7th INTERNATIONAL CONFERENCE ON FINANCIAL CRIMINOLOGY 2015  
13-14 April 2015, Wadham College, Oxford, United Kingdom

Information Security: Risk, Governance and Implementation Setback

M.R, Fazlida\textsuperscript{a}\textsuperscript{*}, Jamaliah Said\textsuperscript{b}

\textsuperscript{a}Faculty of Accountancy, Universiti Teknologi MARA, 40450 Shah Alam, Malaysia  
\textsuperscript{b}Accounting Research Institute, Universiti Teknologi MARA, 40450 Shah Alam, Malaysia

Abstract

The growing emergence of information security threat call for information security to be integrate in the organization’s corporate governance and been treat as high important as other critical corporate governance area by Boards and executive management. This paper provides an overview of information security risk, governance and implementation setback. Review shows that Information Security can complement IT Governance (ITG), in term of assurance on the confidentiality, integrity, and availability of information. Well-known ITG Framework such as ISO 27001 and COBIT could be used by organizations to help ease Information Security Governance (ISG) implementation. Amongst hindrance to ISG implementation is lack of awareness on the important of information security by BOD and stakeholders, unclear policies and staff rejection.

© 2015 The Authors. Published by Elsevier B.V. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).  
Peer-review under responsibility of ACCOUNTING RESEARCH INSTITUTE, UNIVERSITI TEKNOLOGI MARA

Keywords: Information security; Governance;

1. Introduction

The intense shift in financial records from manual to electronic media has significant implications of Information Technology (IT) for the purposes of financial reporting. High dependency on IT could expose company data to information security risk. Sound information security governance could signal Boards overall attitudes towards information security risk. This paper will provide an overview of Information Security Risk, Information Security Governance and Implementation Setback.

* Corresponding author. Tel.: +6012-6520452; fax: +603-55444992.  
\textit{E-mail address:} fazlidarazali@yahoo.com
2. Information Security Risk

The growing vulnerability of an IT risk specifically Information Security (InfoSec) risk has become the major attention in most global information security survey conducted by Public Accountant (Ernst and Young, 2013, 2014; PricewaterhouseCoopers, 2014). Among InfoSec risk area that the respondent place top priorities is business continuity and disaster recovery, cyber risks and cyber threats, data leakage and data loss prevention, information security transformation, and compliance monitoring (Ernst & Young, 2014). The purpose of Information Security is to protect and preserve the confidentiality, integrity, and availability of information. It may also involve protecting and preserving the authenticity and reliability of information and ensuring that entities can be held accountable (ISO 27000). ISO 31000 define risk as “effect of uncertainty on objectives”. Therefore Information Security Risk (ISR) is define by ISO 31000 as “a combination of two factors: probability and consequences. It asks two basic questions: what is the probability that a particular information security event will occur in the future? And what consequences would this event produce or what impact would it have if it actually occurred? Information security risks often emerge because potential security threats are identified that could exploit vulnerabilities in an information asset or group of assets and therefore cause harm to an organization”.

“EY’s Global Information Security Survey 2014 - Get ahead of cybercrime” highlighted that respondent opined higher vulnerability and InfoSec threat mainly caused by outdated information security controls or architecture. It is follow by careless or unaware employees, cloud computing use, mobile computing use, and unauthorized access. EY’s Global Information Security Survey 2013- Under Cyber Attack” statistically reported that although there is increase in investment of information security control (46%) and alignment of bank’s business strategy with their correspond information security strategy (46%) by respondent’s entities, yet 31% of the respondents admitted that number of information security incidents within their organization has increased over the last 12 month at least by 5%.

Financial Institutions especially banking institutions place greater emphasis on cyber risk and cyber threats due to its nature of information intensive industries (N. Mohamed & Jasber Kaur, 2012). Based on PWC’s Global Economic Crime 2014, cybercrime is become more common (39% out of 5 actual economic crime reported in 2014) as compare to money laundering, fraud, bribery and corruption in banking industry. Recently, on Sept 28, 2014 Malaysian awakened following reports of ATMs in 14 bank branches in Selangor, Johor and Malacca hacked by a group of Latin American countries, who stole more than RM 3 million in just two days (The Star, Sept 30, 2014). Hackers is one of big InfoSec threat face by banking institution around the world. Banking institution is vulnerable to countless InfoSec threat due to its high dependency on IT to perform it core business operation (N. Mohamed & Jasber Kaur, 2012) and support its financial reporting process.

