Available online at www.sciencedirect.com

ScienceDirect

Procedia Economics and Finance 28 (2015) 243 – 248

Procedia Economics and Finance

www.elsevier.com/locate/procedia

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[a]*, Jamaliah Said[b]

[a]*Faculty of Accountancy, Universiti Teknologi MARA, 40450 Shah Alam, Malaysia*
[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.

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.
E-mail address: fazlidarazali@yahoo.com

Peer-review under responsibility of ACCOUNTING RESEARCH INSTITUTE, UNIVERSITI TEKNOLOGI MARA
doi:10.1016/S2212-5671(15)01106-5

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 RM3 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, &