IT/IS security models for protected data.**

***Index Terms*—Data; Information; IS/IT; Model; Security; Threat;**

I. INTRODUCTION

Security governance as a system refers to a rule conceived by corporate performers and individuals targeting at managing, coordinating and regulating the overall existence in regards to threats to their ontological and physical security. The ruling systems chiefly depend on the political authorities of agreed-upon institutions, practices, and norms as well as on the technologies, spatial forms, rationalities and identities across which transnational and international security activity takes place. In the present study, the security practices have been discussed along with their mechanisms from which they are derived.

The self-interest of organization can be enlightened by implementing the effective IT security program. Companies are taking serious actions to preserve their information commended to them by suppliers, customers, and their partners. They are maintaining the responsibility for the companies' security plans and adopting the programs to address and evaluate the internal and external threats and vulnerabilities of the economic information.

Mechanisms of the security governance are apparently delineated set of norms, rules, and practices that coordinate the security associations in the International system between performers. The association between the norms and individuals that motivate specific mechanisms of security governance is constantly and mutually re-enacted. The State or city-states (units) may constitute the mechanism of the power of balance through the practices. This mechanism constitutes this unit in a specific relationship based on sovereign *deterrence* and independence. Concerning the rising abundance of regulations, rules, and guidelines, it becomes apparent that information security is not just a technical issue, but it is an organizational governance challenge. Increased scrutiny is being faced by the businesses today when it comes to accountability, ethics, and governance.

Lack of involvement by the board and senior management in understanding the IS/IT security issues and improper implementation plan of IS/IT security within the formal, informal and technical components has led the study to focus on the evaluation of security governance model. It might be important to focus on the limited internal control applications over IS/IT security. The gaps in the literature have led to the development of two important research questions, which have driven the development of the conceptual framework and the model of IT/IS security governance:

Question 1: In what way do the involvement of Boards and senior management impact on the implementation of IS/IT security governance?

Question 2: How can directing and monitoring actions in the technical, formal and informal components of IS/IT security governance in corporations be implemented effectively and efficiently?

The conceptual framework has been extended by incorporating the security governance model, which suggests various areas regarding the elements of the three components formal, technical and informal and component interactions (Relationship Type 1-Formal/Informal, Relationship Type 2-Formal/Technical and Relationship Type 3-Technical/Informal) within Malaysian Publicly Listed Corporations. The risk management and internal control practices are ought to be included in the IS/IT security according to the suggested model, through monitoring and directing actions. It also emphasizes the relationship between the holder and supervisor of the responsibility. Because the nature of the study is confidential and sensitive so, the study has opted a triangulation method to eliminate the research gap.

The study has contributed to enhance the IS/IT security governance process, which is a complicated task and requires the giver/supervisor and the holder of the responsibility to resolve the issues in an effective and efficient way at minimum risk. Failure to understand the responsibilities in discharging IS/IT security may bring the

potential risks to the organization such as bad reputation name of practicing IS/IT security, loss of money, loss of potential investors for publicly listed corporations.

The IT/IS governance model may suggest the role of supervision in the monitoring and directing actions over the elements of the formal, informal and technical components and the component interaction. The elements of these components and interaction component may serve as an indicator or checklist for the organizations to ensure the achievement of IS/IT security governance.

II. LITERATURE REVIEW

Computers have a long association with the field of mathematics and science to evaluate the critical problems. First, of the operating computers have been known to be developed in 1940's during the period of World War II. However, due to the lack of appropriate technologies and concrete framework; the scientists were unable to develop the computer on time [1]. Later on after few years of progression, one of the prominent personalities in the field of the computing sciences named Alan Turing came up with the remarkable discovery of the processing mediums. Moreover, possessed the capability of developing such algorithms that were capable of processing huge bulks of data. Therefore, since then the field of computing sciences has been witnessing such emerging patterns that are supplementing in the enormous growth of the domain. Right after the development of self-sustained processing mediums; the scientists found that the field was lacking some huge performance gap that was hindering the transmission of the data over the distant places. However, by 1965, the scientists were capable of transmitting the data over to huge distance; which includes the successful transmission of the instruction to Apollo 11 (the first carrier to take the humans to moon); yet they were facing some huge slackness that could have addressed the need for the data transmission [1]. In this regard, various techniques had been found to be under the phase of progression that could have supplied with the proposition of strategy to address the need of the situation. Thus, most of the government-funded projects have been known to be witnessed that were intended for the development of the solution. On this note, the humans were successful in transmitting the data over the Internet in 1970's which was in the form of first E-mail. Since then, the development of the Internet has taken a swift transition in the procedural norms that could have addressed the need for the data processing and transmission.

