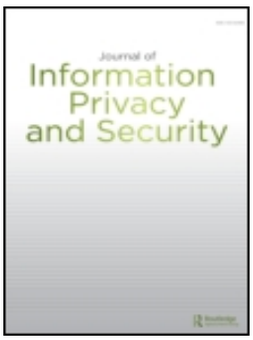

Journal of Information Privacy and Security

ISSN: 1553-6548 (Print) 2333-696X (Online) Journal homepage: http://www.tandfonline.com/loi/uips20

An Exploratory Study of the Relationships between Selected Contextual Factors and Information Security Concerns in Global Financial Services Institutions

Princely Ifinedo

To cite this article: Princely Ifinedo (2011) An Exploratory Study of the Relationships between Selected Contextual Factors and Information Security Concerns in Global Financial Services Institutions, Journal of Information Privacy and Security, 7:1, 25-49, DOI: 10.1080/15536548.2011.10855904

To link to this article: http://dx.doi.org/10.1080/15536548.2011.10855904

An Exploratory Study of the Relationships between Selected Contextual Factors and Information Security Concerns in Global Financial Services Institutions

Princely Ifinedo, Cape Breton University, Sydney, Canada
princely_ifinedo@cbu.ca; pifinedo@gmail.com

ABSTRACT

This paper examines the relationships between three contextual factors i.e. transparency levels, information and communication technologies (ICT) use laws, and national legal systems efficiency and information security concerns in the global financial services institutions (GFSI). This research essentially seeks to expand the breadth of knowledge provided in the 2009 Deloitte Touche Tohmatsu (DTT) survey, which reported on information security issues in GFSI. This current study used secondary data sources for its analysis. The inference from the 2009 DTT survey was that information security concerns across GFSI are being informed solely by industry-related standards or imperatives. To that end, perceptions and attitudes toward such issues were thought to remain unchanged in differing national contexts. However, this study's data analysis showed that the perceptions of information security concerns among GFSI employees across the world compare somewhat and also differ, in other respects. Also, this research's findings indicated that GFSI practitioners need to be aware of two information security concerns: a) how information security and business initiatives are appropriately aligned in their organizations, b) the issue of who has the responsibility for privacy in their setups. Against the backdrop of the countries used in this study and the three contextual factors considered, this study found that these two issues to be significantly relevant to the management of security and privacy concerns in GFSI. The implications of the study' findings for practitioners and academic researchers are discussed, and possible areas of future research outlined.

KEYWORDS

Information Security Concerns, Non-malicious Internal Threats, Financial Services Industry, Transparency Levels, Information and Communication Technologies (ICT) Use Laws, Legal Systems Efficiency

INTRODUCTION

Today's businesses are confronted with unprecedented security challenges. 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; Ifinedo, 2009a; DTT-Global Security Survey, 2009). Global Financial Services Institutions (GFSI) operate in an industry where constant efforts must be made toward

proactively protecting customer data and thwarting emerging threats (Goodhue and Straub, 1991; Jung et al., 2001; Kankanhalli et al., 2003; Ifinedo, 2009b). In fact, one of the objectives of GFSI is to ensure that clients' data and information are not compromised; as such, GFSI need to be aware of the critical nature of information security. The description of GFSI as provided by the Deloitte Touche Tohmatsu (DTT) survey will be used in this paper. Therein, GFSI included global financial institutions, banks, insurance companies, payment processors, and asset management companies.

According to Kritzinger and Smith (2008, p. 224), 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, 2009a). 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, absence of executives with responsibility for privacy issues in organizations, a lack of programs for managing privacy compliance, incompetent information systems (IS) security skills, and a lack of IS awareness programs, among others (Kankanhalli et al., 2003; Chang and Yeh, 2006; DTT-Global Security Survey, 2005; 2009).

GFSI practitioners, perhaps realizing the need to focus on information security concerns and gain an understanding of emerging threats in their industry, have themselves started 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 information 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 (DTT - Global Security Survey, 2009).

This current research focuses on the financial services industry for two reasons. First, GFSI is one of the backbones of major economies around the world (Alexander et al., 2004; Johnson, 2000; Moshirian, 2007). Second, researchers (e.g. Goodhue and Straub, 1991; Jung et al., 2001; Kankanhalli et al., 2003; Chang and Yeh, 2006) have called for separate attention to be paid to the financial services sector as that industry's characteristics and experiences with respect to information security issues are somewhat different from those of other industries'. In fact, Kankanhalli et al. (2003) and Chang and Yeh (2006) found that significant differences exist across industries, including the financial services sector in relation to the types and scope of IS threats encountered (see also Jung et al., 2001). As a consequence, more useful insights will emerge by focusing attention on the realities in the GFSI industry.

Interestingly, Goodhue and Straub (1991) offer several reasons as to why firms in the financial services sector may be more wary of breaches and threats relative to other businesses. The reasons they provided include the following: a) over-reliance on 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. To some degree, the foregoing discussion offers insight as to why the perceptions of information security concerns in the GFSI need not be conflated with those of other industries.

That being said, the findings in the 2009 DTT survey infer that the perceptions of, and attitudes toward *information security concerns across GFSI are being informed solely by industry-related standards or imperatives.* This thinking seems to suggest that contextual factors may mean very little. Were this to be true, studies would not indicate that countries and even blocs of nations, for example, the European Union, establish different codes of conduct related to IS and security compliance issues, to enable them properly manage ensuing concerns in their contexts (Bia and Kalika, 2007; Chung et al., 2006; Chen et al., 2008). It is posited in this paper that contextual factors such as national transparency levels, information and communication technologies (ICT) use laws, and the efficiency of legal systems (or legal systems efficiency) might be related to how GFSI employees around the world assess such concerns in their contexts.

