Journal of Computing and Information Technology - CIT 21, 2013, 4, 235–246
doi:10.2498/cit.1002237

Relationships Between Relevant Contextual Influences and Information Security Threats and Controls in Global Financial Services Industry

Princely Ifinedo

Shannon School of Business, Cape Breton University, Sydney, Nova Scotia, Canada

Businesses operating in the Global Financial Services Industry (GFSI) know the importance of protecting information assets from ever-growing security threats and risks. This paper aims at shedding light on the relationships between four relevant contextual factors i.e. national legal infrastructure, transparency levels, ethical behavior of firms, and capacity for innovation, on the one hand, and information security threats and controls, on the other. To some extent, this study enriches the information provided in the 2012 Deloitte Touche Tohmatsu Limited (DTTL) survey. This study's findings indicated that contextual factors such as national transparency levels and ethical behavior of firms do have positive associations with, and effects on some information security threats and controls. Information provided in this study is beneficial to both practitioners and academicians.

Keywords: global financial services industry, information security threats and controls, national legal infrastructure, transparency levels, ethical behavior of firms, capacity for innovation

1. Introduction

Firms operating in the Global Financial Services Industry (GFSI) are faced with ever-growing information security threats, risks, and vulnerabilities [1]. Examples of GFSI include firms from a variety of sectors such as banking, insurance, tax consultancy, and asset management. The primary function of a GFSI is to act as an agent for its clients and customers [2], and to ensure that their information assets are protected. Chang and Yeh [3] 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, the Deloitte Touche Tohmatsu Limited (DTTL) survey [1] concluded that "[w]ith increasing business demands and evolving regulatory frameworks [in GFSI], information security is a top priority for financial services industry (FSI) organizations." As a consequence, GFSI operatives must make constant efforts to protect customer data and effectively manage any emerging threats [4].

Schatz [5, p. 94] commented 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." Hence, corporate managers, including those in the financial services industry, are advised 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 [5], [6]. Threats in the financial services industry can manifest in several forms such as the introduction of malwares, industrial espionage, cyber crimes, and so forth. Suffice it to note that such threats can undermine the functioning and public standing of a business organization, if not properly managed [4]. Realizing the need to focus on information security threats and gain an understanding of such industry concerns, GFSI practitioners have themselves started investigating and reporting such issues. A series of surveys conducted by DTTL

in this regard [1], [7-9] is noteworthy. The first survey was published in 2003 and others have followed since. These surveys educated practitioners about information security threats; comparative insights across regions of the world are also provided. Key findings in the latest survey for 2012 are available online [1].

Although the findings in the 2012 DTTL survey show noticeable differences across selected regions of the world, with respect to the assessment of information security threats and controls across GFSI, inference from past reports by the company has suggested that the perceptions of and attitudes toward information security concerns across GFSI are being informed by industry-related standards or imperatives. This supposition seems to suggest that contextual factors may mean very little in such assessment. Were this viewpoint accepted as the only truth, empirical studies would not have suggested that countries and even blocs of nations differ in the way they relate to information security management issues [10], [11-14].

This study is designed to examine the potential relationships between contextual factors such as national transparency levels, legal infrastructure, ethical behavior of firms, capacity for innovation, on the one hand, and information security threats and controls, on the other. Prior research has underscored the pertinence of contextual factor in the assessment of information security issues in organizations [10], [11], [13]. For example, Ifinedo [4] showed that socioeconomic factors are particularly relevant in the discourse of information systems (IS) security concerns in GFSI. Very few have provided information about the relevance of the aforementioned contextual factors considered in this study. Admittedly, there are other relevant contextual factors such as national culture that could be considered; the aforementioned factors were chosen for illustration purposes.

The objective of this study is twofold. First, it seeks to increase the depth of information provided in the 2012 DTTL survey as it examines the relationships between the aforementioned contextual factors and six (6) information security threats and controls in the report. Second, it complements and adds to the growing body of work specifically discussing information security concerns in GFSI [4], [14]. In particular, this study aims at providing answer to the following questions: What relationships exist between the selected contextual factors and information security threats and controls across GFSI? Which information security threats and controls should GFSI practitioners pay more attention to?

2. Background Information

2.1. Definitions and overview

GFSI practitioners realize that securing the future of their organizations is linked to how well emerging challenges are understood and subsequently contained [7-9], [14]. It is almost impossible to come out with a perfect security plan to mitigate every threat confronting an organization. Interestingly, savvy corporate managers constantly assess their environments and adjust their security programs and policies accordingly [4]. A series of surveys on information security threats and controls produced by DTTL is done with that understanding. The summarized results provided by DTTL contain information regarding security threats and controls.

Drawing from definitions provided in ENISA [15] and ISO 27005 [16], information security threats refer to circumstances or events with a potential to cause harm to an organization's IS resources. Similarly, descriptions provided in ISO/IEC 27001:2013 [17], refer to information security controls as countermeasures or measures employed to avoid, counteract or minimize security risks to an organization's IS resources.