In the light of the recently observed progressions, it has been observed that the computers have replaced many of the manual procedure of recording the data. Ever since the development of the business procedures; most of the corporate sector and government level organizations have been engaged in the development of such practices that could have eased the storage of the data [1]. Moreover, recent advancements in the technological era have added millions of user to the Internet which has significantly altered the environment of the economic, social and political activities that are conducted. Therefore, the world has significantly been witnessed with such activities that can be termed to be boosting the procedural norms of the data storage. The development of Internet has supplied with ample of opportunities that can be used to store the data at the remote locations and access it accordingly. However, along having the added advantage of the remote access of the data, there comes an added risk of securing the data as well. In the past few years of the progression, the social media has provided huge opportunity to produce the data that is publicly available to the world. Therefore, it has also posed a higher risk of breaching the data; such that it can be easily misused for any of the purposes. On the other hand, huge scale enterprises, which include the government as well as the private organizations are also observed to be producing a massive amount of data that contains highly confidential data. Proper attainment of such data can easily help the intruder to plot such plans that can ultimately harm the well-being of the owner of the data [2].

In this regard, experts have come up with such remedial strategies that could be deployed to preserve the security and integrity of the data. On the other hand, multiple fraud ventures have also been witnessed in the past that can easily delude an individual; ultimately, costing the person a valuable asset. In this case, the most precious asset can be the data which can be manipulated such that, it produces some meaningful results. Some of the most popular strategies that have been found to be preventing such events are the deployment of the encryption techniques that transform the data in such form that it may not be understood by the intruder. However, there exist such algorithms that are capable of decrypting the data in a manner that, it can be transformed back to its original state. Therefore, the business disciplines have been engaged in developing a range of philosophies to labor the relations [2]. Thus, this investigation has been promoted by the confusion in the literature relating to the business disciplines and information technology/ information systems (IT/IS).

The sole responsibility for the application of information systems technology has been laid on the board of directors. One of the reasons for the subjected cause is that they can be the one approving the allocated budgets for the subjected cause. Therefore, the board of directors shall be the one that may improve or reduce the security of the data. Most of the organizations operating today are paying a little attention to the inter relationship between the: technical component, formal content and the informal content. Therefore, the board and the senior aspects such as the IS/IT management rather than on a comprehensive view. Hence, a slightest of the deficiencies may result in the unbalanced IS/IT security implementation. In further analysis of the literature, it has been inferred that there is a significant lack of the informal aspects that are being deployed that addresses the need of the IT/IS security [3]. Moreover, the compilation has focused on the technical implementation of the formal things such as the management involvement, standards, assessment of the standards and most importantly the certifications that are being deployed for the evaluation of the IT/IS issues.

In the light of the governance practices and previous studies, it has been found that majority of the IT/IS incidents have been the result of the continuous negligence of the company to address the need of the IT security governance [3]. Moreover, most of the cases have been the result of either intentional or unintentional motives of the employees. The intended actions may be the result of the malicious attacks that include: virus, worms, spyware, Trojan horse and etc. On the contrary, the unintended errors can be the ignorance of the situation, human error and trust, lack of integrity, lack of education, lack of awareness and most

importantly the appropriate provision of the training. In a whole, human errors, either intentionally or unintentionally have caused financial losses that may include the data and the non-financial losses that can include the loss of the confidence by the customers and most importantly the business reputations. Adding to it, the risk for the information system may vary. Even after the inclusion of the technical and formal aspects; the board and the senior management are evenly responsible for the IT risks that may be caused by the people issues.

In the elaboration of the IS/IT, it can be said that the security incident is the violation of the security policies or the standards that have been set in the books of IS/IT security practices. Considering the historical data, most of the IT incidents have been the result of the technical issues of the computer systems; more primarily the operating system [4]. In addition, the systems have also been the victim of the data leak due to the: flow of the information between the or across the computers and more importantly, the access to the computers. In this regard, the experts have evolved several formal methods that could have improved the multi-level mode where some of the information on the computer systems may have been the classified as to the higher level of the interaction of the computer users. On the contrary, the technical issues have caused some of the IS/IT security incidents [5]. In the deeper elaboration of the fact, most of the unresolved organizational vulnerabilities have led to the initiation of the attacks on the IS/IT applications. Therefore, it has been found that most of the commonly observed incidents have been the result of the poorly designed systems, which are susceptible to a variety of attacks including the computer viruses, computer fraud, and most commonly the computer hacking and cracking. In the light of the previously prevailed events, it has been found that the computer hackers were considered to be honored personalities [6]. Moreover, the same hackers were found to be considered to be working for 40 hours and were perceived to be fixing the bug that may have been encountered in the execution of the program. However, after the enormous progression of the prevailing conditions, the same hackers are considered to be one of the most significant threats to the IT professionals [6]. Therefore, it has created an added burden for the network security professionals to come up with such practices that can be applied in the field to eliminate such hazards of the data security [7]. According to previous studies, the data theft has been highlighted as one of the prominent crimes [8]. Therefore, exhaustive efforts are now being deployed in the field to address the need for the data security along with ensuring the maximum protection of the system from the unwanted intruders harming the system. The IS/IT security is categorized under three relationship types. The relations have been mentioned as under:

