Chapter 7
Information Security Governance Practices and Commitments in Organizations

ABSTRACT

Despite the existence of referential and standards of the security governance, the research literature remains limited regarding the practices of organizations and, on the other hand, the lack of a strategy and practical model to follow in adopting an effective information security governance. This chapter aims to explore the engagement processes and the practices of organizations involved in a strategy of information security governance. The statistical and econometric analysis of data from a survey of 1000 participants (with a participation rate of 83.67%) from large and medium companies belonging to various industries such as retail/wholesale, banking, services, telecom, private and governmental organizations provides a record of current practices in information security governance. The findings allowed the authors to propose a practical framework to evaluate the information security governance in organizations.

DOI: 10.4018/978-1-5225-7826-0.ch007

INTRODUCTION

The threat to technology-based information assets is greater today than in the past (Maleh, Sahid, Ezzati, & Belaissaoui, 2018). The evolution of technology has also reflected in the tools and methods used by those attempting to gain unauthorized access to the data or disrupt business processes (L. Goodhue & Straub, 1991). Attacks are inevitable, whatever the organization ("Information Security Governance," 2006). However, the degree of sophistication and persistence of these attacks depends on the attractiveness of this organization as a target (F. Rockart & D. Crescenzi, 1984), mainly regarding its role and assets. Today, the threats posed by some misguided individuals have been replaced by international organized criminal groups highly specialized or by foreign states that have the skills, personnel, and tools necessary to conduct secret and sophisticated cyber espionage attacks. These attacks are not only targeted at government entities. In recent years, several large companies have infiltrated, and their data have been "consulted" for several years without their knowledge. In fact, improving cybersecurity has emerged as one of the top IT priorities across all business lines. So, while companies (von Solms & van Niekerk, 2013; Bowen, Chew, & Hash, 2007)

Areas such as the aerospace industry and strategic resources can be ideal targets for cyber espionage by nation-states, others managing financial assets or large-scale credit card information are equally attractive to international criminal groups (Posthumus & von Solms, 2004; Humphreys, 2008).

These malicious actors no longer content themselves with thwarting the means of technical protection. Instead, they survey and exploit a variety of weaknesses detected in the targeted environment (Galliers & Leidner, 2014). These shortcomings are not only technological but also result from failures in protection procedures or gaps in vulnerability management practices. The best technology in the world, if misused will not provide an adequate defense against such threats (von Solms & van Niekerk, 2013).

Ensuring the information system IS security in a large organization is a real challenge (Sohrabi Safa, Von Solms, & Furnell, 2016). Only a good governance can reassure the general management, customers and partners, shareholders and ultimately the public at large (Mark Duffield, 2014).

The problem is that the security governance framework is designed to guide organizations in there IS security governance strategy but does not define the practical framework for the engagement in this strategy.