In view of the growing vulnerability of an IT risk particularly Information Security Risk (ISR), there is a considerable amount of literature stressed the importance of incorporating Information Security as part of organizations Corporate Governance (Moulton & Coles, 2003: Posthumus & Solms, 2004: Kooper, Maes, & Lindgreen, 2011; Bahl & Wali, 2014). The emergence exposure to the information security risk create a needs for Information security to be treat as high priority as other critical corporate governance area by Board of Directors (BOD) (Posthumus & Solms, 2004). In the next section we will discussed in depth on Information Security Governance (ISG).

3. Information Security Governance

3.1. Information Technology Governance and Information Security Governance :The Gaps

The research to date has tended to focus on IT Governance (ITG) rather than Information Security Governance (ISG) per se. Souza Bermejo et al., (2014) defines ITG as “structures, processes, and relational mechanisms for guidance and control or literature uniformly identifies it as an organizational skills of great importance for alignment and organizational value achievement through information technology”. As cited in previous research, ITG being a part of corporate governance to help organizations manage risk and protects themselves from IT related risk. Recent developments in Information Security Risk have heightened the needs for Information Security to be a part of organizations Corporate Governance (Moulton & Coles, 2003: Posthumus & Solms, 2004: Kooper, Maes,
Lindgreen, 2011; Bahl & Wali, 2014) to achieve competitive edge, provide client satisfaction and create trust. Kooper et al., (2011) argued that although ITG is now broadly accepted and recognized by many authors as compulsory mechanisms to manage IT risk, it has some limitations. Major limitation emphasized by author is that ITG focus on managing the resources to transform information and its related risk, but then overlooked the transformation process (created, sought, processed and exchanged) itself. Furthermore, author’s stressed that in practice imperfect implementations of ITG (i.e. delayed or aborted information security project, service level remain unmonitored etc.) and futile policies is the main cause of ITG failure.

Mohamed & Kaur a/p Gian Singh, (2012), analyzed the perspectives of IT Governance from previous literature and found four perspectives of ITG namely Governance Mechanism; Decision- Making; Strategic Alignment of business and IT; and Strategic IT Planning and Control. They also found that supportive action has been taken from various association and regulatory body to inculcate ITG via introduction of IT Governance frameworks which cater specific objectives including IT control structure, protection of IT investment, security and control of IT, protection of information from losses, assuring information integrity, quality IT services, and quality software. Within the ITG, information security governance becomes very focused activity, with specific value drivers including integrity of information, continuity of services and protection of information assets (Williams, 2001). The limitation argued by Kooper et al., (2011), possibly can be address by incorporating the elements of Information Security Governance in IT Governance so that the loopholes can be expands. Both ISG and ITG can be a complement to effective Corporate Governance (Moulton & Coles, 2003: Posthumus & Solms, 2004: Kooper, Maes, & Lindgreen, 2011).

3.2. Information Security Governance

To better understand on information security governance, the definition of ISG is discussed. In view of ISG is the subset of Corporate Governance, Moulton & Coles, (2003) extend The IT Governance Institute (2001) definition of Corporate Governance by incorporating element related to information security particularly; security responsibilities and practices; strategies and objectives for securities; risk assessment and management; resources management for security; compliance with legislation, regulations, security policies and rules; and Investor relations and communications activity in relations to security. Moulton & Coles, (2003) defined Information Security Governance as “the establishment and maintenance of the control environment to manage the risks relating to the confidentiality, integrity and availability of information and its supporting processes and systems which is not a part of audit (ensuring that governance processes been properly established and are functioning), security operation (day-to-day performance of security administrative activities) and security development (engineering of new IT or processes to meet security objectives”).

