Chapter 22
ISMS Building for SMEs through the Reuse of Knowledge

Luís Enrique Sánchez
SICAMAN NT, Spain

Eduardo Fernandez-Medina
University of Castilla-La Mancha, Spain

Antonio Santos-Olmo
SICAMAN NT, Spain

Mario Piattini
University of Castilla-La Mancha, Spain

ABSTRACT

The information society is increasingly more dependent upon Information Security Management Systems (ISMSs), and the availability of these systems has become crucial to the evolution of Small and Medium-size Enterprises (SMEs). However, this type of companies requires ISMSs which have been adapted to their specific characteristics, and these systems must be optimized from the point of view of the resources necessary to deploy and maintain them. Over the last 10 years, the authors have obtained considerable experience in the establishment of ISMSs, and during this time, they have observed that the structure and characteristics of SMEs as regards security management are frequently very similar (since they can all be grouped by business size and sector), thus signifying that it is possible to construct patterns for ISMSs that can be reused and refined. In this chapter, the authors present the strategy that they have designed to manage and reuse security information in information system security management. This strategy is framed within a methodology designed for integral security management and its information systems maturity, denominated as "Methodology for Security Management and Maturity in Small and Medium-size Enterprises (MSM2-SME)," and it is defined in a reusable model called "Reusable Pattern for Security Management (RPSM)," which systematically defines, manages, and reuses the aforementioned methodology through a sub-process denominated as "Generation of Security Management Patterns (GSMP)." This model is currently being applied in real cases, and is thus constantly improving.

DOI: 10.4018/978-1-4666-3886-0.ch022

INTRODUCTION

The information society is increasingly more dependent upon Information Security Management Systems (ISMSs), and the availability of these systems has become crucial to the evolution of Small and Medium-size Enterprises (SMEs). However, this type of companies requires ISMSs which have been adapted to their specific characteristics, and these systems must be optimized from the point of view of the resources which are necessary to deploy and maintain them. Our wide experience in the implantation of ISMS over the last 10 years, has allowed us to observe that, with regard to security management, SMEs frequently share many characteristics and structures (which can be grouped by size and business sector), thus making it possible to construct patterns for ISMSs which can be reused and refined. In this paper we show the strategy that we have designed for the management and reuse of security information in the information system security management process. This strategy is set within the framework of a methodology that we have designed for the integral management of information system security and maturity, denominated as "Methodology for Security Management and Maturity in Small and Medium-sized Enterprises (MSM2-SME)". More specifically, this is a reusable model that we have denominated as "Reusable Pattern for Security Management (RPSM)", which is systematically defined, managed and reused through a sub-process of the aforementioned methodology denominated as "Generation of Security Management Patterns (GSMP)". This model is currently being applied in real cases, and is thus constantly improving.

It is extremely important for enterprises to introduce security controls which will allow them to discover and to control the risks that they may be confronted with (Dhillon & Backhouse, 2000; Fernández-Medina, Jurjens, Trujillo, & Jajodia, 2009; Kluge, 2008). However, the introduction of these controls is not sufficient, and systems which manage security in the long term, thus permitting a swift reaction to new risks, vulnerabilities and threats are also necessary (Barlette & Vladislav, 2008; De Capitani, Foresti, & Jajodia, 2008). Unfortunately, present-day companies often do not have security management systems, or those which do exist have been created without the appropriate guidelines or documentation, and with insufficient resources (Vries, Blind, Mangelsdorf, Verheul, & Zwan, 2009; T. Wiander & Holappa, 2006). Moreover, the majority of the security tools available on the market help to solve part of the security problems, but very few tackle the problem of security management in a global and integrated manner. In fact, the enormous diversity of these tools and their lack of integration suppose a huge amount of spending on resources with which to be able to manage them (Alfawaz, Nelson, & Mohannak, 2010; Valdevit, Mayer, & Barafort, 2009).

Therefore, in spite of the fact that real-life has shown that for a business to be able to use information technology and communication with guarantees it needs to have at its disposal guidelines, measures and tools which will allow it to know at all times both the level of its security and those vulnerabilities which have not been covered (T Wiander, 2008), the level of successful deployment of these systems is, in reality, very low. This problem is particularly accentuated in the case of SMEs, which have the additional limitation of not having sufficient human and economic resources to be able to carry out an appropriate management (T. Wiander & Holappa, 2006).

According to recent research (Dojkovski, Lichtenstein, & Warren, 2006; Siponen & Willison, 2009), the success of ISMSs depends mainly upon the following factors:

1. The security is focused on the business;
2. The security is implemented in accordance with the company's business culture;
3. The company's management provides unarguable, visible and committed support,