Previous research has underscored the critical importance of contextual factor such as national culture on the assessment of IS security issues in organizations (Milberg et al., 1995; 2000; Kankanhalli et al., 2003; Chen et al., 2008). Likewise, Ifinedo (2009a) showed that socio-economic factors are particularly relevant in the discourse of IS

security concerns in financial services organizations. However, much remains to be learned about the relevance of the three selected contextual factors for this discourse. These factors, as the literature suggests, could influence the responses, values, and attitudes of GFSI workers with regard to how they perceive new practices, including those related to information security concerns (e.g., Oxley and Yeung, 2001; Kovačić, 2005; Shih et al., 2005; Bagchi et al., 2006; Chung et al., 2006; Bia and Kalika, 2007). Importantly, it is believed that the inclusion of the three selected factors in this study serves to complement emerging knowledge regarding their critical importance in the assessment of IS security issues in financial services and related industries. Admittedly, there are other relevant contextual factors that could be considered; the aforementioned factors were chosen for illustration and brevity's purposes as well as for their pertinence to IS security issues.

Specifically, this present study's main purpose is to expand the breadth of information provided in the 2009 Deloitte Touche Tohmatsu (DTT) survey by examining the correlations between the aforementioned contextual factors and the thirteen (13) reported information security concerns in the financial services industry. This study is particularly designed to provide answers to the following questions: What relationships exist between the selected contextual factors and information security concerns across GFSI? Against the backdrop of three selected contextual factors, which information security issues should GFSI practitioners be paying more attention to in their industry?

BACKGROUND OF THE STUDY

The advent of new technologies, the introduction of new business models, and the imposition of new government regulations have increased the complexity, threats, and risks facing modern organizations, including GFSI (DTT - Global Security Survey, 2005; 2009; Chao et al., 2006; Pontus and Erik, 2008; Ifinedo, 2009b). As previously noted, it is almost impossible to fashion a perfect security plan to mitigate every threat confronting an organization. What savvy corporate managers do is constantly assess their risk environments and adjust their security programs and policies accordingly (infoLock Technologies, 2006). Better informed managers know that securing the future of their organizations is linked to how well emerging challenges are understood and subsequently contained (Ifinedo, 2009b; Reinhold et al., 2009).

However, there are managers who still find it difficult to assess their risk environment and sensitize employees to security issues (DTT - Global Security Survey, 2005; Chang and Yeh, 2006). According to the DTT - Global Security Survey (2005), about 45 percent of GFSI organizations does not adequately convey the importance of IS security concerns to their workers. Indeed, information security awareness is one exercise among various organizational mechanisms used to contain insider or internal threat management concerns (e.g. infoLock Technologies, 2006). It can be equally

argued that the inability to assess relevant IS security concerns and provide security awareness to employees may be inimical to the organization.

For the purpose of this study, information security concerns refer to threats, risks, and other vulnerabilities to IS assets in the GFSI. Also, the scope of the definition is extended to privacy issues, which relevant literature notes are a major concern for financial services organizations (Jung et al., 2001; Kankanhalli et al., 2003; DTT - Global Security Survey, 2005; 2008). ISACA (2006) defines risks as "events that negatively impact the accomplishment of business objectives". Rezgui and Marks (2008, p. 243) cite the description of risk provided by the International Organization of Standardization (ISO) as "the potential that a given threat will exploit vulnerabilities of an asset or group of assets."

Published research on the general assessment of information security concerns in organizations is still evolving (e.g. Kritzinger and Smith, 2008; Chao et al., 2006; Sumner, 2009). Kritzinger and Smith (2008) suggest a framework for information security awareness for industry that covers both technical and non-technical issues. Chao et al. (2006) also offer an assessment of security controls for organizations. Sumner (2009) writes about the assessment of information security threats and the impacts on organizations and Hoesing (2009) discusses emerging security assessment techniques and tools in modern enterprises. The foregoing frameworks are generic and do not specifically address security concerns in the financial services industry. This explains why they are not used in this current study. Further to this, it was decided that it will be worthwhile to scope this study's discussion to frameworks and guidelines that are in line with this stated objective.

To some degree, relevant international bodies offer guidelines on how GFSI should assess or deal with emerging information security concerns in the industry. The ISO/TR 13569 (2005) has guidelines that address the development of an information security program for institutions in the financial services industry. Likewise, EDS (2007) recommends ways in which financial institutions could manage information risk and priority issues. The Control Objectives for Information and Related Technology (COBIT) guidelines from ISACA (2006) can also be tailored to the needs of GFSI. As well, a modified version of the Carnegie Mellon's Capacity Maturity Model (CMMI) can be used for assessing security programs in GFSI. Insights from the work of Schatz (2008) as well as items from the 2009 DTT survey permit us to suggest that both the CMMI and COBIT models informed the composition of items used for the DTT survey. The 13 security concerns investigated and reported in the 2009 DTT survey are highlighted in Table 1.

The Deloitte Touche Tohmatsu (DTT) Survey and Findings

Deloitte Touche Tohmatsu (DTT) is an international firm that provides audit, tax, consulting, and financial advisory services to both public and private clients. DTT has a global network of member firms in 140 countries. The financial services sub-unit of the organization employs more than 1,500 partners and 17,000 financial services professionals in more than 40 countries. Over the past five years, this sub-unit has used its contacts, networks, and reach to research IT security concerns and issues in GFSI around the world. The first survey issued by the financial services sub-unit appeared in 2003 and four others have since followed (see DTT - Global Security Survey, 2005; DTT - Global Security Survey, 2007). Participants in the 2009 DTT study came from 31 countries and almost all regions of the world, i.e., Asia Pacific (AP) excluding Japan (JP), Europe, the Middle East & Africa (EM), Latin America and the Caribbean Region (LC), and North America (NA). The DTT researchers excluded Japan from the Asia Pacific region's data set to suggest that Japan's perceptions of the issues are significantly different from those of regional counterparts.

Other information in the 2009 DTT survey pertinent to this study are as follows: Their data came from 169 major GFSI, of which 29% were among the top 100 global financial institutions, 26% were among the top 100 global banks, and 14% were among the top 50 global insurance companies. The annual revenues of the respondent companies ranged from less than $1 billon to over $15 billion. The unit of analysis of the DTT survey was the organizational level of each institution. In that regard, responses from knowledgeable members such as Chief Information Security Officers and Chief Security Officers were used. They were asked to give perceptions representative of their organizations' views or standing on the issues being investigated.