“Information Security Governance’ terms portray how organization’s executive deals with security (Posthumus & Solms, 2004). The authors urged that Information security to be treat as high priority as other critical corporate governance area by Board of Directors (BOD). As sighted in Williams, (2001) Ronald Saull, (Chief Information Officer and Senior VP of Great-West Life Assurance Company) stated that “Director have responsibility to protect shareholder value. This responsibility applies just as stringently to valued information assets as it does to any other asset. Board must recognize that securing that information is not just an investment; it is essential for survival in all cases and for many it can even create competitive advantage”.

Information security is often view as technical problems (Posthumus & Solms, 2004;Moulton & Coles, 2003; Williams, 2001), with low BOD’s attention and the responsibilities continuously rest on technical manager (Williams, 2001). Ultimately, BODs held responsible and liable (Humphreys, 2008) for any legal duties should there any breach of the governance particularly information security governance. BODs and executive management should ensure that due diligence is undertaken in identifying risk (both existing and emergence), implementing effective system of controls and regular monitoring to ensure control remain relevant and keep pace with emerge information security threat (Ernst and Young, 2013, 2014: Humphreys, 2008; Posthumus & Solms, 2004). It is essential that BODs and executive management get hold of organization’s information security effort because it entails non-stop improvement over time (Williams, 2001). The implementation of information security governance as directed by BODs requires involvement and commitment of multi-department within the organizations with adherence to corporate information security policy and reference to information security codes of conduct (Posthumus & Solms, 2004). The codes of conduct, framework or guidelines exist in order to guide the practitioners
in implementing the best governance. The next section we will discuss on IT Governance framework generally and particularly in information security.

3.3. Information Security Governance Framework

Mohamed & Kaur a/p Gian Singh (2012) stated that supportive action has been taken from various association and regulatory body to inculcate ITG via introduction of IT Governance frameworks which cater specific objectives including IT control structure, protection of IT investment, security and control of IT, protection of information from losses, assuring information integrity, quality IT services, and quality software. Thus signifying that Information Security (IS) fall under the domain of ITG. Among well-known ITG Framework includes COSO, COBIT, ISO 27001 and Statement of Auditing Standard No.70 (Allen, 2005; Campbell, 2003; Ula, Ismail, & Sidek, 2011; Williams, 2001). Tuttle & Vandervelde (2007) highlighted that although COSO 2002 framework has been used widely as a guide to assess internal control, its fall short as general nature of COSO does not address the complexity and special risks inherent in information technology. Even the revise version of COSO 2013, has been criticized as not specifically address information technology (Janvrin, Payne, Byrnes, Schneider, & Curtis, 2012). Control Objectives for Information Related Technology (COBIT) is a widely recognized control framework that is emerging as the supplemental framework of choice to the Treadway Commission's Committee of Sponsoring Organizations (COSO) evaluation framework (Huang, Hung, Yen, Chang, & Jiang, 2011). However, there is still loopholes that as COBIT framework lacks of some important variable for assessing risk on IT process (Tuttle & Vandervelde, 2007) specifically information security risk.

Mohamed & Kaur a/p Gian Singh (2012) listed ISO 27001 as the main information security framework to cater information security objective under ITG category framework. ISO 27001 (formerly known as BS 7799) provides a formal set of specifications for organizations to manage information security risk and seek certification for their Information Security Management System (ISMS) (N. Mohamed & Jasber Kaur, 2012). Posthumus & Solms (2004) stated that “ISO 27001 could be able to suggest appropriate security controls that can successfully preserve the confidentiality, integrity and availability of business information and thus could serve to integrate information security into the daily activities and function of an organization”. This is contrary to Dzazali & Zolait (2012) who argue that COBIT could assist senior management in having excellent information security management capability with an alignment to business overall strategic goals. This is further supported by (Tokhid, Abdul Rashid, & Abdul Roni, 2012) who cited that COBIT is useful in helping organization in term of compliance with regulation and assurance of the information security. Recently, Chang et al., (2014) combined the Auditing Standard (ISA and SOX) and Information Security organization Bylaws (COSO, COBIT, ISO27001/BS7799) in order to assist auditors with the best framework in which will complement any deficiencies found in the individual framework. Therefore choosing the right framework is vital to assure that practitioners making reference to the best framework for effective information security governance.