Frameworks provided by ISO 27005 [16] and OWASP [18] conceptualize connections between threats, controls, and business impact; these frameworks have been modified in Figure 1 to depict the linkages between threat agents and business impact in GFSI. Namely, threat agents (i.e. crackers, criminal organizations) through an attack vector (i.e. phishing, malware attack, sabotage) exploit vulnerabilities or weaknesses of IS resources (i.e. lack of antivirus software, firewall) and related security controls (i.e. lack of security awareness and training, poor access control) to cause technical impacts (i.e.

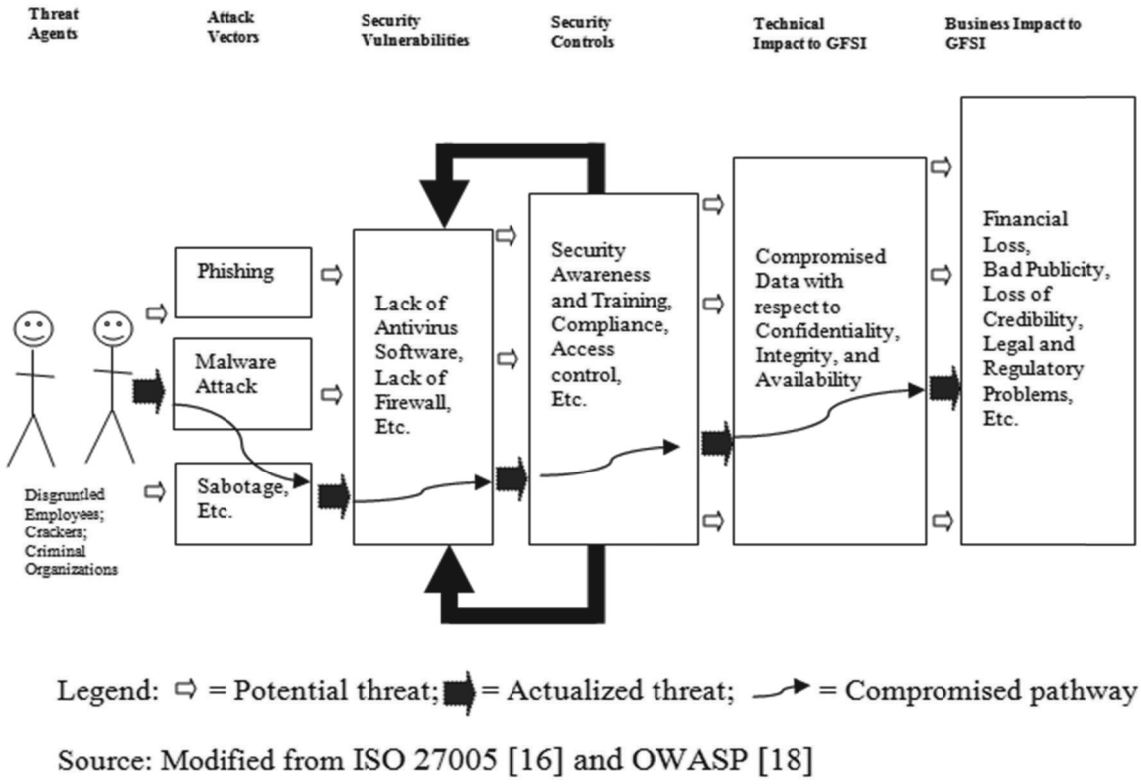

Figure 1. Connections between threat agents to business impact in GFSI.

compromised confidentiality, integrity or availability (CIA) issues) to an organization's IS resources, which result in huge negative impacts for GFSI (i.e. financial loss, bad publicity, loss of credibility, legal, and regulatory problems). Usually, organizations deploy security controls to counter weaknesses in their contexts; hence, the reverse arrows in Figure 1 (please see [17] and [18] for details).

2.2. Background theory

This study draws from the contingency theory, which was developed by Lawrence and Lorsch [19]. The theory posits that favorable outcomes can result from matching relevant contingency factors with dependent phenomena i.e. organizational effectiveness and related issues. With regard to this study, the favorable, effective or quality assessment of information security threats and controls by GFSI respondents can be linked to contextual factors considered herein. In brief, favorable assessment of information security threats and controls is positively linked to the assessor's contextual influences.

3. The 2012 Deloitte Touche Tohmatsu Limited (DTTL) Survey and Findings

Deloitte Touche Tohmatsu Limited (DTTL) is an international firm that provides audit, tax, consulting, and financial advisory services to both public and private clients. DTTL has a global network of member firms in about 140 countries. Participants in the 2012 DTTL study came from about 40 countries and almost all regions of the world, i.e. Asia Pacific (APAC) excluding Japan (JP), Europe, the Middle East and Africa (EMEA), Latin America and the Caribbean Region (LACRO), Canada, and the United States (US). DTTL researchers excluded Japan from the Asia Pacific region's data set to suggest that Japan's perceptions of the issues are significantly different from other regional counterparts.

The unit of analysis used in the DTTL survey was the organizational level of each institution. To that end, responses from chief information security officers, chief security officers and other senior security and privacy professionals

within the Deloitte member firm network were used. They were asked to give perceptions representative of their organizations' views or standing on the issues being investigated. The 2012 DTTL report [1] notes:

The questionnaire comprised questions composed by the global study team made up of senior Deloitte member firm Security & Privacy Services professionals. Questions were selected based on their potential to reflect the most important operating dimensions of a consumer business organization's processes or systems in relation to security and privacy. The questions were each tested against global suitability, timeliness, and degree of value. The purpose of the questions was to identify, record, and present the state of information security and privacy in the industry.

