Internal Control and Standard Operating Procedures in Malaysian Corporations

Nadianatra Musa[1], Bob Clift[2]
[1]*Faculty of Computer Science and IT, Universiti Malaysia Sarawak, Kota Samarahan, Malaysia.*
[2]*School of Accounting and Corporate Governance, University of Tasmania, Hobart, Australia.*
nadia@unimas.my

***Abstract*—The security, standards, and related controls of IT/IS infrastructure along with its implementation in Malaysian Corporation has been the main focus of the study. A cross sectional analysis has been implemented, using the qualitative research design, to evaluate the importance of internal control and standard operating procedures. The interview data, website analysis, and mail surveys have been collected concerning the perfection of boards and senior management about the IS/IT security processes. Both the senior and board management are ought to be responsible and accountable to ensure that IS/IT risks are addressed in the standards and policies of IS/IT security. Success and failure of development are also the responsibility of boards and senior management. IT/IS procedures must be implemented by corporation to control the risk related with the use of operation and information systems that supports the mission of business.**

***Index Terms*—Board Management; IS/IT;Security; Senior Management.**

I. INTRODUCTION

In most of the countries, the corporate rules and principles about the responsibilities and power of the corporations are mainly related to theboard of directors [1]. It is apparently known that incompetence within the association and tolerance for dishonesty is observed as negligence [2]. There is a series of management models, standards, and case laws, suggesting the procedures and ways to the board of directors for operating the system. The interest of the study lies in the role of IT/IS that fits into the model of governance. The study has been designed in a manner that emphasizes the responsibilities,potential and role of IT/IS, which can contribute in developing the best outcomes for the interest of corporation [3]. The development of IT/IS model for the security governance might contribute to the decision of turf war that may enhance the practice of governance. The model is expected to provide with a structure for the advances of more general corporate governance framework that is presumed to be helpful for the organizations, using computers [4].

The literature has not presented any study that may have discussed the involvement of senior managements and the board of directors in IT/IS security governance among public listed companies in Malaysia. Eventually, no understanding has been found in the interaction of IT/IS security issues among the senior managers and other line managers. There are evidences that the major incidents and the failures of security in IS/IT were triggered by the staff members. For instance, it has been observed that many employees do not bring their problems,concerning the security of IS/ITto the observance of HODs or departments for many possible strategic policies [5]. The literature has suggested that incompetency of the senior managers and the boards with regard to the security problems related to the IS/IT may lead to ineffective security controls.

Threats and susceptibility have been identified as the major causes of the security issues. Yet, the Malaysian corporation has still not recognized the ways by which these susceptibilities and threats can be controlled [6]. The understanding to control these incidents is strongly encouraged as it can mark positive impact on supporting and protecting the IS/IT business information and assets. It is well known that if the business assets and information about IS/IT of the organization are exploited and remain in a susceptible state, they can lead to the failure of availability and integrity in the system [7]. If the integrity, availability, and confidentiality of business information are negotiated, corporations might incur indirect and direct losses to the business. For instance, in the case of Arthur Anderson, the commodity and service company, Enron and its auditor, the senior management was represented to be involved in the establishment of 'off-balance sheet' activities that helped to enhance the performance financially and increased the stock prices [8]. These evidences have represented that fraudulent behavior has been the key factor that lead to the fall of Enron (Services Company).Human error was also one of the main issues of Enron fall as it was presumed that the senior managers and board were incapable to recognize and defend the security threats and vulnerabilities, which lead to various security attacks [9].

A company, having IT/IS security control and standards, does not mean that IT/IS will be well mannered and managed as previously suggested by Baker, et al. [10]. Many past studies haveconcentrated on the absence and presence of security procedures and controls; however, limited focus has been directed to the quality of implementation. Baker et al. developed a web survey to generate a better understanding of the ways IS/IT procedures have been implemented to manage the security risks of assets and business.The web survey addressed 16 categories of general security domains. These security domains were intended to cover three components of formal, informal and technical elements. For example, the controls of antivirus software, like back-up and recovery, has been identified as a technical component. Business continuity and incident response were the examples of general security control domains for the formal component. Among all the 16 categories, none of them presented any informal component exclusively. It has been presumed that the informal component has been opted within the execution of both technical and formal components.