Perhaps due to space limitations, the authors of the survey reported aggregate results/responses for each of the regions, which they implied provides a rough indicator of security concerns for countries in each region. A full list of the participating counties in the DDT survey is not available online; however, DTT researchers have obliged this current study with a list of all countries in the 2009 survey. The countries/regions sampled in this study are diverse. The regions' data is shown in Table 1. It is important to relate the items in Table 1 to the issues being discussed in this study. Some of the examples of non-malicious insider threats that GFSI could encounter have been adequately reflected. For example, the absence of commitment and funding for regulatory requirements, a lack of formal information security strategy, and lack of programs for managing privacy compliance, correspond to items numbered #2, #3, and #11, respectively on Table 1.

Table 1. Summary of security concerns in GFSI across regions

No.	Security concern	AP	JP	EM	NA	LC
#1	Respondents who feel that security has risen to executive management and/or board as a key imperative	77%	79%	70%	63%	78%
#2	Respondents who feel they have commitment and funding to address regulatory requirement	69%	65%	56%	58%	63%
#3	Respondents who indicated that they had a defined and formally documented information security strategy	62%	50%	64%	62%	68%
#4	Respondents who feel that information security and business initiatives are appropriately aligned	31%	30%	32%	28%	40%
#5	Respondents who indicated that their information security budget has increased	54%	25%	60%	65%	75%
#6	Respondents who indicated that their expenditures and information security were 'on plan' or 'ahead of requirements' based on the organization's current needs	31%	5%	50%	26%	59%
#7	Respondents who incorporated application security and privacy as part of their software development cycle	38%	40%	26%	32%	41%
#8	Respondents who feel they presently have both the required competencies to handle existing and foreseeable security requirements	23%	25%	41%	33%	33%
#9	Respondents whose employees have required at least one training and awareness session on security and privacy in the last 12 months	58%	90%	64%	82%	82%
#10	Respondents who have an executive responsible for privacy	23%	85%	58%	82%	24%
#11	Respondents who have a program for managing privacy compliance	38%	84%	43%	76%	18%
#12	Respondents who have experienced repeated internal breaches over the last 12 months	33%	17%	26%	27%	30%
#13	Respondents who have experienced repeated external breaches over the last 12 months	58%	17%	49%	51%	50%

Source: DTT-Global Security Survey (2009)

Contextual Factors: Transparency Levels, ICT use Laws, and Efficient Legal Systems

The three contextual factors considered here are as follows: countries' transparency levels, ICT use laws, and legal systems efficiency. Prior studies have used such factors as variables in cross-country, comparative research (e.g., Gust and Marquez, 2004; Kovačić, 2005; Shih et al., 2005; Bagchi et al., 2006). Transparency level refers to the extent to which honesty and fairness prevails in a country; to some extent, this variable impacts the management of privacy and security compliance issues. ICT use laws refer to how the laws related to the use of IS and related technologies have been instituted and enforced in a country. The legal systems efficiency refers to the degree to which rules and regulations in a country are defined, enforced, and above all, free from manipulation.

The research's premise is that personal attitudes and behaviors can be influenced by the law of the land, in particular those enacted for IS use (Shih et al., 2005; Ifinedo, 2009b; Cohn et al., 2010; Azad et al., 2010). It is asserted here that the attitudes and

behaviors of GFSI employees with respect to their views on information security concerns are linked to the quality of the ICT use laws and other regulatory oversights in their various countries. Indeed, Shih et al. (2005) showed that countries with an efficient rule of law fared better with the diffusion of innovations than counterparts with poorer legal environments. It is believed that accepting new security practices, policies, and strategies to enable GFSI better manage non-malicious insider threats is innovative (Ifinedo, 2009a).

Furthermore, entities in differing countries and regions of the world are conditioned by socio-cultural imperatives (Gust and Marquez, 2004; Bagchi et al., 2006; Chen et al, 2008; Ifinedo, 2009b). Individuals based in differing localities may view issues in ways that have been preconditioned by their environments. For example, individuals from societies rife with corruption (i.e. less transparency) may have little or no need for adherence to organizational security and privacy compliance policies, and so forth. To examine the relationships between the information security concerns and the three variables, data was obtained from reputable international sources. Table 2 shows the transparency levels, the quality of ICT use laws, and legal systems efficiency for each of the countries used in this study.

PROPOSITIONS FORMULATION

Three relevant propositions were formulated to test the relationships between the three contextual factors and the perceptions of security concerns by GFSI employees. Chung et al. (2006) assert that countries sometimes employ legal and technological-related approaches in rallying against IS security threats. Evidence in the literature shows that national legal environments and information security issues/concerns are positively associated (e.g. Milberg et al., 1995; 2000; Shih et al., 2005). Likewise, other researchers (e.g. Bertort et al., 2001; Oxley and Yeung, 2001; Kovačić, 2005; Bagchi et al., 2006; Azad et al., 2010) have shown that the spread of innovative practices and systems correlate with transparency levels across countries. Thus, it is predicted that:

Proposition (P1): The perceptions and attitudes toward IS security concerns in GFSI will correlate with transparency levels across countries.

Prior academic research and development reports indicate that there is a positive correlation between the availability of quality ICT use laws and the implementation of technological innovations across countries (e.g. Oxley and Yeung, 2001; Shih et al., 2005; Bagchi et al., 2006; Bia and Kalika, 2007; World Economic Forum, 2009). Likewise, researchers (e.g. Milberg et al., 2000; Gust and Marquez, 2004; Ifinedo, 2009a) have shown that the availability of efficient national legal systems has a direct relationship on how innovative security practices, concepts, and policies are being accepted across countries. Thus, it is predicted that:

Proposition (P2): The perceptions and attitudes toward IS security concerns in GFSI will correlate with the quality of ICT use laws across countries.

Proposition (P3): The perceptions and attitudes toward IS security concerns in GFSI will correlate with legal frameworks efficiency across countries.