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 DDTL survey is not available online; however, DTTL researchers obliged this current study with a list of all countries examined in the 2012 survey. The countries/regions sampled in this study are diverse. The regions' summarized data is shown in Table 1.

Findings from the DTTL report also included the highlights provided below (bulleted points); however, the information does not provide an indication of influences arising from external contexts. This study seeks to make a contribution in that aspect.

- With the exception of Canada and Japan, more than 50% of respondents in each region report an increase in the information security budget
- Despite the economic downturn and corporate budget cuts, the majority of regions believe that their information security expenditure is on or above plan
- Identity and access management is the top security initiative in Canada and United Kingdom. IS governance is the top security initiative for Japan and APAC region
- When it comes to the adoption of new technology, United States and United Kingdom respondents have the highest number of organizations that implemented cloud computing services
- United Kingdom and United States respondents have experienced more privacy-related breaches in the past year than other regions

4. Selected Contextual Factors

The literature suggests that factors such as national transparency levels, legal, ethical behavior of firms, and innovative infrastructure could influence the responses, values, and attitudes of GFSI workers with regard to how they perceive new practices and guidelines, including those related to information security concerns [20-26].

No.	Threats and Controls	AP	JP	EM	LA	UK	US	CA
#1	Respondents who believe there is an increase in their information security budget	73	14	55	62	56	94	46
#2	Respondents who believe their information security expenditure is on or above plan	50	27	50	50	44	50	31
#3	Respondents who believe identity access management is the top security initiative	18	9	38	18	44	33	46
#4	Respondents who believe IS governance as the top security initiative	36	36	31	29	11	11	8
#5	Respondents that implemented or purchased cloud computing services	50	41	54	30	89	89	62
#6	Respondents who experienced privacy-related breaches in the past year	32	23	26	21	67	50	23

Note: Entries are expressed in percentages

Table 1. Summary of information security threats and controls in GFSI across regions.

National transparency levels refer to the extent to which honesty and fairness prevail in a country [27]. Transparency is critically important to businesses in the financial sector as it helps to reinforce trust and accountability in the industry [28-30]. Ethical behavior of firms refers to the standards that firms hold with respect to honesty, responsibility, and treatment of others in their dealings [31]. This factor is essential for organizations including GFSI [32], [33]. Legal infrastructure refers to the degree to which rules and regulations in a country are defined, enforced, and above all, free from manipulation [31]. There is evidence to suggest that where quality legal infrastructure is in place, financial and related operations tend to be more effective and resilient [29]. Innovative infrastructure describes the extent to which the application or introduction of new or original solutions help improve existing needs. According to researchers, including Delimatsis [30], innovations specific to the financial industry and a variety of others are essential for the industry.

5. Propositions Formulation

Entities in differing countries and regions of the world are conditioned by socio-cultural imperatives [13], [14], [23], [24]. To that end, 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, thereby indirectly increasing their organization's risk for experiencing information security threats. A prior study that used the DTTL data reported significant relationships between selected information security issues and the variable of national transparency levels [4]. The study showed that information security was more likely to be prioritized among GFSI respondents where openness, honesty, and fairness seem to be valued. It is therefore proposed that:

P1: There will be a positive relationship between selected information security threats and controls, and national transparency levels.

Past research on corporate responsibilities and firms' ethical behavior has suggested that such issues vary across nations [26], [32]. Workers' perceptions, beliefs, and attitudes toward a wide range of issues, to some extent, can be linked to salient influences arising from their environments [33], [34]. Thus, it is reasonable to expect that perceptions related to information security threats and controls that GFSI employees hold may be impacted by the inherent ethical values of their organizations. Namely, when a GFSI accepts responsibility related to protecting the data of others (customers) in its care, its employees will act accordingly to ensure the CIA of such data is not compromised. It is possible that countries with firms that have positive ethical behavior will have more respondents assessing information security threats and controls more favorably. It is therefore proposed that:

P2: There will be a positive relationship between selected information security threats and controls, and the indicator of ethical behavior of firms.

Research [10-13] shows that countries sometimes employ legal and technology-related approaches to rally against IS security threats and risks. Evidence in the literature suggests that national legal environments and information security issues or concerns are positively associated [10], [11], [35]. Ifinedo [4] showed that the attitudes and behaviors of GFSI employees, with respect to information security threats, are linked to the quality of the legal systems and other regulatory oversights in their contexts. The supposition here is that GFSI employees in contexts where quality rules and regulations are available would readily appreciate the dire consequences of noncompliance with guidelines designed to prevent or control incidents of security threats to organizations' IS resources. It is therefore proposed that:

P3: There will be a positive relationship between selected information security threats and controls, and the legal infrastructure indicator.

