Chapter 12
An Integrated Security Governance Framework for Effective PCI DSS Implementation

Mathew Nicho
University of Dubai, UAE

Hussein Fakhry
University of Dubai, UAE

ABSTRACT

This paper analyses relevant IT governance and security frameworks/standards used in IT assurance and security to propose an integrated framework for ensuring effective PCI DSS implementation. Merchants dealing with credit cards have to comply with the Payment Card Industry Data Security Standards (PCI DSS) or face penalties for non-compliance. With more transactions based on credit cards, merchants are finding it costly and increasingly difficult to implement and interpret the PCI standard. One of the top reasons cited for merchants to fail PCI audit, and a leading factor in data theft, is the failure to adequately protect stored cardholder data. Although implementation of the PCI DSS is not a guarantee for perfect protection, effective implementation of the PCI standards can be ensured through the divergence of the PCI standard into wider information security governance to provide a comprehensive overview of information security based not only on security but also security audit and control. The contribution of this paper is the development of an integrated comprehensive security governance framework for ‘information security’ (rather than data protection) incorporating Control Objectives for Information and related Technology (COBIT), Information Technology Infrastructure Library (ITIL) and ISO 27002.
1. INTRODUCTION

Compliance is one of the major issues in information security management (Al-Hamdani, 2009), but due to time deadline, lack of expertise in this area, multitude of regulations, lack of experienced staff, and cost factor they generally adopt a highly fragmented and siloed approach to governance, compliance and security. It has been stated that in order for information security measures to become effective, security should not only be built like a staircase of combined measures (Hagen, Albrechtsen, & Howden, 2008) but the range of security policies and support activities needs to be broadened (Sundt, 2006). While it is a widely accepted fact that information security has currently moved away from its technical focus, it still needs to be addressed from a multidimensional, holistic and comprehensive view for ensuring a secure information systems environment (von Solms, 2001). Implementing information security is thus not only a time consuming and complex process, but also a multidisciplinary concept cutting across several related disciplines (Eløf & Eløf, 2005). IS security viewed from this holistic perspective considers strategic, tactical, and operational issues surrounding the planning, analysis, design, implementation, and maintenance of an organization’s information security (Choobineh, Dhillon, Grimaila, & Rees, 2007). This perspective requires the PCI DSS version 2.0 not only to diverge from its focused technical domain and expand to its outer concentric rings of the greater IS domain, but also forces it to link to the organizational strategic goals which is a major concern for IS managers. This strategic alignment of IS with business is the main focus of IT governance. In a survey conducted by PWC and IT Governance Institute in 2005 and 2008 (ITGI, 2006, 2008b) the importance of strategic alignment of organisational goals with the IT goals was cited by 90% of the respondents as being vital to the organisation. Hence, strategic alignment can come about (result) if the PCI DSS goal of securing cardholder data is aligned with the IS goals and finally to the higher level organisational goals. Thus, an information security governance approach of PCI DSS can ensure greater security than an isolated siloed approach of PCI DSS standards implementation.

Since the purpose of this paper is to ensure the effectiveness of the PCI DSS implementation through an integrated approach of linking it with the wider relevant IT governance and security frameworks, the result is an integrated security governance framework. With this objective in mind the paper is divided into the following three sections. The first section provides an overview of the PCI DSS and its relevance followed by cases of security breaches. Section 2 takes a multidimensional view of information security by analysing relevant IT governance models that are relevant for ensuring a comprehensive but optimally integrated IS security. Section 3 proposes the final conceptual model incorporating PCI DSS along with the selected governance models.

2. PCI DSS

The Payment Card Industry Data Security Standards is an open global forum launched in 2006 by the five global payment brands namely American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. It was created for developing, managing, educating, and communicating the PCI Security Standards, including the Data Security Standard (PCI DSS), Payment Application Data Security Standard (PA-DSS), and PIN Transaction Security (PTS). It is the very first industry-wide standard which focuses on the credit card industry that aims at achieving a strong protection of sensitive consumer and cardholder data, and preventing major security issues (Liu, Xiao, Chen, Ozdemir, Dodle, & Singh, 2010). The objective of the standard was to enhance the security of the cardholder through protection of cardholder data and thus help facilitate global adoption of consistent data security measures.