A. Relationship Type 1 (RT1)

The relationship between the formal and the informal components shall be termed as RT1. The implementation of the IS/IT security requires a balance formal and the informal components. Therefore, the formal component needs to be aligned with the informal components in order to lubricate the flow of the security system [8]. The informal components like the personal values and the organizational culture needs to be aligned with the formal component.

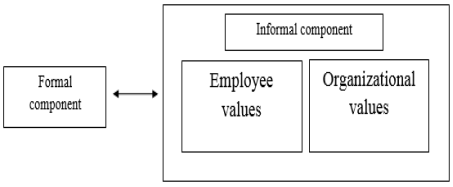

Figure 1: Formal component has a relation to the Informal component

B. Relationship Type 2 (RT2)

The RT2 considers the relationship between the formal and the technical components. The formal component sets the strategic direction for the technologies along with the technological implementations on the basis of the enterprise's visions and mission [9]. Therefore, it has been needed to develop the strategic flows such that, the formal components of the organization are in direct alignment of the technical components that are to be deployed for the system.

C. Relationship Type 3 (RT3)

The RT3 is the existence of the relationship between the informal and the technical components. The alignment of the components in this specific type of the relationship is to achieve the IS/IT security. Therefore, slightest of the misalignment can result in the production of heavy loss. The business losses in the organizations are due to the security incidents by the number [10]. According to the study, it has been found that 70% of the incidents have been the result of the minor negligence of the information security techniques. Therefore, it has been advised as a highly mandatory step to implement the information security at the huge scale organizations.

III. METHODOLOGY

This study has incorporated the use of the triangulated method to answer research questions. The goal of triangulation was to collect interview data (qualitative), mail survey data (quantitative) and website data (quantitative) to highlight the understanding of the research issues being investigated. The study collected the interview data primarily from the board members, senior and junior managers of Malaysian publicly listed corporations. Implementing the qualitative method, two types of secondary data were gathered, which included the organization's documents and website data. The data was gathered to strengthen the qualitative results and answer the research questions. The interviews were also conducted to collect data regarding how Boards and senior management thought about IT/IS security processes within their work-place. Mail survey and website analysis assisted in generating the data regarding the security awareness and attitudes towards IS/IT security governance. The triangulation approach has provided both the subjective and objective perspectives of the participants. Therefore, the data has been collected in three phases First of all; the data has been collected from the analysis of the website, in the second phase the data has been collected through the interviews. Finally, a survey was conducted via mail.

The first phase of the website analysis has been reported to keep the paper concise. Therefore, the sample population of the study has been divided into three groups. Group A has been categorized as the top group, Group B is deemed as the

middle group, and finally, the Group C has been named as the bottom group. The rankings of the groups have been done as per the capitalization recorded in Malaysia. Out of all of the phases, phase 1, phase 2 and phase 3 have been sourced from the samples of the three groups. The website analysis has been done from the annual reports of the domestic corporations. Moreover, the collected data has specifically been taken from the three groups of the companies that have been categorized above. Keeping in mind, all of the included companies have been categorized on the basis of the data that is either used or produced by the data centers deployed in the companies. In the light of the considerations of the facts, it has been found that IS/IT is the model of security governance and is a comprehensive conceptual framework. One of the supporting clauses for the mentioned statement is that the IS/IT governance emphasizes on the two-way relationship between each of the components. The main interaction between the three of the components that are: formal, technical and the informal.

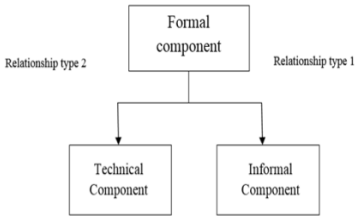

Figure 2: Relationships between Formal, Technical and Informal components

The analysis of the study has been done on the basis of the above-mentioned methodology. Therefore, the results are expected to be somewhat close to the endorsement of the application of the IS/IT governance in the huge scale business sectors.