Acceptance of practices aimed at containing or militating against information security threats in the financial industry is considered innovative [1]. Innovative infrastructure capable of improving existing needs, including those specific to the financial sector, are relevant to societal progress [30], [36]. Indeed, capacity for innovation – in almost all aspects of human endeavor

– is positively associated with societal advancement and progress [25]. That is, regions with a higher capacity to innovate have quality outcomes in such issues. Recently, Comin and Hobijn [37] showed that technological innovation diffused more readily in advanced societies; others found that innovation varied by nations and corporate practices or culture [38]. With regard to firm innovativeness and organizational performance, Rubera and Kirca [39] uncovered evidence to suggest that both constructs are positively related. In view of the foregoing insights, employees in GFSI from parts of the world with more favorable innovative infrastructure or capacity will appreciate and appraise information security threats and controls favorably. Conversely, those in relatively less innovative contexts will have lesser needs for such.

P4: There will be a positive relationship between selected information security threats and controls, and the capacity for innovation indicator.

6. Methodology

To examine the relationships between information security threats and controls in the 2012 DTTL survey and selected contextual factors considered in this study, secondary data was obtained from reputable international sources. Table 2 shows the variables used in this study. As per information security threats and controls in GFSI, these were taken from the DTTL survey [1]. The six variables in this regard are shown in Table 1.

Data for the other variables was obtained from internationally recognized bodies such as the World Economic Forum [31] and Transparency International [27]. These bodies produce cross-country data on a variety of indicators annually. Their data is considered suitable for this study as they have easily accessible indicators of value to this effort. More importantly, their data collection efforts allow for cross-national comparison given the fact that they were collected in the same time frame and used comparable methods. Researchers comparing issues at the national level have used data from such sources in their studies [4], [24], [35]. Table 2 shows data for the four contextual factors for countries in the regions included in this study.

Region	Country	TCI	EBFI	LII	CII
	Australia	85	6.1	5.3	4
	New Zeeland	90	6.7	5.9	3.8
	Indonesia	32	3.4	3.7	3.8
	Malaysia	49	4.9	4.9	4.3
AP	China	39	4.1	4.1	4.2
	Philippines	34	3.2	2.9	2.7
	Singapore	87	6.6	5.7	4.3
	Thailand	37	3.7	4	3.2
JP	Japan	74	5.8	5	5.8
	Bosnia and Herzegovina	42	3	2.9	2.4
	Belgium	75	5.6	4.5	4.7
	Croatia	46	3.7	2.8	3.1
	Finland	90	6.6	6	5.6
	France	71	5.7	4.9	5.1
	Germany	79	5.9	5.4	5.7
	Greece	36	3.1	3	2.7
EM	Iceland	82	5.6	5.1	4.4
	Luxembourg	80	6.2	5.6	4.5
	Slovenia	61	4.1	3.2	3.9
	Spain	65	4.7	3.7	3.5
	Switzerland	86	6.5	5.8	5.8
	South Africa	43	4.4	4.9	3.4
	Turkey	49	3.9	3.5	3
UK	United Kingdom	74	5.9	5.5	4.8
NA	United States of America	73	5.1	4.5	5.2
	Canada	84	6.5	5.6	4.1
LA	Peru	38	3.7	2.9	2.7
	Mexico	34	3.7	3.2	3
	Brazil	43	3.7	3.6	3.8
	Colombia	36	3.7	3.4	3.2
	Costa Rica	54	4.8	4.2	3.4
	Argentina	35	3.2	2.6	2.9
	Dominican Republic	32	3.3	2.9	2.3
	Honduras	28	3.8	3.5	2.8
	Nicaragua	29	3.2	2.9	2.5
	Panama	38	4.10	2.8	2.7
	Venezuela	19	3.00	1.7	2.4
	Uruguay	72	5.30	4.5	3.0

Note: Transparency and Corruption Index (TCI); Ethical Behavior of Firms Indicator (EBFI); Legal Infrastructure Indicator (LII); Capacity for Innovation Indicator (CII)

Table 2. The study's contextual variables for each country.

Transparency International's [27] website offered data on corruption indices for each country. The scores ranged from "100" (highly uncorrupt) to "0" (highly corrupt). The World Economic Forum [31] provided data for the remaining three variables. As no data was available for assessing legal system efficiency across

nations, this study used a composite score of related items. Data for the legal infrastructure indicator was gauged from each country's scores on the following items: a) judicial independence, which was assessed with "1" = heavily influenced and "7" = entirely independent; b) efficiency of legal framework in setting disputes, which was assessed with "1" = extremely inefficient and "7" = highly efficient; c) efficiency of legal framework in challenging regulations, which was assessed with "1" = extremely inefficient and "7" = highly efficient. The average of these three items was used to represent the legal infrastructure indicator. The same source provided data for the ethical behavior of firms indicator; this was assessed by scores ranging from "1" = among the worst in the world and "7" = among the best in the world. As for the capacity for innovation indicator, each country's data was assessed according to the extent to which companies located in that country obtain their technology. Scores ranged from "1" = exclusively from licensing or imitating foreign companies to "7" = by conducting formal research and pioneering new products and processes.

