Information Technology Security Concerns in Global Financial Services Institutions: Do Socio-Economic Factors Differentiate Perceptions?

Princely Ifinedo, Cape Breton University, Canada

ABSTRACT

Practitioners in Global Financial Services Institutions (GFSI) know that they must concern themselves with protecting customer data and thwart emerging threats in their industry. The objective of this study is to provide a level of understanding and insight not apparent in a recent survey that investigated Information Technology (IT) security concerns across GFSI. This research builds on that prior effort and aims to investigate whether socio-economic factors differentiate IT security concerns across GFSI. It has been suggested that security concerns vary by socio-economic contexts. The authors' analysis of Deloitte Touche Tohmatsu (DTT) data showed that perceptions of IT security issues across surveyed GFSI varied on a few security concerns, but remained unchanged on a majority of issues when grouped according to selected socio-economic measures. This finding permitted us to suggest that IT security threats and risks in the financial sector compare reasonably well across socio-economic contexts. As a consequence, managers of GFSI may avail themselves of this information as they develop and propose measures (and counter-measures) for managing security concerns in their industry. Further, the attention of managers is alerted to areas where differences were noticed. [Article copies are available for purchase from InfoSci-on-Demand.com]

Keywords: Financial Industry; Global Financial Services Institutions; IT Security Concerns; IT Security Management; Security Threats; Socio-Economic Indicators

INTRODUCTION

The use of information technology (IT) by Global Financial Services Institutions (GFSI) in their operations provides them with tremendous benefits and advantages (Johnson, 2000; Hee et al., 2003). At the same time, there are inherent threats associated with the use of such technologies in this industry (Chaturvedi et al., 2000; Bank of Japan, 2007; Ifinedo, 2008). GFSI practitioners know that they must proactively work towards protecting customer data and thwarting emerging threats. In this paper, the description of GFSI as provided by the Deloitte...
Touche Tohmatsu (DTT) survey will be used. Examples of GFSI in the survey included firms from a variety of sectors, including banking, securities, insurance and asset management. The primary function of a GFSI is to act as an agent for its clients and customers (Johnson, 2000; Moshirian, 2007; DTT-Global Security Survey, 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).

The literature on GFSI suggests that they often comply with comparable performance measurements, benchmark assessments, and other industry-related standards and practices (Johnson, 2000; Berger and DeYoung, 2001; Alexander et al., 2004). By the same token, the use of Information and Communication Technologies (ICT), including the Internet has become a standard practice in the financial institutions industry (Johnson, 2000; Gupta et al., 2004; Business, Wires, 2005; DTT-Global Security Survey, 2006; 2007; Bank of Japan, 2007). Suffice it to say that the increasing use of ICT in the operations of GFSI ushers in new risks and concerns (Chaturvedi et al., 2000; Bank of Japan, 2007; DTT-Global Security Survey, 2007). Chaturvedi et al. (2000), citing the Information Security Industry Survey (1999), indicate that since 1998, upwards of 20 percent of financial institutions have suffered disruptions to their information and network systems. They add that “information security [management], therefore, is a pivotal business and technical undertaking for any company involved [in] … financial activities.” It is worth mentioning that the recent Computer Crime and Security Survey (2007) showed that financial fraud has overtaken virus attacks as businesses’ main source of financial loss. A report published by the Bank of Japan (2007) echoes a similar sentiment when it notes, in recent years, the development of information technology (IT) has brought with it a rapid increase in the use of open network systems, as typified by the Internet, to provide financial services. Concurrently, proper management of information security risks such as the risk of service interruptions, theft or alteration of data, impersonation and other events resulting from unauthorized access to the computer system is rapidly becoming critical.

Jung et al. (2001) note that the majority of corporations, including those in the financial sectors face four main threats to organizational IT data and assets: interception (the prevention of data from arriving at where it is intended), 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). They found that while some industries such as retail and manufacturing are concerned with only one or two threats, the same may not be true for financial services institutions where the four threats appear to be a source of significant concern.

Indeed, the literature suggests that IT security threats, risks, and concerns vary by industry (Goodhue and Straub, 1991; Kankanhalli et al., 2003; Yeh and Chang, 2007). 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 note include: a) over-reliance on ICT 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 ICT assets. Financial services institutions, due in part to the aforementioned factors, face a constant challenge and have to find ways to protect and secure their ICT and business transactions from sophisticated criminals (Willison and Backhouse, 2006; Doherty and Fulford, 2005; Kruck and Teers, 2008). In brief, there is a need for studies that investigate the readiness and capability of GFSI to address IT security
Related Content

Evaluating the Quality and Usefulness of Data Breach Information Systems
[www.igi-global.com/chapter/evaluating-quality-usefulness-data-breach/72748?camid=4v1a](www.igi-global.com/chapter/evaluating-quality-usefulness-data-breach/72748?camid=4v1a)

A Clustering Approach Using Fractional Calculus-Bacterial Foraging Optimization Algorithm for k-Anonymization in Privacy Preserving Data Mining
Adaptive Intrusion Detection Systems: The Next Generation of IDSs
www.igi-global.com/chapter/adaptive-intrusion-detection-systems/105811?camid=4v1a

Comprehensive Risk Abatement Methodology as a Lean Operations Strategy
www.igi-global.com/article/comprehensive-risk-abatement-methodology-as-a-lean-operations-strategy/127540?camid=4v1a