IV. Results

The IS/IT security governance model of the inter relationship among the three components of the Formal, Technical and the Informal are important to achieve the good practices of IS/IT security. Therefore, understanding the reciprocal requirements among the components have enabled the board of directors and the senior management to consider the factors that are involved in the implementation of the IS/IT governance model. Therefore, the factors include the: business vision and goals, organizational culture, management strategy, technological fit and employee values, and beliefs.

A. The Relationship between Formal and Informal Components, Relationship Type 1

The inclusion of the educational concepts is one of the formal elements in the IS/IT security governance model. Moreover, the educational concept may increase the organizational and the employee values. The development of the IS/IT security management strategies of the formal components that may include the forums and the training are highly essential for the improvisation of the organizational values of the informal component. Thus, the application of the formal practices includes the provision of the training to all of the employees. The proper training shall result in the appropriate accountability of the respondents that are linked with the system. As a whole, the proper responsibilities and the roles separation of the duties shall result in the proper provision of the IS/IT security.

B. The Relationship between Formal and Technical Components, Relationship Type 2

The formal component is found to be highly significant for the technical component. One of the reasons for this cause can be; it is capable of providing strategic directions policies and strategies for the effective application of the technological resources along with following the IS/IT procedures. In other words, the collected data set has narrated the fact that, the IS/IT security policies have been developed to ensure the maintenance of the security over the IS/IT assets and the business data.

C. The Relationship between Technical and Informal Components, Relationship Type 3

The IS/IT security issue are not only linked to the technological issues, but they are also highly associated with the social problems. The components of the technical and informal needs to be aligned such that: they can be in proper collaboration with the subjected norms to implement the IS/IT infrastructure. The organizational value lies with the employees to achieve the business goals. Therefore, the employees have been found to be valuing the concerns in terms of the personal and the ethical values. Hence, lacking any of the formal procedures may reveal the discrepancies or unexpected behavior.

V. Discussion

Essentially, the software analysis supported the elements of the components, including the policy relating to internal controls and IS/IT security, security issues and risk management, organizational structure, educational aspects and informal aspects. The literature has been enhanced by the results of the software analysis.

All the issues recognized in the interview data have supported three dimensions, formal technical and informal. The elements of formal theme, which include IS/IT security vision and IS/IT security policy, have been supported by the analysis of the interview data. Similar ideas have also been presented within a model of component interaction and also the inter-relationship between the formal component, technical component and informal component. Relationship Type 1-Formal/Informal (RT1), Relationship Type 2-Formal/Technical (RT2) and Relationship Type 3-Technical/Informal (RT3) were the three types of component interaction supported by the interview data analysis.

The management roles among the supervisor and the holder of the responsibility have been explored, which supported the model of IS/IT security governance in terms of the elements of the formal components including the role of communities and IS/IT security policies. The supervision role between the supervisor and holder of the responsibility may be supported. The elements of the technical component including the implementation by entities/structures (IT department, IT committee, business division, and technical group), technical procedures progression, artefacts or the operational reports and project implementation methodology were also supported by the results.

The interaction of the three components are significant in the IS/IT security governance model. The component

interaction has three types that have been defining in the above-mentioned literature. A further collection of the data has been done through the websites that have been previously mentioned in the above literature. From the collected data, the educational aspect has been considered as the example of the formal component. Therefore, the IS/IT model needs to be supplied with ample of education so that, more and more users are capable of getting benefit from the educations of the IS/IT. As for the second type of the relationship, the IS/IT interaction policy has been found to be interacting in two ways with the technical components. Therefore, there exists a two-way relationship between the technological and the security procedures. Finally, the third relationship had an impact on the informal component. From the analysis, it has been found that the automatic security measures controls have been adopted to minimize and control the human actions and the correspondence with the system.

A study stated the praxeological view of the security technology that remains open to the adaptation of specific context despite the normative effects. It concluded that a constitutional framework is achieved with the help of technology that gives durability and stability towards processes and methods [11]. Moreover, extensive research also investigated the importance of information system security (ISS) within the industries and the implementation of Information security system management that can effectively nurture the participation of senior management [12, 13].