The study also aimed to explore the likelihood of a more

rigorous and structured approach to assess overall vulnerability of infrastructure. Also, the purpose included the idea to evaluate the importance of internal control and standard of operating procedures by analyzing the security standards and controls of IT/IS infrastructure implementation in Malaysian Corporation.There are many accepted methods for the corporation to assess the vulnerability of infrastructure. Itmay involve assessment of risk or audit. The assessment might take different factors into consideration for providing the feedback on the weaknesses and strengths of the system[11].

A. Technical Dimension

The board and senior management of an organization play a significant role within the technical dimension for evaluating and monitoring the achievement of IS/IT security controls. There are many models of IS/IT security controls that have been observed by the corporations; mainly including mandatory and discretionary access controls, encryption, audit log, disaster recovery, back-up, authentication, validation check, and verification. The outcomes of security report monitoring for IS/IT are a part of internal control application. The managerial entities that are responsible for the internal management (for example: CIO, IT managers and risk management) would promptly inquire and react to the efficacy of existing structures and may also help with the development. It even suggests that the board should revise the acceptable degree of risk to ensure that the aim of the procedure is being attained in an efficient and effectual manner [11].

B. Informal Monitoring Dimensions

The IS/IT security governance of an informal monitoring dimension might be observed and supervised in many ways. First, it can be done through the security behavior; and secondly, through the security incidents and failure. The first manner of monitoring and management can control the employees' security behavior through feedback and communication during the meetings and security reports. It can also bescrutinized by observing the security failure or incidents arising within the corporation. For example, if the incidents are resulting due to the social engineering attacks or violations, the management might engage the employees in awareness programs. The cases of incidents that are instigated due to the management issues, such as poor performance might address the risk by conducting more educational and training programs to improve the skills and knowledge of employees. Management might also change the duties of the related individuals or dismiss or move them to tighten up the procedures and practices of the employment.

C. IS/IT Security Management Strategy

The next step after the identification of IS/IT security is to formulate the IS/IT security management policy for the corporation with respect to the aims of IS/IT security vision.The objective of the research has been concerned with the security of IS/IT resources and the business data of the organization [12, 13]. The formulation of IS/IT security management policies considers the normal criteria that has been utilized in the strategic analysis for the tactical information systems. The nature of environment, objective, resources, and values have been included in the criteria. The objectives and values refer to the culture of organization as analyzing the culture of an organization might help to manage and identify whether the strategies are acceptable or feasible among the employees.

D. IS/IT Security Policy

This document has been intended to indicate the involvement and commitment of the senior management of IS/IT security. Thus, the document policy has been recognized as theplatform for communicating the strategies of boards and vision among the lower levels and senior managements. The policy has also been known to offer a framework for the organizational structures that are relevant, such as business IS/IT system, email system, data-base system and other kind of business information. The intended strategies and IS/IT securityhave contributed in deriving the information [16].The policies are described in Figure 1.

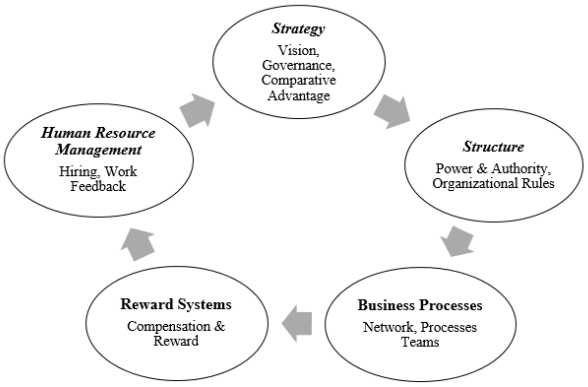

Figure 1: Graphical Representation of strategies of board management

E. Technical Component

There have been two layers of the domainsin the line of technology. The first layer deals with the constituents of foundation and includes the business data and infrastructure of IT. The second layer includes the business information system that derives the values of business from the components of this foundation.The integrity, availability, and confidentiality of the business information might be preserved by using one or more than one security combination or counter measure. The management can employ the measures concerning the security-counter as many times as needed. Eventually, it has been aligned with the objectives of the business. For instance, the managers of IT, who discharges the obligations in protecting the access to particular IT/IS system might use a contrast of the deterrent. Thus, it is required to guard the sensitive business information from being accessed by the irresponsible and unauthorized people in real time situation [16].