4. Information Security Governance: Implementation Setbacks

In this section we will discuss about the problem cited as hindrance to implementation of information security governance. Information security is often view as technical problems (Posthumus & Solms, 2004; Moulton & Coles, 2003; Williams, 2001; Dzazali & Zolait, 2012) with low BOD’s attention and the responsibilities continuously rest on technical manager (Williams, 2001). In addition, organization decided to rely more on technological solution to solve information security issues which result in either over-reliance on technological control or overlooked on other important component of information security, physical control and non-technological control (Dzazali & Zolait, 2012). Having right tone set at the top, will not guarantee a sound information security governance until non-technical issues such as awareness and compliance management is effectively implement through regular compliance and risk reporting to the BOD (Solms, 2006). Awareness is the key challenges in implementation of Information Security Governance. Dzazali & Zolait (2012) cited awareness is social barriers caused by human factor that prevent the successful of ISG such as stakeholder’s reluctant to accept information security as part of corporate objective due lacks of knowledge on the value added benefit it could offer.
Barker (2014) emphasized on the gap between real and perceived security risk. When there is a gap between real and perceived security risk, there is the possibilities that the control policy (risk identification, control, monitoring action, compliance) set at executive management level did not translated in expected manner by lower level staff. This communication breakdown is a hindrance to a good information security governance due to lower level staff perceived low information security risk than the actual risk. The author also stressed that lack of understanding on the real risk exposure, may result in staff rejection (ineffective control procedure, not comfortable, not competent) of the control procedure decide by executive management. The effectiveness of the governance still rest on the user understanding of the threat and the importance of maintaining information integrity by them (Mohamed, 2013). Tokhid et al., (2012) found that half of his respondent from Public Listed companies with good corporate governance practice unfavourable to control procedure statement of monitoring and evaluate under COBIT, which substantiate on the issue of number of IT project were failed or did not produce expected result, delayed or aborted information security project, service level remain unmonitored etc. (Kooper et al., 2011). This eventually expose the organization to the existing and emerging information security risk.

Other hindrance to the implementation of good information security governance is lack of stakeholder’s trust and buy-in to invest in information security measure. Cowan (2011) stressed that return on information security investment can be further enhance via improved reputation as a result of good governance. Nazareth & Choi (2015) differentiate the cost and benefit of low and high security investment. At low level of investment, overall security cost decrease with increased investment in information security. However, at some point of time the cost will exceed the benefit through reduced damages and recovery effort. On other hand, at high level security investment, additional security investment does not change the number of successful attack, thereby incurring additional cost and no material benefits. This is called ‘residual risk” due to inherent security weakness no matter what preventive measure undertaken (Humphreys, 2008). In order to have a good information security governance, all negative perception towards information security need to be swap beyond the traditional boundaries through inculcating the value added advantage of information security (Williams, 2001), which is worth to invest on.

5. Conclusions

Sound information security governance could signal the company’s overall attitude towards information security risk especially for information intensive industries such as financial institution particularly bank. The growing emergence of information security threat call for information security to be integrate in the organization’s corporate governance and been treat as high important as other critical corporate governance area by BOD and executive management. Although information security is a part of IT Governance, yet there are room of improvement to ensure that information security is thoroughly covers under ITG so that its complement ITG in term of assurance on the confidentiality, integrity, and availability of information. Several association and regulatory body emanates the code of conduct, framework or guideline to inculcate and inspire practitioners to implement IT Governance particularly Information Security Governance. ISO 27001 is cited to be main framework for information security whereas COBIT is well-known and largely used by organization although has been criticized of having limitation in area of information security. Information security governance implementation maybe achieved if a) BOD and executive management place extra attention on information security matters instead of treating it as technological issues under technical managers responsibilities; b) information security measure is clearly communicated from the top management to lower level staff; c) low level staff involve in formulation of the information security policies to avoid setback or policy implementation rejection and lastly d) all stakeholders aware of the value added offered by implementation of information security governance which result in higher investment in information security control.
Acknowledgements

We would like to express our sincere gratitude to the Accounting Research Institute (ARI) UiTM, Faculty of Accountancy, Universiti Teknologi MARA, Shah Alam, in collaboration with Ministry of Education Malaysia (MOE) in providing a grant for financial assistance to carry out this research project. The research was supported under the Fundamental Research Grant Scheme (FRGS).

References