The study obtained a list of all 38 countries in the 2012 DTTL security survey from the company's researchers. Although a larger set of countries would ideally be suitable for robust analysis, the sample of 38 diverse countries is sufficient for a preliminary study such as this one. In fact, other researchers (e.g. [4], [24]) in related literature have used limited samples of countries to investigate comparable themes. Given that this study is exploratory in nature, its analysis of data obtained from multiple sources does not pose a serious problem. The use of 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 [4], [20-22] [24] have also used data from multiple sources to assess relationships between data obtained at the national level.

Importantly, security threats and controls in the financial services industry reported in the 2012 DTTL survey compared reasonably well with those published by other financial consultants, i.e. Price WaterhousCoopers [40], for the industry. Namely, security breaches, access controls, and cloud computing were among the issues identified as being important for the industry. Thus, the content validity of the study's main data is assured, to some extent. It is easy to see how these foregoing items are relevant to GFSI. An information breach occurs when there is unauthorized access to, or disclosure of organization's information. Identity access management refers to technologies and practices that help to protect users' identities within or across system and enterprise boundaries. Cloud computing covers the use of shared resources in an organization as well as data security facilities.

7. Data Analysis and Results

Correlation provides an indication that two variables have some association: negative or positive. However, it does not indicate that one variable causes the other [41]. Person's correlation analysis was used to assess the strength of the relationships between the study's variables.

A correlation coefficient between 0.1 and 0.4 shows a weak association; 0.5 and above show a fairly strong relationship. In order to gain more insight on the findings, regression analysis was also used. SPSS 18.0 was used for data analysis. The results of the correlation analysis are presented in Table 3; each is subsequently discussed.

	#1	**#2**	**#3**	**#4**	**#5**	**#6**
TCI	−.174	−.271	.437**	−.165	.557**	.300
	.295	.099	.006	.322	.000	.067
EBFI	−.164	−.314	.325*	−.171	.493**	.286
	.325	.055	.047	.306	.002	.082
LII	−.095	−.272	.323*	−.106	.549**	.368*
	.570	.098	.048	.526	.000	.023
CII	−.214	−.322*	.348*	−.128	.615**	.370*
	.198	.049	.032	.444	.000	.022

Note: ** Correlation is significant at the 0.01 level (2-tailed); * Correlation is significant at the 0.05 level (2-tailed); The associated item for a specific number (#) is provided in Table 1; Transparency and Corruption Index (TCI); Ethical Behavior of Firms Indicator (EBFI); Legal Infrastructure Indicator (LII); Capacity for Innovation Indicator (CII)

Table 3. The study's Person's correlation analysis.

8. Discussions and Conclusion

The results showed a weak association between information security threats and controls indicated by "Respondents who believe identity access management is the top security initiative" and national transparency levels. Likewise, the information security threats and control related to "Respondents that implemented or purchased cloud computing services" has a fairly strong association with national transparency levels. The results only partially supported the relevant proposition as not all information security threats and control issues were found to have associations with this particular contextual factor. With these results, it can be suggested that views of GFSI respondents compare reasonably well across different national transparency level settings; however, the perceptions of GFSI respondents in more transparent countries are more favorable in terms of the importance afforded to identity access management and implementing or purchasing cloud computing services. Perhaps the results are suggesting that financial service organizations based in more open societies are better at managing the authentication and authorization of IS with the goal of increasing security and productivity than their counterparts in less open societies. The result also indicated that more open societies appreciate the need of using cloud computing to improve manageability and availability of IS resources so as to meet fluctuating and unpredictable business demands than counterparts in more corrupt contexts.

There are weak associations between information security threats and controls indicated by "Respondents who believe identity access management is the top security initiative" and "Respondents that implemented or purchased cloud computing services", and ethical behavior of firms. These results permit us to suggest that the views of GFSI respondents in countries/regions with higher scores on the ethical behavior of firms' indicator are more favorable to accepting identity access management as a top security initiative. They are also likely to implement or purchase cloud computing services in their contexts.

There is a fairly strong association between information security threats and controls indicated by "Respondents that implemented or purchased cloud computing services" and national legal infrastructure. The analysis is suggesting that the perceptions of GFSI respondents from countries with more efficient legal systems are more favorable towards implementing or purchasing cloud computing services for their enterprises. The use of such facilities might have been upheld by rules and regulations of a country to mitigate security threats and related issues. Also, there is a weak association between "Respondents who experienced privacy-related breaches in the past year" and national legal infrastructure. This result affirms the viewpoint indicating that lower standards in rules and regulations may provide an ambience for privacy-related breaches to occur. Similarly, a weak relationship between "Respondents who believe identity access management is the top security initiative" and national legal infrastructure, may be suggesting that GFSI respondents in countries with inadequate legal infrastructure may have more need to prioritize identity access management, perhaps as a consequence of less robust legal frameworks in their contexts. It might be the case that countries with better legal infrastructures have built-in mechanisms to address emerging security threats; as a consequence, their perception levels of such issues may not be as high as those from the countries lacking such favorable conditions.