II. RESEARCH QUESTIONS

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

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

III. METHODOLOGY

The qualitative research design has been opted in the study. The nature of the IT/IS security governance is sensitive. Due to the sensitivity, the qualitative method offers some different ways to explore and counter the failure including low participation as it contains the authentic data retrieved from different sources.The objective of qualitativemethod is to collect data via interviews to attain a broader understanding of issues under investigation. While, the interview has been planned to acquire qualitative data relating to the perception of boards and senior management concerning IT/IS security processes. A mail survey has been designed to generate the datarelated to the security awareness and attitudes towards IS/IT security governance.The main aim of the qualitative method was to collect the qualitative data and to evaluate the importance of internal control and standard operating procedures in Malaysian Corporations. The semi-structured interview was the second method employed in this study for obtaining rich data from publicly listed companies of Malaysia.

IV. RESULTS AND DISCUSSION

The economic and national security of Malaysia depends on the reliable functioning of infrastructure. The framework of cyber security provides approach to manage and control the risk associated with the cyber security that can be repeatable and display flexibility, performance, and cost effectiveness. The information, processes, and systems are ought to be directly involved in the facilitation of critical services of infrastructure. The model has been developed in collaboration with the industry that offers some guidance to the corporation on managing and controlling the risk of cyber security in Malaysia.

The framework concentrates on utilizing the business drivers to guide the activities regarding cyber securities and consider the risk as a part of the risk management of organization. The framework comprises of three parts: the framework profile, framework core, and the framework implementation level. The core of the framework is the outcomes, activities, and the informative references that are usual across the sectors of critical infrastructure, offering the detailed guidance for organizational profiles and development of individual. The framework assists the corporation in aligning the activities related to the security issues with its risk resources and tolerance. A mechanism has been provided by the framework to the corporation for understanding and viewing the features of the approach in managing the risk associated with the procedures of cyber security [16].The institution or corporation must implement a policy for security and an associated security program that must be monitored and documented. There should be a formal process for the risk management to determine the adequate security levels for the resources of IT [17].

The corporation must implement a procedure to control the risks, linked with the use of information and operation systems that supports the business mission and other functions. The corporationmust also identify the decisions that are well-informed,but based on the risks for the purpose of balancing the advantages and benefits obtained from the operations. The management of security risk, like risk management, is not a precise science. It is known to bring about the best collective judgments from the individuals, together within a corporation, responsible for oversight planning and strategy management.

The corporation must include the security as a main part of the system development cycle. They must demonstrate that security has been considered during the development and enhancement of the critical applications. The change management and document development for mission critical systems must be arranged. The assessments must be conducted to verify the security controls to identify the weaknesses [18, 19].

The boards and senior management of the companies participating in the conduct have IT/IS security policiesimplementedas an organizational aspect. They tend to identify these applications as the formal dimension. The theme of IS/IT security and internal controls has prescribed the importance of the internal controls in IS/IT security. It has also provided the assessment for the role of the senior management and board in this area. It has been claimed by majority of the respondents that they had applied the internal controls within the security of IS/IT and have consideredthe important role of the internal controls within its execution in the security risk of IS/IT. Almost two-third of the participants believed that the board possesses the responsibility in the particular field. Senior management is accountable for the implementation of IS/IT security [20].

All the respondents had claimed the importance of informal components for IS/IT security where they felt that the issue of security was not only an organizational or technological issue, but also a social complication. The values of employees that significantly include trust, integrity and ethics must be considered as the primary factors for the implementation of IS/IT security [20].In order to evaluate the level of IS/IT security within the corporation, the respondents were asked to indicate their verdict on the importance of IS/IT security in their corporation. 21 of them agreed in the survey and supported the IS/IT system (Table 1).

The analysis regarding the board and senior management within the corporation significantly reflects the level of agreement towards the importance of IS/IT security. Further analysis included the matters that how senior managers and boards are responsible for the security risks of IS/IT and how it is important within the corporate risk management plan. The analysis displayed that 61.9% of the participants have agreed that IS/IT security is the matter of responsibility that belongs to the Board of Directors. While, 90.4% stated that Senior Managers have a significant responsibility for IS/IT security risks (Table 2).

Most of the respondents have countered that IS/IT security risk is the part of Corporate Risk Management Plan (90.5%) within the corporations. The majority (95.2%) agreed that IS/IT security risk is part of business risks (Table 3).