RESEARCH METHODOLOGY

As previously noted, the data used in this study came from secondary sources. As such, the study's main data – information security concerns in GFSI were taken from the DTT Global Security Survey (2009); the thirteen (13) security concerns are presented in Table 1. Data for other variables were obtained from internationally recognized bodies such as the World Economic Forum (2009) and Transparency International (2009). These bodies produce cross-country data on a variety of indicators annually. Researchers comparing issues at the national level have used data from such sources in their studies (e.g. Shih et al., 2005; Bagchi et al., 2006; Ifinedo, 2009a).

Table 2 shows data for the three contextual factors for each of the countries used in this study. From the World Economic Forum (2009), the data for "ICT use laws" for each country listed in Table 2 is obtained. This variable was assessed with scores ranging from "1" = nonexistent to "7" = well developed and enforced. The same source provided data for "Legal framework efficiency", which was assessed with scores ranging from "1" = is inefficient and subject to manipulation to "7" = is efficient. Transparency International's (2009) website offered data on corruption indices for each country. The scores ranged from "10" (highly uncorrupt) to "0" (highly corrupt).

As noted, this study obtained a list of all 31 countries in the 2009 DTT security survey from DTT researchers. Although a larger sample of countries would ideally be suitable for robust analysis; the sample of 31 countries is sufficient for a preliminary study such as this one; in fact, other researchers (e.g. Bagchi et al., 2006) have used limited samples of countries to investigate comparable themes.

Table 2. The study's contextual variables

Region	Country	Efficiency of Legal Systems	The Quality of ICT Use Laws	Transparency and Corruption Index
	Australia	5.73	5.45	8.7
	India	4.44	4.58	3.4

AP	Indonesia	3.57	3.75	2.6
	Malaysia	5.19	5.31	5.1
	China	3.95	4.24	3.6
JP	Japan	5.34	4.82	7.3
EM	Austria	5.94	5.79	8.1
	Luxembourg	5.48	5.14	8.3
	Egypt	3.92	3.86	2.8
	France	5.46	5.44	6.9
	Germany	6.01	5.51	7.9
	Ireland	5.18	5.02	7.7
	Israel	4.13	4.83	6.0
	Italy	2.80	4.16	4.8
	Netherlands	5.73	5.29	8.9
	Poland	2.89	3.37	4.6
	Saudi Arabia	4.46	4.31	3.5
	South Africa	5.22	4.8	4.9
	Spain	4.39	4.76	6.5
	Sweden	5.95	5.9	9.3
	Switzerland	6.04	5.59	9.0
	Turkey	3.28	4.03	4.6
	United Kingdom	5.34	5.35	7.7
NA	United States	4.91	5.63	7.3
	Canada	5.65	5.5	8.7
LC	Peru	2.79	3.43	3.6
	Mexico	2.88	3.81	3.6
	Chile	4.79	5.02	6.9
	Colombia	3.72	4.09	3.8
	Costa Rica	4.19	3.83	5.1
	Argentina	2.26	2.88	2.9

As this study is exploratory in nature, its analysis of data obtained from multiple sources does not pose a serious problem. The use of the multiple-sourced data for correlation analysis serves the study's objective in two main ways: a) it permits possible associations between selected variables to be empirically examined; b) the results from this present endeavor are intended to inform subsequent inquiries in the area. Of note is the fact that comparable studies have also used data from multiple sources to assess relationships between data obtained at the national level (see e.g. Oxley and Yeung, 2001; Shih et al., 2005; Bagchi et al., 2006; Kovačić, 2005; Azad et al., 2010).

It is worth noting that the security concerns in the financial services industry reported in the 2009 DTT survey compared reasonably well with those published by other

consultants for the industry (see e.g. PricewaterhouseCoopers, 2008). To some extent, it can be argued that the validity of the study's main data is assured. SPSS 18.0 was used for data analysis. Person's correlation analysis was used to assess the strength of the relationships between the study's variables and Regression analysis was used to identify variables with greater relevance in a model containing all the variables.

DATA ANALYSIS AND RESULTS

The study's findings are presented as follows: the data analysis showed that nineteen (19) correlations yielded statistically significant results. There are 39 (13 X 3) possible relationships in the correlation matrix. The correlation results are highlighted in Table 3. It is easy to notice that about a half of the relationships yielded statistically significant results (the numbers in bold fonts are the ones with statistically significance results). Each of the significant relationships will be discussed in the next section.

Table 3. Correlations between information security concerns and the contextual factors

	Security Concern	Legal Systems Efficiency	Transparency and Corruption Index	ICT Use Laws
#1	Respondents who feel that security has risen to executive management and/or board as a key imperative	**-.377(*)**	**-.470(**)**	**-.456(**)**
#2	Respondents who feel they have commitment and funding to address regulatory requirement	-.256	**-.393(*)**	-.301
#3	Respondents who indicated that they had a defined and formally documented information security strategy	**-.372(*)**	-.252	-.279
#4	Respondents who feel that information security and business initiatives are appropriately aligned	**-.502(**)**	**-.386(*)**	**-.479(**)**
#5	Respondents who indicated that their information security budget has increased	**-.392(*)**	-.216	-.271
#6	Respondents who indicated that their expenditures and information security were 'on plan' or 'ahead of requirements' based on the organization's current needs	-.274	-.154	-.225
#7	Respondents who incorporated application security and privacy as part of their software development cycle	**-.402(*)**	**-.408(*)**	**-.408(*)**
#8	Respondents who feel they presently have both the required competencies to handle existing and foreseeable security requirements	.171	.300	.209
#9	Respondents whose employees have	-.256	-.044	-.204

	required at least one training and awareness session on security and privacy in the last 12 months			
#10	Respondents who have an executive responsible for privacy	**.438(*)**	**.527(**)**	**.453(*)**
#11	Respondents who have a program for managing privacy compliance	**.453(*)**	**.450(*)**	**.446(*)**
#12	Respondents who have experienced repeated internal breaches over the last 12 months	-.325	**-.417(*)**	-.288
#13	Respondents who have experienced repeated external breaches over the last 12 months	-.150	-.226	-.082

** Correlation is significant at the 0.01 level (2-tailed).
* Correlation is significant at the 0.05 level (2-tailed).

DISCUSSIONS AND CONCLUSION

The objective of this study was to examine whether new insights can emerge from the 2009 DTT security survey for GFSI. It was noted that the DTT researchers implied that security concerns in GFSI across countries are essentially comparable; yet, the extant literature suggests that the acceptance of innovations and attitudes related to security issues vary according to contextual influences. To enhance understanding in this area, this current study posited that there are correlations between selected contextual factors and GFSI employees' perceptions of information security concerns. Next, this study's significant results will be discussed.

