Chapter 8

Information Security Governance in Large Organizations: A Maturity Framework

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 discuss the information security governance and to address the weaknesses identified in the literature. Based on practices of information security management and governance, the authors propose ISGO, a practical maturity framework for the information security governance and management in organizations. The findings will help organizations to assess their capability maturity state and to address the procedural, technical, and human aspects of information security governance and management process.

DOI: 10.4018/978-1-5225-7826-0.ch008

Copyright © 2019, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
INTRODUCTION

Many organizations today are facing a global governance revolution that could have a direct impact on their information management practices. Information security has become an integral part of daily life, and organizations must ensure that their information security systems are an integral part of daily life.

In a distributed and dynamic services environment, security must not be limited to providing technological solutions but to finding a strategy taking into account business, organizational and technological dimensions (Nassar, Badr, Barbar, & Biennier, 2009). In addition, security must be seen as an ongoing process that aims to optimise security investments and ensure the sustainability of the security measures implemented (Lomas, 2010). However, reference service domain models and architectures have underestimated the definition of security needs, the assets to be protected and the identification of risks to these assets (Huang, Lee, & Kao, 2006; Williams, 2007). For that, we propose to approach the problem of security by a practical approach of governance allowing to identify the various axes of my IT security and to propose the most adequate security measures to the context. However, IT security governance is a real challenge in an open collaborative services environment. In fact, improving security has emerged as one of the top IT priorities across all business lines. So, while companies (R. 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 defence against such threats (R. von Solms & van Niekerk, 2013).

In today’s rapidly changing and evolving environment, IT and security executives have to make difficult calculations and decisions about security with limited information (Dhillon, Syed, & Pedron, 2016). They need to make decisions that are based on analyzing opportunities, risks and security.
CIO Perspectives on Organizational Learning within the Context of IT Governance
[www.igi-global.com/article/cio-perspectives-on-organizational-learning-within-the-context-of-it-governance/180693?camid=4v1a](www.igi-global.com/article/cio-perspectives-on-organizational-learning-within-the-context-of-it-governance/180693?camid=4v1a)

An Analysis of Factors that Influence the Ability of SMEs to Derive Benefit in Four Phases of Electronic Commerce: 34 Australian Case Studies
[www.igi-global.com/chapter/analysis-factors-influence-ability-smes/25903?camid=4v1a](www.igi-global.com/chapter/analysis-factors-influence-ability-smes/25903?camid=4v1a)