Table 1
Importance of IS/IT security

		Frequency	Percent
Importance of IS/IT security	Agree	21	100.0
	Neutral	0	0
	Disagree	0	0
	Total	21	100

Table 2
IS/IT Security Risks by Senior Management

		Frequency	Percent
IS/IT Security Risks by Senior Management	Agree	13	61.9
	Neutral	6	28.6
	Disagree	2	9.5
	Total	21	100.00
		Frequency	Percent
IS/IT Security Risks by Senior Management	Agree	19	90.4
	Neutral	1	4.8
	Disagree	1	4.8
	Total	21	100.0

Table 3
IS/IT Security Risk a Business Risk and IS/IT Security Risk, part of Corporate Risk Management Plan

Survey		Frequency	Percent
IS/IT Security Risk a Business Risk	Agree	20	95.2
	Neutral	1	4.8
	Disagree		
	Total		100
Survey		Frequency	Percent
IS/IT Security Risk, part of Corporate Risk Management Plan	Agree	19	90.5
	Neutral	2	9.5
	Disagree		
	Total	21	100.0

Table 4
IT/IS security policy

Survey Question Topics		Categories	Frequency	Percent (%)
IT/IS security policy		Yes	18	85.7%
		No	3	14.3%
Security areas covered in IT/IS security policy	User access management	Yes	18	100%
		No	0	0%
	Prevention of viruses and worms	Yes	18	100%
		No	0	0%
	Disclosure of information	Yes	18	100%
		No	0	0%
	Violation and breaches of security	Yes	18	100%
		No	0	0%
	Software development and maintenance	Yes	18	100%
		No	0	0%
Security requirements stated in IT/IS security policy	Objectives of the IT/IS security policy	Yes	17	100%
		No	0	0%
	IT/IS security principles	Yes	16	94.1%
		No	1	5.9%
	Roles & responsibilities	Yes	18	100%
		No	0	0%
	Violations and disciplinary action	Yes	16	94.1%
		No	1	5.9%
	Monitoring & review	Yes	18	100%
		No	0	0%

When respondents were asked whether their corporations had an IT/IS security policy, 85.7% replied with a positive response. As for the ones who delivered a negative response, 10.6% belonged to the Manufacturing Industry; while 5.3% were from Agriculture, Forestry and Fishing. Respondents with a positive answer were further inquired about two major factors, including the security area covered in the IT/IS security policy and the security requirement stated in the IT/ISsecurity policy.The results revealedthat all respondents have the security areas that do not cover the "user access management", "prevention of viruses and worms", "disclosure of information", "violation and breaches of security" and "software development and maintenance". In the case of security requirements stated in the IT/IS security policy, all respondents pointed out that their corporation's policy included "objective of the IT/IS security policy", "roles and responsibilities" and "monitoring and review". The majority (94.1%) of respondents indicated that their IT/IS security policy have covered necessities on the"IT/IS security principles" and "violations and disciplinary action" (Table 4).

It has been comprehended from the literature as well as the study that the Board and senior management hold strong responsibility for providing directions. The directions are mainly diverted to the policies in the formal component relating to IS/IT security in order to make it certain that all the IS/IT security risks remain under control.

There are many areas that have reflected the involvement of board and senior management in the formal component in the IS/IT security policy. Therefore, the alignment between the business goals and IS/IT security policy have been the main focus throughout the study.

A. Research Question 1

The findings of research question 1 was explored in order to find out the evidence regarding the development of IS/IT security aspects in accordance with technical, informal and formal constituents. The discussion of research question 1 has been subdivided into three dimensions. The first dimension is about the technical dimension that reflects the controls of development and implementation of the security as well as core duties of senior management and board members. It has been accounted that the success and failure of planning, development, implementation and maintenance of security controls are the responsibilities of boards and senior management. Techniques and controls, system development and the internet or network security have been identified from technical dimensions.

It has been determined from a technical dimension that corporations are a significant component that improves the security controls throughout the network system. Security controls on specific dimensions have been enforced from different techniques and controls that accomplished the demands of the security policies.System development has determined the corporations that signify security elements into the IT/IS development. The inclusion of security controls has been identified through internet or network that utilized the use of internet and network throughout corporations. Mobile networks and wireless have emerged as effective technologies that provide private networks of corporations with threats and vulnerabilities [20].

