THE EFFECTS OF NATIONAL CULTURE ON THE ASSESSMENT OF INFORMATION SECURITY THREATS AND CONTROLS IN FINANCIAL SERVICES INDUSTRY

Princely Ifinedo
Department of Financial and Information Management
Cape Breton University
Nova Scotia, B1P 6L2, Canada

ABSTRACT

This study enriches the information provided in the 2012 Deloitte Touche Tohmatsu Limited (DTTL) survey that dealt with information security threats and controls in the global financial services institutions (GFSI). It seeks to provide information on the effects of national cultural dimensions on information security threats and controls in GFSI. The study's analysis used secondary data, which was acquired from relevant, reputable sources. The study's findings offer partial support for the significance of national culture in the discourse. Namely, cultural dimensions of uncertainty avoidance (UAI), individualism versus collectivism (IDV), and masculinity versus femininity (MAS) have effects on the assessment of information threats and controls related to the acquisition and implementation of security tools such as identity access management and cloud computing services. In addition, national cultural norms had effects on respondents' experiences with privacy-related breaches and assessment of information security budget. The implications of the study's preliminary findings for research and practice are discussed.

Keywords: Global Financial Services Industry, Information Security Threats and Controls, National Culture, Secondary Data Sources, Regression Model

1. INTRODUCTION

In general, global financial services institutions (GFSI) continue to witness sustained growth [2, 11, 37]. 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 [40] and to ensure their information assets are protected [29]. Researchers 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 and privacy issues, are somewhat different from other industries [7, 8, 19].

Goodhue and Straub [6] offered several reasons why firms in the financial services sector may be more wary of breaches and threats compared to other businesses. The reasons they espoused include: a) over-reliance on information systems (IS) used 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. Firms in the financial services industries are subjected to strict regulatory supervision [11]. Indeed, the Deloitte Touche Tohmatsu Limited (DTTL) survey [16] 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 constantly protect customer data and effectively manage any emerging threats [8, 27, 29, 49].

Given the need to focus on information security threats and gain an understanding of industry concerns, GFSI practitioners have themselves started investigating and reporting such issues. The series of surveys [13, 14, 15, 16] conducted by DTTL in this regard is noteworthy. The first survey was published in 2003 and others have since followed. These surveys educated practitioners about information security threats; comparative insights across regions were also provided. Key findings in the latest survey for 2012 are available online [16].

Although the findings in the 2012 DTTL survey showed differences across selected regions of the world with respect to the assessment of information security threats and controls in GFSI, inferences from past reports by the company have

* **Corresponding author: Princely_Ifinedo@cbu.ca**

suggested that the assessment of and attitudes toward information security and privacy concerns across GFSI are being informed by industry-related standards or imperatives [13, 14, 15, 28]. This supposition seems to suggest that contextual factors including national culture may mean very little in such discourse. Were this viewpoint accepted as the only truth, empirical studies would not have indicated that countries and even blocs of nations differ in the way they relate to information security and privacy issues [4, 18, 38].

Very little is known about the impact of environmental or contextual factors on the assessment of information security and privacy issues in general, and in GFSI, in particular. The few researchers that have studied the phenomenon did so by considering the influence of socio-economic factors, which are different from cultural issues [27, 29].

It is argued that cultures at the national level exert a subtle, yet powerful influence on individuals and organizations [34, 35, 44]. In fact, Sagiv et al. [44] and Černe et al. [6] noted that organizations are nested within nations; as such, organizations and their employees tend to develop and evolve in ways that are compatible with the surrounding national culture. Put differently, national culture plays a significant role in shaping the perceptions of employees, management, and whole organizations about a wide range of issues, including those related to information systems (IS) security and privacy-related issues [1, 5, 27, 29, 32, 33, 46]. Given the critical role of national culture, this study is designed to increase knowledge of the effects of such factors in the assessment of information threats and controls in GFSI.

The data provided by the 2012 DTTL information security survey and Hofstede's [21, 23] cross-cultural dimensions was used for analysis. The objective of this study is twofold. First, it seeks to increase the depth of information provided in the 2012 DTTL survey. Second, it aims to contribute to the literature on information security and privacy concerns in GFSI. In particular, this study intends to provide answer to the following questions:

Q1: Is there any significant relationships between national cultural factors or dimensions and the assessment of information security threats and controls in GFSI?

