Chapter 10

Relationships between Information Security Concerns and National Cultural Dimensions: Findings in the Global Financial Services Industry

Princely Ifinedo
Cape Breton University, Canada

ABSTRACT

This study investigates the relationships between the contextual factor of national culture and information security concerns in the global financial services industry (GFSI). Essentially, this study attempts to expand the breath of information provided in the recent 2009 Deloitte Touche Tohmatsu (DTT) survey, which reported such issues in the financial services industry. The inference from the 2009 DTT survey was that information security concerns across GFSI are being informed solely by industry-related standards or imperatives. As such, perceptions and attitudes towards such issues were thought to remain unchanged in differing contexts. Results from this study’s analysis showed that the perceptions of information security concerns in GFSI compared reasonably well, but also varied by some national cultural attributes to debunk such a claim. Corporate managers in the industry may benefit from this research’s findings as they formulate country-wide information security policies and strategies. As well, insights from this current effort indicate that it would be erroneous for practitioners to accept that entities in the financial services hold exactly the same view on information security issues in their industry. Future research avenues are discussed.

INTRODUCTION

It is a known fact that practitioners in the Global Financial Services Institutions (GFSI) are proactive in protecting customer data and thwarting emerging threats in their industry (Goodhue and Straub, 1991; Jung et al., 2001; Chen et al., 2008). In fact, one of the objectives of GFSI is to ensure that clients’ data and information are not compromised. In other words, GFSI have an inherent need
to be aware of the critical nature of information security (Goodhue and Straub, 1991; Kankanhalli et al., 2003). The description of GFSI as provided by the Deloitte Touche Tohmatsu (DTT) survey will be used in this work. In the DTT survey, GFSI included global financial institutions, banks, insurance companies, payment processors, and asset management companies. More precisely, a global financial services institution acts as an agent for its clients/customers (Johnson, 2000; Moshirian, 2007). It is worth noting that the term “GFSI” differs from the closely related phrase “global financial institutions”, such as the World Bank and International Monetary Fund. The job of these bodies includes coordinating and regulating global financial systems at the international level (Alexander et al., 2004; Moshirian, 2007).

For businesses operating in the financial services industry, new technologies, business initiatives, and regulations often give rise to new threats and risks (Chaturvedi et al., 2000; Kankanhalli et al., 2003; DTT-Global Security Survey, 2009). A respondent in a recent DTT security survey comments, “New technologies and new business models are causing us to blindly run full speed toward the unknown. And the hot breath of threats and risk is on our necks at all times” (DTT-Global Security Survey, 2008, p. 1). The very essence of financial services business implies that various attempts must be made to secure clients’ information and related resources. Kritzinger and Smith (2008, p. 224) notes that the “primary goal of information security is to protect information and ensure that the availability, confidentiality, and integrity of information are not compromised in any way.” Schatz (2008, p. 94), however, asserts that “it is impossible to ever achieve a state of perfect security in which all risks are mitigated to a level that is acceptable to the business.” What is advised is for corporate managers including those in the financial services industry to constantly assess their risk environments, gain an understanding of which risks need to be prioritized, and adjust their programs to address new security concerns or threats (ISO/TR 13569, 2005; EDS, 2007; Schatz, 2008).

Threats and risks in the financial services industry may stem from both internal and external sources. Such threats can be either malicious or non-malicious in nature. Both, internal and external malicious threats can manifest in many forms, including the introduction of malwares, the theft of corporate secrets and information, and the corruption, deletion, and alteration of organizational data. This paper’s focus is on internal non-malicious threats, which is understudied compared to malicious outsider threats (Theoharidoua et al., 2005; Walker, 2008; Willison and Siponen 2009). Internal non-malicious threats, encompasses human, operational, and organizational issues. Such threats can undermine the functioning and public standing of an organization if not properly managed (Goodhue and Straub, 1991; Theoharidoua et al., 2005; infoLock Technologies, 2006; Willison and Siponen 2009; Ifinedo, 2009). Examples of non-malicious internal threats include a lack of formal information security strategy, a lack of top executive support in dealing with security threats and risks, absence of commitment and funding for regulatory requirements, a lack of programs for managing privacy compliance, incompetent information security (IS) skills, and a lack of IS awareness programs, among others (Kankanhalli et al., 2003; Chang and Yeh, 2006; DTT-Global Security Survey, 2009).

The innate need to focus on information security concerns as well as gain an understanding of emerging threats in their industry have caused GFSI practitioners to start investigating and reporting such issues. The series of surveys conducted by DTT stand out in this regard (DTT - Global Security Survey, 2005; 2008; 2009). The first of the DTT surveys was published in 2003 and others have since followed. These surveys were designed to educate GFSI practitioners on IS security concerns, i.e. threats, risks, and compliance issues, compare in the global arena. A summary of the 2009 survey’s findings is available online.