Correlates of Information Security Concerns and National Legal Systems Efficiency

With regard to the correlations between the legal systems efficiency variable and information security concerns, the data analysis showed that 7 items out of the 13 concerns had significant statistical relationships. The insights gained from these results are discussed as follows: The significant negative relationship between the item of "Respondents who feel that security has risen to executive management and/or board as a key imperative" and legal systems efficiency seems to suggest that GFSI in countries with relatively poorer legal environments believe that IS security threats can be better contained by alerting the attention of executive management to such concerns. Furthermore, the data seems to be indicating that the views of GFSI employees from countries with more robust legal environments may have different or lesser perceptions of this particular security concern.

The results also showed significant negative relationships between "Legal systems efficiency" and the security concerns labeled as follows: #3, #4, #5, and #7 in Tables 1 and 3. A similar interpretation, much like what was given for the first item, is offered as well. That is, the perceptions toward non-malicious insider threats such as the

availability of formally documented information security strategies, the increment of funding for information security, the proper alignment of information security and business initiatives, and the application security and privacy policies as part of software development process, tend to be higher among GFSI employees from countries with relatively poorer legal frameworks. Although, this current study is not designed to provide answers as to why the observed patterns have been noticed; it is nonetheless relevant to make the following suggestions: It is possible that weaknesses and inadequacies in the legal and regulatory apparatuses of countries with less efficient legal systems have caused GFSI employees from such countries, to accord higher importance to the foregoing non-malicious insider threats (please refer to some of the examples provided above). Moreover, the degree of protection gained in trying moments may be lower in comparison to what counterparts from countries with relatively strong legal system will get. It might be the case that countries with better legal infrastructure have built-in mechanisms to address emerging security threats; as such, their perception levels of such concerns may not be as high as those from countries lacking such favorable infrastructure.

Furthermore, the results indicated significant positive relationships between the variable of legal systems efficiency and two items labeled #10 and #11 in the tables. Namely, GFSI respondents who have an executive responsible for privacy issues and global financial services firms that have programs for managing privacy compliance were more prevalent in countries with more efficient legal systems. This particular insight seems to contradict a previously discussed issue related to the association between the legal systems efficiency variable and security concerns awareness at the board level. Regardless, the data is suggesting that GFSI in countries with more efficient legal frameworks tend to have programs for managing privacy compliance and also appoint executives to oversee such issues. GFSI in countries with less efficient legal frameworks tend have a differing view in this aspect.

Correlates of Information Security Concerns and Transparency Levels

With respect to transparency levels across countries, this current study's results found that 5 items out of the 13 security concerns yielded significant negative relationships. Specifically, for items labeled #1, #2, #4, #7, and #12 in the tables, it was found that the perceptions of, and attitudes toward security concerns of GFSI employees in more transparent countries were lower in comparison to those of counterparts from more corrupt parts of the world. This result is inconsistent with logical rationale. It would seem reasonable to expect that more respondents in countries with more corrupt tendencies would assess highly the need to elevate security concerns to senior hierarchies in the organization, align business with information security issues, commit more resources to security issues, and report more internal breaches in their setups. It is believed that individuals with corrupt tendencies should perceive the elevation of security to higher levels in the organization as a threat to their behaviors.

Along the same line of reasoning, the alignment of business initiatives with information security issues should serve to deter unacceptable practices and behaviors (e.g. Willison and Siponen, 2009). Likewise, the reporting of internal breaches is a control mechanism. As the results on these items are inconsistent with our predictions; it is plausible that the design of this current study, with its limitations, might have impacted the analysis in this aspect. More work is expected in this area.

Consistent with rationale, it was observed that there were positive relationships between transparency levels and items labeled #10 and #11 in the tables. This result can be interpreted to mean that the need for programs to manage privacy and security compliance issues and the appointment of executives to oversee such programs is higher among GFSI employees in countries with more openness, honesty, and fairness. Conversely, counterparts in less transparent societies may be indicating that that there is less need for such programs and control to be instituted or supported in their setups. This would seem logical as people with deviant behaviors develop resistance to change and order (Cohn et al., 2010). Mechanisms and measures for controlling non-malicious insider threats represent a change; as such, programs, procedures, and guidelines for managing security policies in GFSI would readily be acceptable to more transparent employees than those lacking in such qualities.

Correlates of Information Security Concerns and ICT Use Laws

Regarding the link between ICT use laws and information security concerns, the data revealed 3 negative significant relationships. Namely, "respondents who felt that security issues had risen to executive management and/or board level in their organizations" (#1) were more common in countries with relatively poorer ICT use laws. Also, "Respondents who believed their information security and business initiatives were appropriately aligned" (#4) appeared to occur more in countries with relatively poorer ICT use laws. As well, "Respondents who incorporated application security and privacy as part of their software development cycle" (#7) tended to be from countries with relatively poorer ICT use laws. Taken together, the data permits the suggestion that where laws related to the use of IS and related technologies are weaker, GFSI employees in such countries seem to have more need to increase the visibility of security issues within their organizations, forge a close link between their business initiatives and IS security threats, and tend to align security and privacy issues with the development of their IS software in their setups. On the other hand, the perceptions of GFSI employees in countries with stronger ICT use laws were different; it is likely that the depth of their ICT use laws might have influenced their assessment of these issues.