Human aspects have been improved from the informal dimension that regards to the level of acknowledgment and abilities as well as the level of human integrity within security implementation of IT/IS. Integrity has been approached by staff as a level of honesty. It has been indicated that human characteristics are integrated into the factors with regardto the awareness, education and human integrity by senior

management and board members. This technical implementation has been integrated within IT/IS security policies and tactics from minimizing the human errors, lack of awareness and lack of integrity. It has been emphasized that the role of human integrity and accountability throughout IT/IS security implementation is identified from corporations. These features of informal dimension have been concerned with complete features and values of senior management and board members that lack the intended actions, which may include destruction of the business information and stealing information [21].

A security culture has been identified through the dimension of the informal theme in which a security and network culture is established by staff throughout the organization. It has been clarified that IT/IS security policies and tactics are reflected through security culture. For instance, employees within the premises of organization cannot share their usernames, even their passwords, with other members in the IT/IS system in a corporation. Therefore, it has been examined that dedication of staff and senior management in this regard brings success to the policies, tactics and cultural practices.

The results have depicted that security awareness is emphasized by senior management and board members in this regard. The reflection on security awareness has accounted the security policies and tactics from the view of all employees of the organization. The lack of awareness can potentially play a part in breaking the policy, procedures, and outlines that have already been implemented.

The third dimension that reflects the findings of research question 1 in the context of IT/IS security is a formal dimension that includes the development of structures of IT/IS security. The security policies of IT/IS security management is an important factor that critically analyze the objective and procedures of IT/IS security. Furthermore, the relationship between IT/IS security needs and business requirements has been identified from strategic vision and security importance that accomplishesthe strategic vision of IT/IS security as well as reduces operational business risk. Security internal controls reflect the gears that are applied in IT/IS security areas. It is a mechanism utilized by organizations that measure the success of particular corporation's policies implementation and other organizational benefits regarding the risk and security [21-24]. Majority of the results in the survey supported the themes that were established in the framework of the security governance of IT/IS, where primarily the survey supported the elements of the components of both formal and informal nature, as shown in Figure 2. Although, there was no data found regarding the features of the technical components.

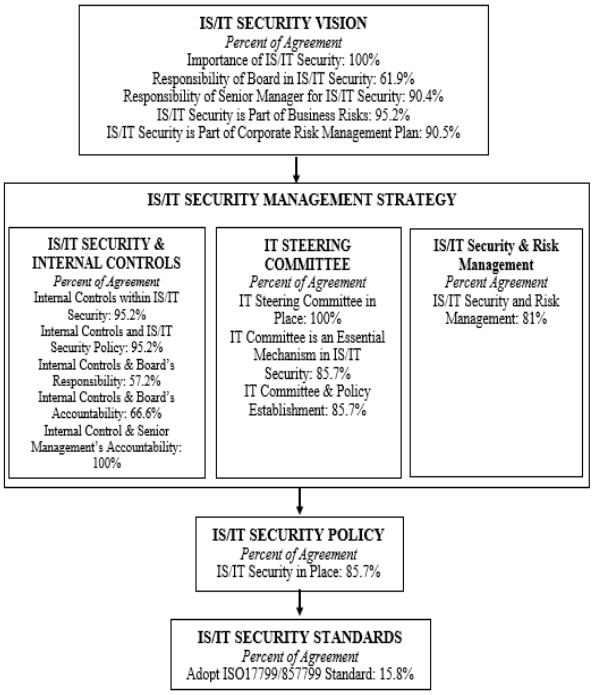

Figure 2: IT/IS Management Strategy

B. Research Question 2

In order to monitor and direct the policies and strategies, board members and senior management are accountable and responsible to make sure that IS/IT risks are addressed in the policies, standards, and procedures of IS/IT security. Responsibility for security is considered as a phase of responsiveness, which may include acceptance of the acts, omissions, and judgments. Today, data and other corporation information can be accessed by employees at cafes, airports, and other wireless hotspots. Moreover, senior management and board members must ensure that communication of employees is managed. The communication medium among staff holding related roles must be reassessed from time to time as IS/IT security tends to be a continuous procedure. The board and senior management must also ascertain that the development of IS/IT value is protected at internal levels in accomplishing the alignment between IT/IS and organization goals.The single case analysis supported the monitoring and directing actions in the manual content analysis over components interactions. The formal and informal technical interaction, with one and other, in regards with the directing and monitoring actions in the light of interactions have been shown in the following figure (Figure 3).