There are weak associations between two information security threats and controls i.e. "Respondents who believe identity access management is the top security initiative" and "Respondents who experienced privacy-related breaches in the past year", and capacity for innovation. These results can be interpreted to suggest that GFSI respondents who believe identity access management should be prioritized and those who have experienced privacy-related breaches in the past year are likely to be found in countries/regions with lower capacity for innovation. Further, the capacity for innovation indicator was found to have a weak, negative relationship with "Respondents [who] believe their information security expenditure is on or above plan." It is possible that GFSI respondents from countries with lower capacity for innovation scores, perhaps realizing their limitations regarding controlling and managing information security issues, opt to spend more money compared to their counterparts from elsewhere. Consistent with prediction, respondents that have

implemented or purchased cloud computing services are readily available where the capacity to innovate is relatively high. This is because facilities such as cloud computing services, which are innovative approaches to mitigating security concerns, tend to diffuse faster where quality innovative infrastructure exists.

8.1. Insights from regression analysis

To gain further insight and improve the study's rigor, four (4) regression models were performed. Namely, the four contextual factors were regressed on each of the six (6) information security threats and control issues. This is a noteworthy point given that this study is designed to investigate the impact of contextual influences on the phenomena.

Model	Variable	Standardized Coefficients (Beta)	t-value	Sig (p value)
Regression model #3	TCI	1.446	2.914	.006
	EBFI	1.436	2.094	.044
	LII	.295	.648	.521
	CII	.131	.521	.606
	R^2 =0.31 Issue #3: Respondents who believe identity access management is the top security initiative			
Regression model #5	TCI	1.000	2.343	.025
	EBFI	1.437	2.438	.020
	LII	.657	1.678	.103
	CII	.453	2.104	.043
	R^2 =0.49 Issue #5: Respondents that implemented or purchased cloud computing services			

Table 4. Regression analysis results.

There were no significant results for information security threats and controls numbered, #1, #2, #4, and #5 in Table 1. The results of the analysis for the information security threats and controls with significant results are shown in Table 4.

Regression results showed that both transparency levels and ethical behavior of firms caused significant variations for regression models with the variable related to "Respondents who believe identity access management is the top security initiative" and "Respondents that implemented or purchased cloud computing services". This insight suggests that these variables perhaps have greater importance than other items that had similar significant correlation results in Table 3. In that respect, it is advised that managers of GFSI should pay more attention to the two information security threats and control issues identified as likely to be relevant to the discourse, especially across differing openness and fairness contexts.

8.2. Limitations and directions for future research

There are obvious limitations in this research. This preliminary study used data from secondary sources. As a consequence, it might have inherited all limitations from the DTTL survey, as well as those from the 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 DTTL survey is limiting. Data analysis might have been more robust had the DTTL data been presented on the Likert scale rather than in percentages. Further to this, the diversity of GFSI used in the DTTL survey might also be problematic. It is possible that opinions in the banking sector may be different from those in the insurance business.

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 DTTL surveys. This, however, was impossible because the DTTL security survey data reflected changing information security concerns over the years [1], [7-9]. This reality is consistent with this study's rationale as IS security concerns in organizations never remain static [5]. As such, this research had to use cross-sectional data i.e. data from 2012 to fulfill its stated objectives. As mentioned above, respondents in the DTTL surveys were management personnel; the views of end users were not considered. It is accepted that both groups' views on IS-related issues differ considerably [4]. Thus, it is difficult to say with certainty whether or not the findings in the DTTL study can be generalized across all work groups.

In addition, more useful insights would emerge if national summaries were used instead of regional aggregates. A larger sample of countries (more than 38) might also permit deeper insights. Although this study's preliminary findings provided initial insights into the discourse, it is advised that its interpretations be applied with caution. Even so, this present effort has opened up future areas of inquiry.

Future studies could elaborate on some of the findings in this study. Researchers could combine both quantitative and qualitative methodologies to deepen knowledge in the area. Future research should endeavor to collect data from a single source; the use of data from multiple sources may have its shortcomings. Likert scale should be used to facilitate research replication. Future studies should employ the longitudinal study approach to understand the dynamic nature of information security threats and controls in GFSI and in comparable organizations. Viewpoints of end users and managers should be considered in future research. The relationships of other relevant contextual factors such as educational standards, management education, national culture, economic wealth, organizational managerial practices, and individual attitudes toward information security threats and controls could also be investigated.

8.3. Contributions to scholarship and practical implications

This exploratory study offers implications for both research and practice. From a theoretical perspective, this study engenders knowledge regarding the relationships between selected contextual factors and information security threats and controls. This study is among the few to discuss information security threats and controls vis-à-vis contextual influences such as transparency levels, ethical behavior of a firm, and capacity for innovation in financial services organizations. It reinforces observations in studies that suggest that more insights can surface by studying links between IS security issues with relevant contextual influences. This study complements the body of work focusing on information security assessment in financial organizations [4], [13], [14].

Considering that it uses contingency theory as its referent framework, this study also extends the applicability of that theory to this study's theme. This study has responded to calls in the literature for IS security researchers to adequately focus on the financial services industry. More importantly, it enhances information provided in the 2012 DTTL survey to the degree that more light is shed on the findings reported in that survey. Another contribution of this study is that it partly shows that it would be erroneous to accept that respondents in GFIS hold exactly the same view of information security threats and controls in their industry. This study helps to advance the notion indicating that contextual factors are of critical importance in the assessment of security concerns in general [10-12], [14], [24]. Insights presented in this study could provide useful input or serve as a foundation for future investigations in the area.