The data analysis showed significant positive relationships between ICT use laws and items labeled #10 and #11 in the tables. Countries with better ICT use laws may have stipulations and guidelines regarding how certain security concerns are treated in their

environments. For example, such laws could instruct that all publicly-quoted GFSI firms have clearly spelled out privacy compliance statements or appoint a functionary to oversee privacy matters. A widely known act in the United States, the Sarbanes-Oxley (SOX) is an apotheosis linking privacy disclosure and ICT use for businesses that are publicly quoted on the stock exchanges. Thus, it can be argued that such stipulations and regulatory oversights might have caused GFSI employees from parts of the world with such quality ICT use laws to assess items #10 and #11 different from counterparts from where such laws are poorly developed.

Additional Insight from Regression Analysis

To gain further insight and to improve the study's rigor, a regression analysis was performed. To that end, items that yielded significant relationships between the information security concerns and the three contextual factors were considered for inclusion in the regression analysis. For example, items #1, #3, #4, #5, #7, #10, and#11 in Table 3 were regressed on the legal systems efficiency variable; a similar exercise was performed for the other two variables. The results of the analysis are provided in the Appendix.

The regression results showed that only item #4 (Respondents who feel that information security and business initiatives are appropriately aligned) caused significant variations for the regression models with legal systems efficiency and ICT use laws to suggest that this particular item has greater relevance than the other items that yielded significant correlation results. Likewise, item #10 (Respondents who have an executive responsible for privacy) produced a similar insight for the analysis with the transparency level variable. That is, only item #10 caused significant variation in the model involving the transparency level variable. These foregoing results indirectly support the viewpoint suggesting that success with the management of security concerns in organizations may depend on having on board knowledgeable individuals who are able to align security issues with business initiatives in their organizations (e.g. Whitten, 2008).

Limitations of the Study and Future Research Avenues

There are obvious limitations in this research. This preliminary study used data from secondary sources. As a consequence, it inherits all limitations from the DTT survey as well those from the two other sources used. It is difficult to ascertain with certainty the reliability and validity of items used in composing the various measures. For example, the omission of relevant demographic information in the DTT survey is limiting. Data analysis might have been more robust, had the DTT data been presented on the Likert scale rather than in percentages. Further to this, the diversity of GFSI used in the DTT survey might also be problematic. It is possible that opinions in the banking sector may be different from those in insurance or asset management.

It is worth noting that an attempt was made to perform a longitudinal analysis with the data that has been accumulated over the years in the DTT surveys. This, however, was impossible because the DTT security survey data had changing information security concerns over the years (see DTT-Global Security Survey, 2005; 2009). However, this reality is consistent with rationale as IS security concerns in organizations never remain static (Kritzinger and Smith; 2008; Schatz, 2008). As such, this research had to use cross-sectional data i.e. the 2009 data to fulfill its stated objective. As was mentioned above, respondents in the DTT surveys were management teams; the views of end users were not considered. It is accepted that both groups' views on IS-related issues differ considerably (e.g. Ifinedo and Nahar, 2006). Thus, it is difficult to say with certainty that the findings in the DTT study can be generalized across all work groups.

In addition, more useful insights would emerge if national summaries were used instead of regional aggregates. Additionally, a larger sample of countries (more than 31) might also permit deeper insights. Although this study's preliminary findings provided initial insights into the discourse, it is however advised that its interpretations be applied with caution. Nonetheless, this present effort has opened up future areas of inquiry.

Future studies should employ the longitudinal study approach to understand the dynamic nature of information security issues in GFSI and in comparable organizations. Future research endeavors should attempt to collect data from a single source; the use of data from multiple sources may have its shortcomings. Future research may consider using the Likert scale to facilitate research replication. The views of end users and/or mid-level managers on information security concerns in GFSI should be considered in future research to enhance insight. Studies could be designed to elaborate on some of the findings in this study; such studies could combine both quantitative and qualitative methodologies to deepen our knowledge. It is worthwhile to further investigate the information produced by the study's data noting that the "security" perceptions of GFSI employees from countries with poorer ICT use laws tend to be higher than those of counterparts in countries with relatively better ICT use laws. It is pertinent to enhance understanding in this area given that "privacy" issues (i.e. #10 and #11), in this study's analysis, indicated positive correlations with the relevant contextual factors.

Furthermore, other similar studies could consider applying some of the aforementioned IS security assessment frameworks proposed by Kritzinger and Smith (2008), Chao et al. (2006), and Sumner (2009) to the financial services industry to further enhance understanding in the area. The impacts of other contextual factors such as educational standards, national economic wealth, organizational managerial practices and individual attitudes toward security compliance could also be

investigated. Research efforts in the future may want to know whether national cultural values impact how IS security concerns in GFSI are assessed or prioritized.

Research Contributions and Managerial Implications

This preliminary study offers implications for both research and practice. This research is an interesting read for practitioners who are alerted to the associations between selected contextual influences and the perceptions of non-malicious insider threats (i.e. security concerns) in the financial services industry. GFSI managers stand to benefit from understanding the relevance of contextual influences in the assessment of security concerns in their industry. Such a perspective may offer a layer of insight to deepen industry-related perceptions and views.
In the context of this study's data, no meaningful results were found for four items (i.e., #6, #8, #9, and #13) across the three contextual factors. This would imply that perceptions of, and attitudes of GFSI employees toward those particular items compared reasonably well across the board. Areas in which significant correlation exist across the board have been highlighted and discussed. However, more studies are required to enhance knowledge as to why the differences have surfaced.

The positive associations found regarding how GFSI employees around the world view information security concerns lead to the suggestion that it may be misleading to accept that that GFSI (and their employees) comply exactly with the same standards and practices, or even hold exactly the same view on information security concerns in their industry. It is incumbent upon practitioners to take note of such information in their decision making processes. Information from this exploratory study may serve them well as they promote IS security policies and practices in their global operations. That is, insights gained from this endeavor could serve to improve the management of global IS security issues and concerns. An understanding that contextual factors matter could be used to an advantage in managing security threats, risk, and vulnerabilities in their settings. Globally, GFSI practitioners need to be cognizant of the importance of two concerns in their industry vis-à-vis the three contextual factors considered in this study. Greater importance should be given to the issue of how information security and business initiatives are appropriately aligned in their industry. The data also indicated that the responsibility of who oversees privacy issues in GFSI is deserving of attention.

