Socio-Economic Correlates of Information Security Threats and Controls in Global Financial Services Industry: An Analysis

Princely Ifinedo, Department of Financial and Information Management, Cape Breton University, Nova Scotia, Canada

ABSTRACT

Threats to data and information assets of Global Financial Services Industry (GFSI) are ever-present; such problems, if not well understood, could lead to huge negative impact. To some extent, the environment where a business operates does matter for its success. This study presents information about the relationships between selected socio-economic factors and information security threats and controls in the financial services industry. Essentially, it seeks to enrich the information provided in the 2012 Deloitte Touche Tohmatsu Limited (DTTL) survey that dealt with about security threats in the industry. This study’s findings indicated that contextual factors, such as national wealth, transparency levels, staff training, tertiary education enrolment, and buyer sophistication, do have positive associations with some information security threats and controls. Practitioners and academicians can benefit from this study’s insights.

Keyword: Buyer (Consumer) Sophistication, Extent of Staff Training, Global Financial Services Industry, Information Security Threats and Controls, National Transparency Levels, National Wealth, Tertiary Education Enrolment

INTRODUCTION

Organizations in the Global Financial Services Industry (GFSI) often ensure that the Confidentiality, Integrity or Availability (CIA) of their data assets is assured. Goodhue and Straub (1991) offer several reasons why firms in the financial services sector may be more wary of breaches and threats relative to other businesses. The reasons they espoused include: a) over-reliance on information systems (IS) use in their operations; b) potential for large losses emanating from breaches in their operations; and c) the need to maintain a good public image and assure the confidentiality and integrity of their data and IS assets. In addition, GFSI are sub-

DOI: 10.4018/ijisss.2015040104
jected to strict regulatory oversight (Ramady & Kantarelis, 2009; Delimatsis, 2013; Fernandes, 2013). Indeed, the DTTL (2012, p.2) concluded that “[w]ith increasing business demands and evolving regulatory frameworks, information security is a top priority for financial services industry organizations.”

It is worth noting that “it is impossible to ever achieve a state of perfect security in which all risks [and threats] are mitigated to a level that is acceptable to the business” (Schatz, 2008, p. 94). To that end, practitioners in the financial services industry are advised to constantly assess their risk environment and adjust their programs to confront any emerging security threats in their industry (ISO/TR 13569, 2005; EDS, 2007). Jung, Han, and Lee (2001) noted that the majority of corporations, including those in the financial sectors face four main threats to organizational IS data assets: interception (the prevention of data from arriving at where it is headed), interruption (the break in data or information flow), modification (the alteration and adjustment of data or information), and fabrication (the reconstruction of data or information with the intent to deceive). Clearly, these threats present CIA concerns to GFSI.

Apparently, the desire to focus on information security threats and subsequently gain an understanding of such concerns in GFSI has made practitioners in the industry to investigate and report such issues. Some firms including PricewaterhouseCoopers and Deloitte Touche Tohmatsu Limited (DTTL) have provided insight on such issues in their industry. This study will make use of the DTTL reports as their publications, which have been produced over a decade, have received the attention of IS security scholars (e.g. Ifinedo, 2009a; 2009b; 2013). These surveys attempt to educate GFSI's practitioners about information security threats; they also provide comparative insights across regions of the world. Key findings in the latest survey for 2012 are available online (DTTL, 2012). Information from such sources is important given the ever-growing cybercrimes in modern organizations (Murthy, Nagadevara, & De*, 2010).

Information in the 2012 DTTL survey provide relevant information about pressing information security threats and controls in GFSI, and regional differences on such issues are provided. However, the report did not provide information related to the influences arising from socio-economic factors. This layer of information may be useful for leaders of GFSI as they manage the attitudes and perceptions of their employees on such issues given that prior researchers have shown that contextual factors notably those of socio-economic underpinnings matter in such discourse (Milberg, Smith, & Burke, 2000; Bagchi, Kirs, & Cerveny, 2006; Bia & Kalika, 2007; Chen, Medlin, & Shaw, 2008; Ifinedo, 2009a; 2013).

In this study, the potential relationships between contextual factors of socio-economic dimensions and information security threats and controls will be examined. The selected contextual factors such as economic wealth, customer (buyer) sophistication, tertiary education enrolment, extent of staff training, and transparency levels have been identified as important factors in the assessment of information security issues across nations. For example, Ifinedo (2009a) found that employees of GFSI from more affluent nations tend to receive more training and awareness sessions on security and privacy issues compared to counterparts from less economically endowed nations. Admittedly, there are other relevant contextual factors such as national culture that could be considered; the aforementioned factors were chosen for illustration purposes.

The purpose of study is twofold. First, it desires to increase the depth of information provided in the 2012 DTTL survey by examining the relationships between relevant contextual factors and six (6) information security threats and controls in the report. Second, it intends to add to growing body of work discussing information security concerns in GFSI. The scan of the relevant literature shows that very little is known about the relationships between the selected factors in the context of GFSI. It is maintained that studies designed to increase understanding in the area will be beneficial to both
Prediction of Non-Functional Properties of Service-Based Systems: A Software Reliability Model
www.igi-global.com/chapter/prediction-non-functional-properties-service/52199?camid=4v1a