The inter-relationship has been explored among the three recognized elements of informal and technical components. The findings have supported the IS/IT governance model for the two relationships. It has been observed that there was no data available regarding the technical and informal support as shown in Figure 4.

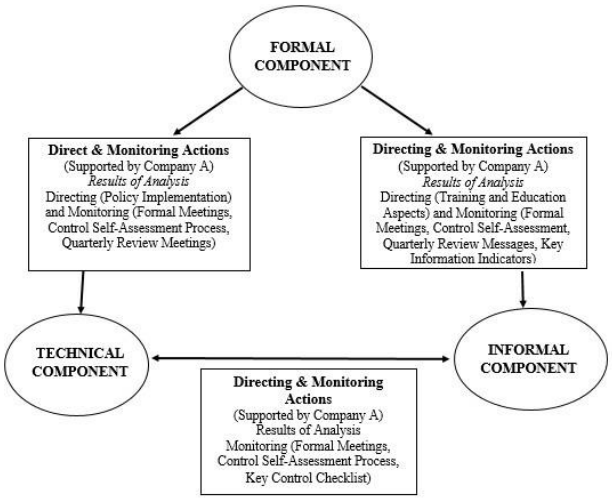

Figure 3: The directing and monitoring actions over the Formal component and its interaction and supporting data: by single case

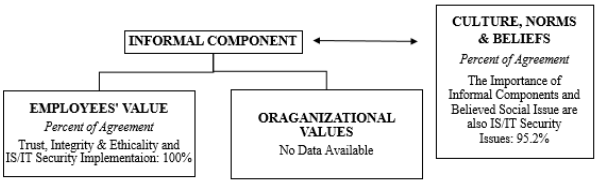

Figure 4: The results of Informal themes and supporting data

V. CONCLUSION

Apart from the enforcement of the policies and security procedures within the organization, reinforcement and improvement are also recognized as the major factors that can be provided by training in IS/IT security governance structure. According to a typical approach, the incidents of security are mostly identified as the outcomes of human actions rather than the technical problems. Future studies might also develop a model to enhance the alignment and gaps between the implementation of technical and training methods. The training must be aligned and specific with the goals and needs of the policies and procedures. The correct training might improve the component interaction between the technical and formal security incidents and problems.A model for future must be designed to explore the role of supervision among the holders of responsibilities to overcome the issues between the application of technical and training procedure. The directing and monitoring actions must be applied in a parallel way with the supervision part between the holder and giver of responsibility, if provided with a particular job concerning security.

ACKNOWLEDGEMENT

The author is 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 and is funded by the Ministry of Higher Education Malaysia, Universiti Malaysia Sarawak (UNIMAS) and University of Tasmania, Australia.

