Chapter 62
Evaluating the Effectiveness of Information Security Governance Practices in Developing Nations: A Case of Ghana

Winfred Yaokumah
Pentecost University College, Ghana

ABSTRACT

The purpose of this empirical study is to evaluate the extent to which information security governance domain practices: strategic alignment, value delivery, resource management, risk management, and performance measurement relate to information security governance effectiveness. Random sampling technique was employed and data were collected via web survey from Ghanaian organizations. Employing three multiple regression models, the results showed there were statistically significant positive linear relationship between information security governance domain practices and information security governance effectiveness. Overall, the model produced R^2 =.505, indicating that 50.5% of the variance in information security governance effectiveness was explained by information security governance domain practices. The results highlighted resource management, performance measurement and risk management practices as the predictors of organizational information security governance effectiveness while strategic alignment contributed only marginally to the models. Therefore, to attain higher information security governance effectiveness, organizations should focus on strategic alignment between the business and information security attributes.

INTRODUCTION

Securing information is an old practice where organizations, governments, military leaders, and individuals have been trying to protect sensitive information from unauthorized access, accidental loss, destruction, disclosure, modification, or misuse (Tassabehji, 2005). With the invention of computers and the Internet, information becomes a more valuable asset. As a result, information

DOI: 10.4018/978-1-4666-8111-8.ch062

is increasingly under threat as vulnerabilities in information technology systems that process, store, and transmit information are constantly being exploited for economic, espionage and other gains. Despite the threats, organizations continue to depend heavily on information systems to manage and operate critical systems in order to meet stakeholders' requirements, create value for the shareholders, and gain strategic advantage (Pironti, 2006; von Solms, 2006).

In the past, research on information security paid much attention to technical issues and technical solutions were developed to deal with denial of service attacks to computing systems, malware, intrusion attacks, spoofing, password attacks, eavesdropping, and others. However, in recent years, it has been acknowledged that human factors play a major part in many security failures (Furnell & Thomson, 2009). While technical threats are usually more high profile and given much media and financial attention (Tassabehji, 2005), non-technical human and physical threats are sometimes more effective and damaging to information security (Kraemer, Carayon, & Clem, 2009).

Although there are no agreement on the actual figures and percentages of the extent of information security risks, empirical evidence from practitioner and scholarly literature over the past years (Dzazali & Zolait, 2009; Johnston & Hale, 2009; Ponemon Institute, 2011) revealed similar trends and patterns of security breaches. Ponemon Institute's second annual cost of cyber crime study benchmarked 50 major U.S. companies. The study revealed that cyber crime costs organizations $5.9 million per year, with a range of $1.5 million to $36.5 million each year per company. This figure indicated an increase of 56 percent from the previous year. Similarly, Johnston and Hale (2009) reported that loss from risks such as virus attacks amounted to $43 million and insider attacks cost organizations $7 million. Similarly, the Overseas Security Advisory Council (OSAC, 2011) of the U.S. Department of State warned that travelers to Ghana should desist from using credit cards while in Ghana because of the increasing number of people who had become victims of credit card fraud.

Accordingly, the studies recommended that organizations should commit to information security governance and risk management, employ compliance solutions, and engage effective governance frameworks (Johnston & Hale, 2009; Ponemon Institute, 2011) to ensure that corporate information resources are secured and devoid of any misuse that could negatively impact business operations. As these studies were based on U.S companies, the situation in developing nations may not differ. This is because the business environment in developing countries is predominantly small- and medium-sized enterprises (SME) that operate under tight budget, limited resources, and expertise (Yeniman et al., 2011).to implement information security governance practices.

Information Security Governance Institute, ITGI (2006) predicted that measuring the effectiveness of organizations' information security governance practices will continue into the future. A recent study found that an effective information security governance practices improve information security (Johnston & Hale, 2009). Therefore, a great need exists for information security and its governance in the developing countries (Yeniman et al., 2011) and gauging the effectiveness of information security governance in the developing nations is essential (Dzazali, Sulaiman, & Zalait, 2009). However, despite over a decade of global information security governance (ISG) initiatives, how well information security governance has been practiced within organizations in most developing nations remains largely unknown (Abu-Musa, 2010), making the top organizational leaders oblivious of information security threats and vulnerabilities. The problem is ineffective implementation (Abu-Musa, 2010) and assessment of information security governance in developing countries. Coertze (2012) pointed out that many businesses, particularly SME and