Chapter 1.4
The Adoption of Information Security Management Standards
A Literature Review

Yves Barlette
GSCM-Montpellier Business School, France

Vladislav V. Fomin
Vytautas Magnus University, Lithuania

ABSTRACT

This chapter introduces major information security management methods and standards, and particularly ISO/IEC 27001 and 27002 standards. A literature review was conducted in order to understand the reasons for the low level of adoption of information security standards by companies, and to identify the drivers and the success factors in implementation of these standards. Based on the findings of the literature review, we provide recommendations on how to successfully implement and stimulate diffusion of information security standards in the dynamic business market environment, where companies vary in their size and organizational culture. The chapter concludes with an identification of future trends and areas for further research.

DOI: 10.4018/978-1-60566-326-5.ch006

INTRODUCTION

In service-oriented, highly industrialized countries, information itself is both a raw material and a product (Castells, 1996). The critical economic role of information and information processing on a firm's productivity may be more important than that from operational efficiency or product innovation (Steinmueller, 2005).

The relevance of information assets to businesses and governments alike can be measured by, for example, the percentage of contributions to gross domestic product (GDP) stemming from information-related processes and services (OECD, 2005). Another argument for the importance of information assets is to see them as "*the 'life-blood' of all businesses*" (Humphreys, 2005, p.15) losing which may bring the business to a dead halt. Lou-

derback (1995) reported in 1995 that one-half of the companies that lose business critical systems for more than 10 days never recover and go out of business. This is increasingly true as companies rely more on their information systems (Kankanhalli et al., 2003). Between 1997 and 2001, U.S. organizations spent $2.5 trillion on information technology, nearly double the amount than the previous five years (Temkin, 2002; Fomin et al., 2005). Informational processes effectively become so critical that private and public institutions alike need to take an active role in ensuring the security of this critical asset (Fomin et al., 2008; GAO, 2004). In order to achieve this task, however, many issues have to be addressed.

With the growing level of interconnectivity between organizations (Barnard & von Solms, 1998), each company is taking its own measures for information security. This leads to the proliferation of different hardware-, software- and processes-based information security measures (von Solms, 1988). The poor security practices of one agent may threaten its partners in the global informational economy (Castells, 1996). This situation calls for a consistent approach to information security management at a company, inter-company, industry, and international levels. Not having proper information security measures in place can be detrimental to a business, while adopting methods for information protection can be a welcomed signal to the business partners that builds trusting relationships with customers, suppliers and stakeholders (Posthumus & von Solms, 2004). The task of adopting proper information security methods is a difficult one. Organizations need to address the task from legal, operational and compliance perspectives; the penalties for failing to succeed are greater than ever (Myler & Broadbent, 2006).

Inadequate levels of security of information systems (IS) in organizations may result in more than monetary penalties to a company. Top management and board directors can become personally accountable for the security of their IS (OECD, 2004). The leading example is the Sarbanes-Oxley Act (2002) which makes corporate executives legally responsible for the validity of reported financial data and thus responsible for the security of their information systems (Hurley, 2003). Despite the criticality of information assets to business operations and the negative implications of poor security, previous research indicates that the level of information security awareness among many managers is low (Broderick, 2006; Knapp et al., 2006).

It is common for a manager of a contemporary organization to ask questions like these: How does my organization's IS become secure? What are the best practices for establishing IS security management? What is my organization's level of security? Which security level should be appropriate? How much money should I invest?

Information security standards could provide answers to many, if not all of these questions. Nevertheless, there are few research studies that examine the effectiveness of management strategies and tools for information security management (Hong et al., 2003). The suitability of available information security management standards for small and medium enterprises (SMEs) has already been questioned (Barlette & Fomin, 2008) although regardless of the size of a company, implementation of information security standards is not a straightforward process.

Responding to the call for rising awareness on the information security management issues (Barlette & Fomin, 2008; Knapp et al., 2006), in this paper we aim to 1) provide an overview of the major information security standards and discuss their adoption factors, 2) analyze the reasons for the low adoption level of information security standards by companies, and 3) examine various possibilities to foster information security standards adoption in the future.

This chapter is structured as follows. In the first section, we provide the definitions and an overview of information security management methods and standards. In the second section, we review