As per implications for research, this present effort is among the few studies to discuss non-malicious insider threats vis-à-vis contextual influences in financial services organizations. This current effort, to some extent, reinforces observations in studies suggesting that more insights can be gained from endeavors linking IS security issues with relevant contextual influences. In that regard, this study complements and advances emerging works focusing on security assessment in organizations. It adds to the limited body of research examining information security concerns in relation to

contextual influences (Milberg et al., 1995; 2005; Chen et al., 2008). It has responded to calls in the literature for IS security researchers to adequately focus on the financial services industry. More importantly, this endeavor enhances the information provided in the 2009 DTT survey, to the degree that more light is shed on the findings reported in that survey.

A major contribution of this research is that it notes that it would be erroneous to accept that entities in GFIS hold exactly the same view on information security issues in their industry. On the basis of this study's results, it is difficult to posit that future efforts will undermine the importance of contextual factors in the assessment of security concerns, in general. Rather, future research may be enticed to further explore insights and information provided in this paper. In that regard, preliminary insight presented in this study could provide useful input or serve as a foundation for future investigations in the area. It is not suggested that the findings presented herein represent the final word in this area – more studies are expected.

REFERENCES

Alexander, K., Dhumale, R., & Eatwell, J. (2004). Global governance of financial systems. The international regulation of systemic risk. New York: Oxford University Press Inc, USA.

Azad, B., Faraj, S., & Goh J. F. (2010). What Shapes Global Diffusion of e-Government: Comparing the Influence of National Governance Institutions. Journal of Global Information Management, 18(2), 85-104.

Bagchi, K., Kirs, P., & Cerveny, R. (2006). Global software piracy: Can economic factors alone explain the trend? Communications of the ACM, 49(6), 70-75.

Bertort, J. C., Jaeger, J. T, & Grimes, J. M. (2001). Using ICTs to create a culture of transparency: E-government and social media as openness and anti-corruption tools for societies. Government Information Quarterly, 27, 264-271.

Bia, M., & Kalika, M. (2007). Adopting an ICT code of conduct: an empirical study of organizational factors. Journal of Enterprise Information Management, 20(4), 432-446.

Chang, A., J-T., & Yeh, Q-J. (2006). On security preparations against possible IS threats across industries. Information Management & Computer Security, 14(4), 343-360.

Chao, S-C., Chen, K., & Lin, C-H. (2006). Capturing industry experience for an effective information security assessment. International Journal of Information Systems and Change Management, 1(4), 421- 438.

Chen, C. C., Medlin, B. D., & Shaw, R. S. (2008). A cross-cultural investigation of situational information security awareness programs. Information Management & Computer Security, 16(4), 360-376.

Chaturvedi, M., Gupta, M. Mehta, S., & Valeri, L. (2000). Fighting the wily hacker: modeling information security issues for online financial institutions using the SEAS environment. In Leite Gouvêa (Ed.), Proceedings of Internet Society (INET 2000), 18-21 July, 2000, Yokohama, Japan. Retrieved Jan. 14, 2009 from: http://www.isoc.org/inet2000/cdproceedings/7a/7a_4.htm.

Chung, W., Chen, H. Chang, W., & Chou, S. (2006). Fighting cybercrime: A review and Taiwanese experience. Decision Support Systems, 41(3), 669-682.
Cohn, E. S, Bucolo, D., Rebellon, C. J., & Van Gundy, K. (2010). An integrated model of legal and moral reasoning and rule-violating behavior: The role of legal attitudes. Law and Human Behavior, 34(4), 295-309.

DTT-Global Security Survey (2005). The Global Security Survey, 2004, Deloitte Touche Tohmatsu (DTT). Retrieved Jan 14, 2009 from: http://www.deloitte.com/assets/Dcom-Argentina/Local%20Assets/Documents/global_security.pdf

DTT-Global Security Survey (2008). The Global Security Survey, 2007, Deloitte Touche Tohmatsu (DTT). Retrieved January 14, 2009 from: http://www.deloitte.com/assets/Dcom-Shared%20Assets/Documents/dtt_gfsi_GlobalSecuritySurvey_20070901.pdf

DTT-Global Security Survey (2009). The Global Security Survey, 2008, Deloitte Touche Tohmatsu (DTT). Retrieved June 20 from: https://www.deloitte.com/assets/Dcom-Serbia/Local%20Assets/Documents/rs_gfsi_globalsecuritysurvey_0901%282%29.pdf

EDS (2007). Eight Financial Services Security Concerns. Retrieved May 10, 2008 from: Http://www.eds.com/news/features/3620/. 2007.

Goodhue, D. L., & Straub, D. W. (1991). Security concerns of system users: a study of the perceptions of the adequacy of security, Information and Management, 20(1), 13-22.

Gust, C., & Marquez, J. (2004). International comparisons of productivity growth: the role of information technologies and regulatory practices. Labour Economics, 11(1), 33-38.

Ifinedo, P., & Nahar, N. (2006). Do top and mid-level managers view enterprise resource planning (ERP) systems success measures differently? International Journal of Management and Enterprise Development, 3(6), 6, 618-635.

Ifinedo (2009a). Information technology security concerns in global financial services institutions: Do socio-economic factors differentiate perceptions? International Journal of Information Security and Privacy, 3(2), 68-83.

Ifinedo (2009b). Information technology security management concerns in global financial services institutions: Is national culture a differentiator? Information Management & Computer Security, 17(5), 372-387.

infoLock Technologies (2006). Insider threat management. Retrieved Oct. 8, 2009 from: www.infolocktech.com/download/ITM_Whitepaper.pdf.

Information Security Industry Survey (1999). Information security magazine. Retrieved Jan 14, 2008 from: http://www.infosecuritymag.com/, July 1999.

ISACA (2006). Information Systems Audit and Control Association Manual, 2006 edition. Rolling Meadows, IL. ISACA Press

ISO/TR 13569 (2005). Financial services - Information Security Guidelines. http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=3724.

Johnson, H. J. (2000). Global financial institutions and markets. New York: Blackwell Publishing.