REFERENCES

[1]. V. J. Marsick, K. Watkins,"Informal and Incidental Learning in the Workplace, (Routledge Revivals)," Routledge,2015 Jun 11.
[2]. D. M. Dozier, L. A. Grunig, J. E. Grunig,"Manager's guide to excellence in public relations and communication management,"Routledge, 2013 Oct 18.
[3]. R. Pereira, M. C. Baranauskas, S. R. da Silva,"Social Software and Educational Technology: Informal, Formal and Technical Values,"*Educational Technology & Society*, 2013 Jan 1, 16(1), pp. 4-14.
[4]. W. Pieters, T. Dimkov, D. Pavlovic,"Security policy alignment: A formal approach", IEEE Systems Journal, 2013 Jun, 7(2), pp. 275-287. Doi.org/10.1109/jsyst.2012.2221933
[5]. N. Musa, "Role of the boards and senior management within formal, technical and informal components: IS/IT security governance in the Malaysian publicly listed companies(Doctoral dissertation," University of Tasmania). Doi.org/10.1109/icitst.2013.6750242
[6]. G. Soda, A. Zaheer,"A network perspective on organizational architecture: performance effects of the interplay of formal and informal organization",*Strategic Manage J*, 2012 Jun 1, 33(6), pp. 751-771. Doi.org/10.1002/smj.1966
[7]. M. Schumacher, E. Fernandez-Buglioni, D. Hybertson, F. Buschmann, P. Sommerlad,"Security Patterns: Integrating security and systems engineering," John Wiley & Sons, 2013 Jul 12.
[8]. R. Von Solms, J. Van Niekerk,"From information security to cyber security",Comput Secur, 2013 Oct 31, 38, pp. 97-102. Doi.org/10.1016/j.cose.2013.04.004
[9]. T.R. Peltier,"Information Security Policies, Procedures, and Standards: guidelines for effective information security management," CRC Press, 2016 Apr 19. Doi.org/10.1201/9780849390326
[10]. W. H. Baker, L. Wallace, "Is information security under control?: Investigating quality in information security management,"*IEEE Security & Privacy*, 2007 Jan, 5(1), pp. 36-44. Doi.org/10.1109/msp.2007.11
[11]. A. Gemino, B. H. Reich, C. Sauer,"Plans versus people: Comparing knowledge management approaches in IT-enabled business projects",*International Journal of Project Management*, 2015 Feb 28, 33(2), pp. 299-310. Doi.org/10.1016/j.ijproman.2014.04.012
[12]. Kucharska, Wioleta, and Rafał Kowalczyk. "Trust, Collaborative Culture and Tacit Knowledge Sharing in Project Management–a Relationship Model." (2016).
[13]. A. J. Wood, B. F. Wollenberg,"Power generation, operation, and control," John Wiley & Sons, 2012 Nov 7.
[14]. A Amran, S. K. Ooi, R. T. Mydin, S. S. Devi. "The Impact of Business Strategies on Online Sustainability Disclosures",*Business Strategy and the Environment*, 2015 Sep 1, 24(6), pp. 551-564. Doi.org/10.1002/bse.1837
[15]. Lai, Alessandro, Gaia Melloni, and Riccardo Stacchezzini. "Corporate sustainable development: is 'integrated reporting'a legitimation strategy?."*Business Strategy and the Environment* 25, no. 3 (2016): 165-177. DOI: 10.1002/bse.1863
[16]. S. Mishra, G. Dhillon,"Information Systems Security Governance Research: A Behavioral Perspective", Annual NYS Cyber Security Conference, 2007.
[17]. S. P. Williams, C. A. Hardy, J. A. Holgate,"Information security governance practices in critical infrastructure organizations: A socio-technical and institutional logic perspective,"*Electronic Markets*, 2013 Dec 1, 23(4), pp. 341-354. doi.org/10.1007/s12525-013-0137-3
[18]. S. Mishra,"Organizational objectives for information security governance: a value focused assessment",*Information & Computer Security*, 2015 Jun 8, 23(2), pp. 122-144. Doi.org/10.1108/ics-02-2014-0016
[19]. Dhillon, Gurpreet, Lemuria Carter, and Javad Abed. "Defining Objectives For Securing The Internet Of Things: A Value-Focused Thinking Approach." (2016).
[20]. J. A. Sherer, T. M. Hoffman, E. E. Ortiz, "Merger and Acquisition Due Diligence: A Proposed Framework to Incorporate Data Privacy, Information Security, E-Discovery, and Information Governance into Due Diligence Practices", Rich. JL & Tech, 2014,21, pp. 1.
[21]. M. Mueller, A. Schmidt, B. Kuerbis, "Internet security and networked governance in international relations,"*International Studies Review*, 2013 Mar, 15(1), pp. 186-104. Doi.org/10.1111/misr.12024
[22]. Debreceny RS. "Research on IT governance, risk, and value: Challenges and opportunities",*Journal of Information Systems*, 27(1), 2013 Jun, 129-135. Doi.org/10.2308/isys-10339
[23]. Flores WR, Antonsen E, Ekstedt M. "Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture", Comput Secur, 43, 2014 Jun 30, 90-110. Doi.org/10.1016/j.cose.2014.03.004

[24]. Rafiee, Abozar Solat, Akbar Alem Tabriz, and Mohammadreza Babaei. "Organizational Characteristics Role in the Implementation of Information Security in Knowledge Management with a Focus on Employee Safety Behavior." Modern Applied Science 10, no. 2 (2016): 123. DOI: http://dx.doi.org/10.5539/mas.v10n2p123

[25]. Tejay GP, Barton KA. "Information System Security Commitment: A Pilot Study of External Influences on Senior Management", InSystem Sciences (HICSS), 46th Hawaii International Conference on 2013 Jan 7 (pp. 3028-3037). IEEE. Doi.org/10.1109/hicss.2013.273.