Chapter 47
Adoption of ISO 27001 in Cyprus Enterprises: Current State and Challenges

Ioanna Dionysiou
University of Nicosia, Cyprus

Skevi Magirou
University of Nicosia, Cyprus

Angelika Kokkinaki
University of Nicosia, Cyprus

Theodosios Iacovou
University of Nicosia, Cyprus

ABSTRACT

This chapter presents the findings of an investigation on current security practices in Cypriot organizations, including enterprises and public sector divisions. In order to gain knowledge on the deployed security technologies by organizations, a survey was conducted and concluded in late 2010. The survey primarily examined compliance of enterprise current security policies and procedures with ISO 27001 security guidelines. A research analysis has been performed and identified that security mechanisms and the management of information technology (IT) resources may be improved on a number of aspects. Based on the research findings, an assessment of the viability of ISO 27001 in Cyprus is given as well as recommendations on the further deployment of ISO 27001.

INTRODUCTION

Along with the benefits of the universal connectivity (wireless, broadband, 3G), comes an increased risk of security breaches. Attackers, without any specialized knowledge, could launch sophisticated attacks as they have at their disposal easily downloadable software (attack toolkits) capable of breaching computers and networks. Any networked computer is susceptible to an attack, as the majority of attackers belong to the opportunistic hacker category looking for vulnerabilities to exploit, regardless of the physical location of the computer. It only takes a click on an email attachment to launch a virus or start spreading a worm. To make things even worse, if the infected computer belongs to a corporation, the entire corporate network could be contaminated, with severe financial implications.

There is an emergent need for enterprises to protect their resources and assets by taking all necessary measures to prevent, detect, and recover

DOI: 10.4018/978-1-4666-8111-8.ch047

from security attacks (Stallings, 2010). Increased vulnerability and the threat of massive financial damage due to malicious or non-intentional security violations are augmenting the pressure to prevent damage and minimize the risk through active IT security management. However, IT security strategies are perceived to require high investment in security technology while their implementation is also considered to be demanding in terms of highly skilled human resources. In view of these, security is not usually assigned high enough priority by organizations.

Yet, the design and implementation of an effective security strategy in enterprises need not necessarily be an unrealistic goal. The main success factor is well thought out organizational procedures and reliable, informed staff who observe security requirements in a disciplined manner. ISO 27001, an Information Security Management System (ISMS) standard published by the International Organization for Standardization (ISO) provides assurance that the management system for information security is in place. To be more specific, ISO 27001 specifies "the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System within the context of the organization's overall business risks" (ISO, 2005). Compliance to ISO 27001 does not guarantee that the enterprise will never experience any security exploitations; it does though assure that the company has taken all protective measures to avert security attacks, thus lowering the risk of interruptions during business conduct.

Security attacks are on the rise, even in Cyprus, a Eurasian island country in the Eastern Mediterranean. Recent security incidents include a phishing attack targeting the online subscribers of a Cypriot Bank Corporation and the defacement of Cypriot company web sites. It has been observed that many organizations in Cyprus place at relatively low priority initiatives related to IT security. In order to substantiate this hypothesis, an investigation was launched in April 2010 to study existing IT security strategies and policies that are deployed by Cypriot enterprises, focusing on compliance with the ISO 27001 standard. The statistical analysis of the nationwide survey indeed indicated lack of awareness regarding proper security practices. The results were further exploited to unveil the underlying reasons for this situation, especially the non-compliance with the ISO 27001.

Analytically, the following objectives have been set for this chapter:

- Investigate the security policies, procedures, mechanisms, and technologies in Cyprus enterprises towards the detection of the level of compliance with ISO 27001.
- Draw prescriptive conclusions on the subject of ISO 27001 compliance in Cyprus.
- Identification of the contributing factors that delay the ISO 27001 implementation in Cyprus.
- Recommendations and overall directives on the use of ISO 27001 in Cyprus.

The remaining of the chapter is unfolded as follows: Section 2 briefly gives an overview of the ISO 27001 standard. Section 3 describes the logistics on preparing the questionnaire on IT security strategies and policies, which is the investigation's primary research instrument. Section 4 constitutes the analysis part of the paper, where the survey findings are analyzed, followed by Section 5 that assesses the viability of ISO 27001 in Cypriot enterprises by discussing the adoption process and the factors that drive or avert enterprises to adapt the ISO 27001. Recommendations for enterprises, SME (small to medium) and Large, are given in Section 6. Section 7 outlines a framework for security governance in SME. Finally, section 8 concludes this chapter with overall observations.