Jung, B., Han, I. and Lee, S. (2001). Security threats to Internet: A Korean multi-industry investigation. Information and Management, 38(8), 487-498.

Hoesing M. T. (2009). Virtualization security assessment. Information Security Journal: A Global Perspective, 18(3), 124-130.

Kankanhalli, A., Teo, H. H., Tan, B. C. Y., & Wei, K-K. (2003). An integrative study of information systems security effectiveness. International Journal of Information Management, 23(2), 139-154.

Kovačić, Z. (2005). A brave new eWorld? An exploratory analysis of worldwide eGovernment readiness, level of democracy, corruption and globalization. International Journal of Electronic Government Research, 1(3), 15-32.

Kritzinger, E., & Smith, E. (2008). Information security management: An information security retrieval and awareness model for industry. Computers & Security, 27(5-6), 224-231.

Milberg, S., Burke, S., Smith, H. J., & Kallman, E. A. (1995). Values, personal information privacy, and regulatory approaches. Communications of the ACM, 38(13), 65-74.

Milberg, S., Smith, H. J., & Burke, S. (2000). Information privacy: corporate management and national regulation. Organization Science, 11(1), 35-57.

Moshirian, F. (2007). Financial services and a global single currency. Journal of Banking and Finance, 31(1), 3-9.

Oxley, J. E., & Yeung, B. (2001). E-commerce readiness: institutional environment and international competitiveness. Journal of International Business Studies, 32(4), 705-723.

Pontus, E. and Erik, J. (2008). Assessment of business process information security. International Journal of Business Process Integration and Management, 3(2), 118-130.

PricewaterhouseCoopers (2008). The Global State of Information Security Survey 2008
http://www.pwc.com/extweb/home.nsf/docid/c1cd6cc69c2676d4852574da00785949

Rezgui, Y., & Marks, A. (2008). Information security awareness in higher education: An exploratory study. Computer & Security, 27(7-8), 241-253.

Reinhold, C., Frolick, M. N., & Okunoye, A. (2009). Managing your security future. Information Security Journal: A Global Perspective, 18(3), 116-123.

Schatz, D. (2008). Setting priorities in your security program, In H. F. Tipton and K. Krause (Eds), Information Security Management Handbook. Boca Raton, FL.: Taylor & Francis Group.

Shih, C-F, Dedrick, J., & Kraemer, K. L. (2005). Rule of law and the international diffusion of E-commerce. Communications of the ACM, 48(11), 57-62.

Sumner, M. (2009). Information security threats: A comparative analysis of impact, probability, and preparedness. Information Systems Management, 26(1), 2-12.

Theoharidoua, M., Kokolakisb, S., Karydaa, M., & Kiountouzisa, E. (2005). The insider threat to information systems and the effectiveness of ISO17799. Computers & Security, 24(6), 472-484

Transparency International (2009). Corruption Perception Index – 2008. Retrieved Jun 20, 2009 from: http://www.transparency.org/.

Walker, T. (2008). Practical management of malicious insider threat – An enterprise CSIRT perspective. Information Security Technical Report, 13(4), 225-234.

Whitten, D (2008). The chief information security officer: An analysis of the skills required for success. Journal of Computer Information Systems, 48(3), 15-19

Willison, R. and Siponen, M. (2009). Overcoming the insider: Reducing employee computer crime through situational crime prevention. Communications of the ACM, 52(9), 133-137.

World Economic Forum (2009). Global competitiveness for 2007-2008. http://www.weforum.org.

Appendix

A) Results of the analysis with the Legal systems efficiency

R	R Square	Adjusted R Square	Std. Error of the Estimate
.502[a]	.252	.226	1.04553

a. Predictors: (Constant), a4 (item #4)

ANOVA[b]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	10.685	1	10.685	9.775	.004[a]
	Residual	31.701	29	1.093		
	Total	42.386	30			

a. Predictors: (Constant), item #4; b. Dependent Variable: Legal systems efficiency

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	
		B	Std. Error	Beta	t
1	(Constant)	10.176	1.761		5.779
	#4	-.166	.053	-.502	-3.127

a. Dependent Variable: Legal systems efficiency

B) Results of the analysis with the Transparency levels

R	R Square	Adjusted R Square	Std. Error of the Estimate
.527[a]	.278	.253	1.87901

a. Predictors: (Constant), item #10

ANOVA[b]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	39.444	1	39.444	11.172	.002[a]
	Residual	102.389	29	3.531		
	Total	141.834	30			

a. Predictors: (Constant), a10 (item #10); b. Dependent Variable: Transparency levels

Coefficients[a]

Model	Unstandardized Coefficients	Standardized Coefficients	t	Sig.

		B	Std. Error	Beta		
1	(Constant)	3.171	.894		3.547	.001
	a10	.057	.017	.527	3.342	.002

a. Dependent Variable: Transparency levels

C) Results of the analysis with the ICT use laws

R	R Square	Adjusted R Square	Std. Error of the Estimate
.479[a]	.230	.203	.75575

a. Predictors: (Constant), a4 (item #4)

ANOVA[b]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	4.936	1	4.936	8.642	.006[a]
	Residual	16.564	29	.571		
	Total	21.500	30			

a. Predictors: (Constant), a4 (item # 4); b. Dependent Variable: *ICT use laws*

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	8.370	1.273		6.576	.000
	a4	-.113	.038	-.479	-2.940	.006

a. Dependent Variable: *ICT use laws*

Princely Ifinedo is an Associate Professor at Cape Breton University, Canada. He earned his PhD in Information Systems Science from the University of Jyväskylä, Finland. He obtained an MBA in International Management from Royal Holloway, University of London, UK. His current research interests include IS security and privacy management issues, Global IT management, ERP system success measurement, and IT adoption in SME and Healthcare. His papers have appeared in such journals as *Computers in Human Behavior, Journal of Computer Information Systems, Information Management & Computer Security, Enterprise Information Systems, International Journal of Information Security and Privacy, Journal of Global*

Information Technology Management, and *Journal of Organizational Computing and Electronic Commerce*. He has authored (and co-authored) about 70 peer-reviewed papers, and he is affiliated with AIS and ISACA.