Chapter 4

Information Security Governance

Janne J. Korhonen
Aalto University, Finland

Kari Hiekkonen
Aalto University, Finland

Juha Mykkänen
University of Eastern Finland, Finland

ABSTRACT

In today’s economic, regulatory, and social environment, information security governance and management are topics of great interest to practitioners and researchers alike. In response to the increasingly interconnected, information intensive business landscape, legal pressures, and ongoing scrutiny to transparency and overall governance, organizations are increasingly interested in frameworks and methodologies for security governance and management. As the traditional view of governance as a control and conformance mechanism turns out to be inadequate in changing environments, a specifically contrived, more encompassing and design-oriented approach to information security governance is called for. In this chapter, the authors subscribe to the design science approach in order to outline a prescriptive reference model for information security governance that aims to help institute cross-functional information security management throughout the organization and build it into the organizational design.

INTRODUCTION

As the amount of information and the number of interconnected organizations and individuals continues to increase, so do the risks and costs of security breaches. The tightening regulations of data privacy, loss prevention and transparency require organizations to demonstrate due care and diligence with respect to security. Information security used to cover technical, and in many cases minor, security issues, but has recently evolved to proactive protection of business assets, reputation, profitability, customer confidence and economic performance. Security risks have evolved respectively from accidental computer worms and
viruses to targeted attacks by malevolent parties with specific motivations such as direct economic gain or access to intellectual property. At the same time, an organization’s ability to take advantage of new opportunities, create new markets and operate in the emerging service-based economy depends heavily on its ability to provide open, accessible and available network connectivity and services. Security measures, policies and guidelines must simultaneously both protect information and enable its safe passage to interested parties in different business ecosystems.

While the existing information security frameworks range from detailed technical guidance to high-level principles (Federal Information Security Management Act, 2002; International Organization for Standardization, 2005), there are few actionable organization-wide frameworks that would guide in designing and developing security arrangements, incorporating them in the organization’s operations and monitoring their implementation. Also, the responsibility for information security is too often delegated to the chief information officer (CIO) or the chief security officer (CSO) who is conflicted with demands and lacks leverage to address the problem across multiple business lines or divisions, while too little attention is given to the issue at the chief executive officer (CEO) or board level.

In this chapter, we outline a reference model for information security governance that aims to help the CIO/CSO a) obtain a clearance from the board to organize information security activities by identifiable organizational loci and b) identify and assign respective key roles with requisite responsibilities and accountabilities. The reference model extends and builds on an abstract meta-level governance structure, Agile Governance Model (AGM) (Korhonen, Hiekkanen and Lähteenmäki, 2009, Korhonen, Yildiz and Mykkänen, 2009) and is instantiated for information security.

In order to outline a pragmatic information security governance model that is both actionable and open to validation, we subscribe to the design science approach (e.g. Simon, 1996; Banathy, 1996; Hevner et al., 2004; van Aken and Romme, 2009). Van Aken (2004) argues that understanding a problem is only halfway to solving it and that in management research description-driven research needs to be complemented with prescription-driven development of field-tested and grounded technological rules applicable as design exemplars to classes of managerial problems. Hevner et al. (2004) promote design approach in the context of information systems research.

**BACKGROUND**

As information and information technology are of increasing strategic importance, effective management of IT and information assets becomes a critical strategic concern. IT Governance (ITG) deals with the management of an organization’s use of IT. According to the IT Governance Institute (2007), it is “an integral part of enterprise governance and consists of the leadership and organizational structures and processes that ensure that the organization’s IT sustains and extends the organization’s strategies and objectives”.

Information security has traditionally been defined as the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information (Whitman and Mattord, 2008). Traditional viewpoints on information security included access to information systems, securing communications, security management and development of secure information systems (Siponen and Oinas-Kukkonen, 2007). However, while security considerations are an essential part of IT governance, information security governance goes beyond the IT realm. Information security is increasingly a business issue (von Solms and von Solms, 2005) that calls for governance of its own (von Solms, 2006).

In the networked, always-on business environment of today, it may seem futile to try and