Practitioners can benefit from this study's findings as well. For GSFI managers, attention is drawn to the importance of contextual influences. Such additional information may offer a layer of insight to deepen industry-related perceptions and views. The positive associations between some of the contextual factors and information security threats and controls, and the regression analysis's results, might be valuable to GFSI managers across contexts. Notably, the consideration of contextual influences with regard to employees' behaviors and perceptions of information security issues was a worthwhile endeavor. In light of this study's conceptualization, GFSI managers have an understanding of information security threats and controls that might require more attention, and, in particular, in which settings. Practitioners may benefit by taking note of such information in their decision making processes, especially where global operations are in place. Another way that managers can benefit from the findings of this study is by promoting IS security policies and practices that take into account regional differences. The assumption that GFSI are impelled to act according to industry standards may not be entirely true. Greater importance should be accorded to the issue related to the adoption of identity access management and cloud computing services, especially in parts of the world lagging behind on transparency and corporate ethics issues.

References

[1] DTTL, GFSI – 2012, 2012 DTTL Global Financial Services Industry Security Study Breaking Barriers, 2012. http://www.deloitte.com/view/en_GX/global/industries/financial-services/42a6436f82559310VgnVCM2000001b56f00aRCRD.htm#.Ukxb34aTjmc

[2] F. MOSHIRIAN, Financial Services and a Global Single Currency. *Journal of Banking and Finance*, **31**(1) (2007), 3–9.

[3] A. J-T. CHANG, Q-J. YEH, On Security Preparations against Possible IS Threats across Industries. *Information Management & Computer Security*, **14**(4) (2006), 343–360.

[4] P. IFINEDO, Information Technology Security Concerns in Global Financial Services Institutions: Do Socio-Economic Factors Differentiate Perceptions? *International Journal of Information Security and Privacy*, **3**(2) (2009a), 68–83.

[5] D. SCHATZ, Setting Priorities in your Security Program. In *Information Security Management Handbook* (H. F. TIPTON, K. KRAUSE, Eds.), (2008). Taylor & Francis Group. Boca Raton, FL.

[6] ISO/TR 13569, Financial services – Information security guidelines, 2013. http://www.iso.org/iso/catalogue_detail.htm?csnumber=37245

[7] DTT-GLOBAL SECURITY SURVEY – 2005, The Global Security Survey, 2004, Deloitte Touche Tohmatsu (DTT), 2005. http://www.deloitte.com/assets/Dcom-Argentina/Local%20Assets/Documents/global_security.pdf

[8] DTT-GLOBAL SECURITY SURVEY – 2008, The Global Security Survey, 2007, Deloitte Touche Tohmatsu (DTT), 2008. http://www.deloitte.com/assets/Dcom-Shared%20Assets/Documents/dtt_gfsi_GlobalSecuritySurvey_20070901.pdf

[9] DTT-GLOBAL SECURITY SURVEY – 2009, The Global Security Survey, 2008, Deloitte Touche Tohmatsu (DTT), 2009. https://www.deloitte.com/assets/Dcom-Serbia/Local%20Assets/Documents/rs_gfsi_globalsecuritysurvey_0901%282%29.pdf

[10] S. MILBERG, S. BURKE, S. H. J. SMITHAND, E. A. KALLMAN, Values, Personal Information Privacy and Regu-latory Approaches. *Communications of the ACM*, **38**(13) (1995), 65–74.

[11] S. MILBERG, H. J. SMITH, S. BURKE, Information Privacy: Corporate Management and National Regulation. *Organization Science*, **11**(1) (2000), 35–57.

[12] M. BIA, M. KALIKA, Adopting An ICT Code Of Conduct: An Empirical Study of Organizational Factors. *Journal of Enterprise Information Management*, **20**(4) (2007), 432–446.

[13] C. C. CHEN, B. D. MEDLIN, R. S. SHAW, A Cross-Cultural Investigation of Situational Information Security Awareness Programs. *Information Management & Computer Security*, **16**(4) (2008), 360–376.

[14] P. IFINEDO, Information Technology Security Management Concerns in Global Financial Services Institutions: Is National Culture a Differentiator? *Information Management & Computer Security*, **17**(5) (2009b), 372–387.

[15] ENISA, European Union Agency for Network and Information Security, 2013. http://www.enisa.europa.eu

[16] ISO/IEC, Information Technology – Security Techniques-Information Security Risk Management, ISO/IEC FIDIS 27005:2011. 2013. http://www.iso.org/iso/catalogue_detail?csnumber=56742

[17] ISO/IEC 27001:2013, Information technology – Security Techniques – Information Security Management Systems – Requirements, 2013. http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54534

[18] Open Web Application Security Project (OWASP), T10-ArchitectureDiagram 2013. https://www.owasp.org/index.php/ASVS

[19] P. R. LAWRENCE, J. W. LORSCH, Organization and Environment. Division of Research, Graduate School of Business Administration, Harvard University, Boston, Massachusetts, 1967.