The findings of the study have emphasized that the data has supported the dimensions created in the IS/IT security governance model that supports mainly the major elements of security policies in the organization. It has been assessed from the results section that IS/IT security throughout the risk management, and internal controls applications emerged in Malaysian corporations. The important elements have been depicted from the findings, which include directing and monitoring actions within the IS/IT security. The IS/IT security governance was pivotal in supervising the role and responsibilities of the supervisor and the holder. Formal, informal and technical dimensions have emerged as effective components from the findings of across case analysis and single case analysis [13]. These dimensions were further sub-classified into themes that understand the context of IS/IT security governance. Furthermore, the findings have emphasized that group type and industry type are the two components that affect the practices of IS/IT security governance within the Malaysian publicly listed companies.

VI. CONCLUSION

The findings of this study have emphasized that the data has supported the dimensions created in the IS/IT security governance model that supports mainly the major elements of security policies in the organization. It has been assessed from the results section that IS/IT security throughout the risk management, and internal controls applications emerged in Malaysian corporations. The important elements have been depicted from the findings, which include directing and monitoring actions within the IS/IT security. The IS/IT security governance was pivotal in supervising the role and responsibilities of the supervisor and the holder. Formal, informal and technical dimensions have emerged as effective components from the findings of across case analysis and single case analysis. These dimensions were further sub-classified into themes that understand the context of IS/IT security governance. Furthermore, the findings have emphasized that group type and industry type are the two components that affect the practices of IS/IT security governance within the Malaysian publicly listed companies.

ACKNOWLEDGMENT

The author is very thankful to all the associated personnel in any reference that contributed in/for the purpose of this research. Further, this research holds no conflict of interest.

REFERENCES

[1] Flores, W. R., Antonsen, E., Ekstedt, M.: Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. Computers & Security, Vol. 43, 90-110. (2014). Doi.org/10.1016/j.cose.2014.03.004

[2] Herath, H. S., Herath, T. C.: IT security auditing: A performance evaluation. (2014). Doi.org/10.2139/ssrn.1534192

[3] Cherdantseva, Y., Hilton, J.: A reference model of information assurance & security. In Availability, reliability, and security (ares), 2013 eighth international conference on (pp. 546-555). IEEE. (2013, September). Doi.org/10.1109/ares.2013.72

[4] Kong, H. K., Woo, J. H., Kim, T. S., Im, H.: Will the Certification System for Information Security Management Help to Improve Organizations' Information Security Performance? The Case of K-ISMS. Indian Journal of Science and Technology, Vol. 9, No. 24. (2016). Doi.org/10.17485/ijst/2016/v9i24/96106

[5] Pearson, S.: Privacy, security and trust in cloud computing. In Privacy and Security for Cloud Computing (pp. 3-42). Springer London. (2013). Doi.org/10.1007/978-1-4471-4189-1_1

[6] Steinbart, P. J., Raschke, R. L., Gal, G., Dilla, W. N. SECURQUAL: An instrument for evaluating the effectiveness of enterprise information security programs. Journal of Information Systems, Vol. 30 No. 1, 71-92. (2015). Doi.org/10.2308/isys-51257

[7] Janahi, L., Griffiths, M., Al-Ammal, H.: A conceptual model for IT governance in public sectors. In 2015 Fourth International Conference on Future Generation Communication Technology (FGCT) (pp. 1-9). (2015). IEEE. Doi.org/10.1109/fgct.2015.7300242

[8] Hagen, J. M., Valdal, A. K., Pettersen, K., Gjerstad, B.: Evaluation of comprehensive security systems for public transport–a methodological approach. Journal of Risk Research Vol. 18, No. 7, 822-839. (2015). Doi.org/10.1080/13669877.2014.961512

[9] Mishra, S.: Organizational objectives for information security governance: a value focused assessment. Information & Computer Security, Vol. 23, No. 2, 122-144. (2015). Doi.org/10.1108/ics-02-2014-0016

[10] Mijnhardt, F., Baars, T., Spruit, M.: Organizational Characteristics Influencing SME Information Security Maturity. Journal of Computer Information Systems,Vol. 56, No. 2, 106-115. (2016).Doi.org/10.1080/08874417.2016.1117369

[11] Kaufmann, S.: Security through Technology? Logic, Ambivalence and Paradoxes of Technologised Security. European Journal for Security Research, Vol. 1, No. 1, 77-95. (2016). Doi.org/10.1007/s41125-016-0005-1

[12] Barton, K. A., Tejay, G., Lane, M., Terrell, S.: Information system security commitment: A study of external influences on senior management. Computers & Security, Vol. 59, 9-25. (2016) Doi.org/10.1016/j.cose.2016.02.007

[13] Gashgari, G., Walters, R., Wills, Gary: A Proposed Best-practice Framework for Information Security Governance. In Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security, (pp. 295-301) (2017), Doi.org/10.5220/0006303102950301