Chapter 7
Building a Maturity Framework for Information Security Governance Through an Empirical Study in Organizations

Yassine Maleh
University Hassan I, Morocco

Mounia Zaydi
University Hassan I, Morocco

Abdelkbir Sahid
National School of Commerce and Management (ENCG), Morocco

Abdellah Ezzati
Faculty of Science and Technology (FST), Morocco

ABSTRACT

There is a dearth of academic research literature on the practices and commitments of information security governance in organizations. 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 via a 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. Based on the results of the survey regarding practices of information security management and governance, a practical maturity framework for the information security governance and management in organizations is presented.

DOI: 10.4018/978-1-7998-7705-9.ch007

Copyright © 2021, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

INTRODUCTION

The threat to technology-based information assets is greater today than in the past. 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 (IT Governance Institute, 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 Today, the threats posed by some misguided individuals have been replaced by international organized criminal groups highly specialized or by foreign states that have the skills, personnel, and tools necessary to conduct secret and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 cyber security 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.

To address these concerns, some practice repositories (ITIL, Cobit, CMMi, RiskIT) and international standards (ISO 27000 suite, ISO 15408) now include paragraphs on security governance. The first reports or articles in academic journals that evoke the governance of information security date back to the early 2000s.

The proposed referential and best practices designed to guide organizations in their IT security governance strategy. However, does not define the practical framework to implement or to measure the organization engagement in term of IS security governance.

In this paper, we will study the practices and commitments of organizations in IS security governance. A survey of 836 medium and large companies at the international level (USA, UK, France, Morocco, China, Russia, etc.) was set up to define the best practices of these organizations regarding information security governance and management. This study allowed us to propose a practical framework to evaluate the organization in their maturity state and to improve their level of IS security governance according to their needs and resources.

The chapter is structured as follows. Section 2 presents the previous work on information security governance proposed in the literature. Section 3 describes the survey carried out among 836 medium and large international companies and gave a faithful picture of their practices in IS security governance through

29 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/building-a-maturity-framework-for-information-security-governance-through-an-empirical-study-in-organizations/270596

Related Content

Fruit-Fly Optimization Algorithm for Disability-Specific Teaching Based on Interval Trapezoidal Type-2 Fuzzy Numbers
Deepak Aeloor (2020). *International Journal of Fuzzy System Applications (pp. 35-63).*
www.irma-international.org/article/fruit-fly-optimization-algorithm-for-disability-specific-teaching-based-on-interval-trapezoidal-type-2-fuzzy-numbers/245270

Rough Set Based Clustering Using Active Learning Approach
Rekha Kandwal, Prerna Mahajanand Ritu Vijay (2013). *Investigations into Living Systems, Artificial Life, and Real-World Solutions (pp. 234-244).*
www.irma-international.org/chapter/rough-set-based-clustering-using/75932

Improving Learning Outcomes for Higher Education Through Smart Technology
James O. Connellyand Paula Miller (2018). *International Journal of Conceptual Structures and Smart Applications (pp. 1-17).*
www.irma-international.org/article/improving-learning-outcomes-for-higher-education-through-smart-technology/206903

Reassessing the Foundations of Semiotics: Preliminaries
Mihai Nadin (2012). *International Journal of Signs and Semiotic Systems (pp. 1-31).*
www.irma-international.org/article/reassessing-foundations-semiotics/64637

Generalized Scaled Prioritized Intuitionistic Fuzzy Geometric Interaction Aggregation Operators and Their Applications to the Selection of Cold Chain Logistics Enterprises
Shanshan Mengand Yingdong He (2018). *International Journal of Fuzzy System Applications (pp. 1-21).*
www.irma-international.org/article/generalized-scaled-prioritized-intuitionistic-fuzzy-geometric-interaction-aggregation-operators-and-their-applications-to-the-selection-of-cold-chain-logistics-enterprises/195673