[20] Z. KOVAČIĆ, A Brave New Eworld? An Exploratory Analysis of Worldwide E-government Readiness, Level of Democracy, Corruption and Globalization. *International Journal of Electronic Government Research*, **1**(3) (2005), 15–32.

[21] J. E. OXLEY, B. YEUNG, E-commerce Readiness: Institutional Environment and International Competitiveness. *Journal of International Business Studies*, **32**(4) (2001), 705–723.

[22] C.-F. SHIH, J. DEDRICK, K. L. KRAEMER, Rule of Law and the International Diffusion of E-Commerce. *Communications of the ACM*, **48**(11) (2005), 57–62.

[23] C. GUST, J. MARQUEZ, International Comparisons of Productivity Growth: The Role of Information Technologies and Regulatory Practices. *Labour Economics*, **11**(1) (2004), 33–38.

[24] K. BAGCHI, P. KIRS, R. CERVENY, Global Software Piracy: Can Economic Factors Alone Explain the Trend? *Communications of the ACM*, **49**(6) (2006), 70–75.

[25] K. ZHU, K. L. KRAEMER, S. XU, The Process of Innovation Assimilation by Firms in Different Countries: A Technology Diffusion Perspective on E-Business. *Management Science*, **52**(10) (2006), 1557–1576.

[26] I. MAIGNAN, Consumers' Perceptions of Corporate Social Responsibilities: A Crosscultural Comparison. *Journal of Business Ethics*, **30**(1) (2001), 57–72.

[27] Transparency International, Corruption Perception Index – 2012. 2012. http://www.transparency.org/

[28] E. NIER, Bank Stability and Transparency. *Journal of Financial Stability*, **1**(3) (2005), 342–354.

[29] R. TOMASIC, F. AKINBAMI, The Role of Trust in Maintaining the Resilience of Financial Markets. *Journal of Corporate Law Studies*, **11** (2011), 369–394.

[30] P. DELIMATSIS, Transparent Financial Innovation in a Post-Crisis Environment, *Journal of International Economic Law*, **16**(1) (2013), 159–210

[31] World Economic Forum, Global Competitiveness for 2011-2012. 2012. http://www.weforum.org

[32] J. SNIDER, R. P. HILL, D. MARTIN, Corporate Social Responsibility in the 21st Century: A View from the World's Most Successful Firms. *Journal of Business Ethics*, **48**(2) (2003), 175–187.

[33] C. ROBERTSON, P. A. FADIL, Ethical Decision Making in Multinational Organizations: A Culture-Based Model. *Journal of Business Ethics*, **19**(4) (1999), 385–392.

[34] S. VITELL, S. NWACHUKWU, J. BARNES, The Effects of Culture on Ethical Decision-Making: An Application of Hofstede's Typology. *Journal of Business Ethics*, **12**(10) (1993), 753–760.

[35] C.-F. SHIH, J. DEDRICK, K. L. KRAEMER, Rule of Law and the International Diffusion of E-Commerce. *Communications of the ACM*, **48**(11) (2005), 57–62.

[36] D. AWREY, Complexity, Innovation and the Regulation of Modern Financial Markets. *Harvard Business Law Review*, **2**(2) (2012), 235–294.

[37] D. COMIN, B. HOBIJN, An Exploration of Technology Diffusion. *American Economic Review*, **100**(5) (2010), 2031–2059.

[38] G. J. TELLIS, J. C. PRABHU, R. K. CHANDY, Radical Innovation across Nations: The Pre-eminence of Corporate Culture. *Journal of Marketing*, **73**(1) (2009), 3–23.

[39] G. RUBERA, A. H. KIRCA, Firm Innovativeness and Its Performance Outcomes: A Meta-Analytic Review and Theoretical Integration. *Journal of Marketing*, **76**(3) (2012), 130–147.

[40] PricewaterhouseCoopers, The Global State of Information Security Survey 2012, 2012. http://www.pwc.com/jg/en/media-article/2012-global-state-of-information-security-survey.jhtml

[41] J. F. JR. HAIR, R. E. ANDERSON, R. L. THATHAM, W. C. BLACK, *Multivariate Data Analysis*. Prentice-Hall International, Inc Upper Saddle River, NJ, 1998.

Received: October, 2013
Accepted: December, 2013

Contact address:
Dr. Princely Ifinedo
Shannon School of Business
Cape Breton University
P. O. Box 5300
Sydney, Nova Scotia
B1P 6L2, Canada
e-mail: princely_ifinedo@cbu.ca

PRINCELY IFINEDO is an Associate Professor in the Shannon School of Business at Cape Breton University, Canada. He holds a doctoral degree in information systems science from the University of Jyväskylä, Finland, master's degrees from the Royal Holloway, University of London, UK and Tallinn University of Technology, Estonia, bachelor's degree from the University of Port-Harcourt, Nigeria. He has presented research at various international IS conferences, contributed chapters to several books/encyclopedias, and published in several reputable journals including I&M, JCIS, C&S, JSS, DATA BASE, CHB, JOCEC, JITM, IMDS, EIS, IJITDM, JITD, JITM, JGTIM, EG, JISP, and Internet Research. He has authored over 90 peer-reviewed publications and he is affiliated with AIS, IEEE, ISACA, and CIPS.