Q2: If so, do national cultural dimensions have an effect on the assessment of information security threats and controls in GFSI?

2. BACKGROUND INFORMATION

2.1 Definitions and Overview

GFSI practitioners accept that securing the future of their organizations is linked to how well emerging challenges in their industry are understood and subsequently contained [13 14, 15, 16]. It is almost impossible to implement a perfect security plan that mitigates every threat confronting an organization [29, 36, 45, 49]. Interestingly, savvy corporate managers constantly assess their environments and adjust their security programs and policies accordingly.

The series of surveys on information security threats and controls produced by DTTL was carried out with that understanding. The summarized results provided by DTTL contain information regarding security threats and controls. Drawing from definitions provided in ENISA [18] and ISO/IEC-27005 [30], 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 [31] 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/IEC-27005 [30] and OWASP [41] conceptualize connections between threats, controls, and business impacts; these frameworks have been modified in Figure 1 to depict the linkages between threat agents and business impacts in GFSI. Namely, threat agents (i.e. crackers, criminal organizations) through an attack vector (i.e. phishing, malware attack, sabotage) exploit the 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) causing technical impacts (i.e. compromised confidentiality, integrity or availability (CIA) issues) to an organization's IS resources that 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 ISO/IEC-27005 [31] and OWASP [41] for details). Accordingly, DTTL researchers lumped together information security threats and controls i.e. breaches and identity access management, in their report.

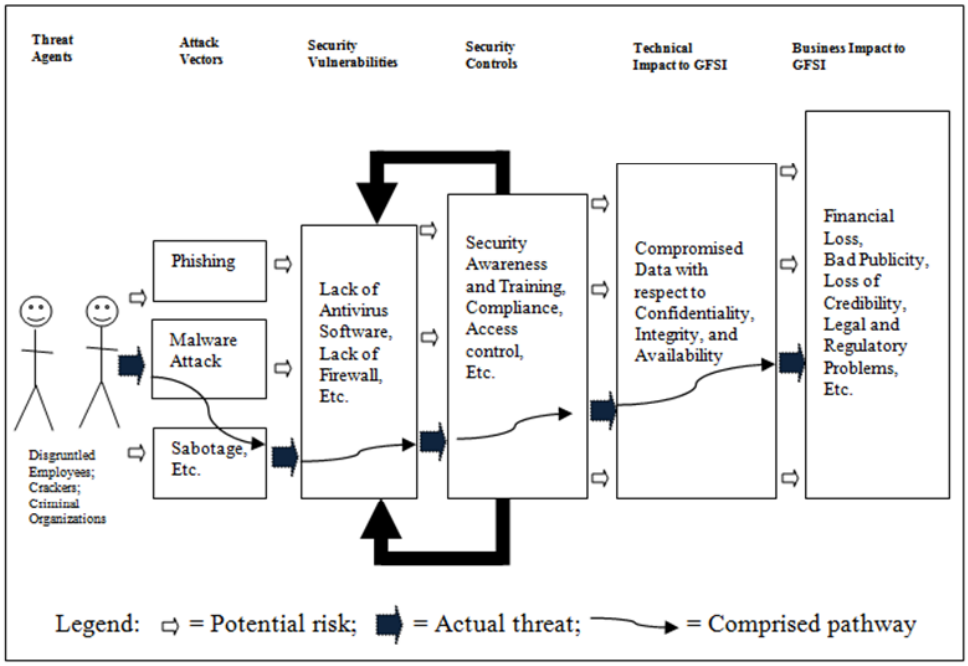

Figure 1: Connections between threat agents to business impact in GFSI [31, 41]

2.2 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 approximately 140 countries. Participants in the 2012 DTTL study came from 40 countries and almost all regions of the world i.e. Asia Pacific (APAC) excluding Japan, Europe, the Middle East and Africa (EMEA), Latin America and the Caribbean Region (LACRO), Canada, and the United States of America. 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. As noted by DTTL [16]:

"*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 survey's authors reported aggregate results/responses for each of the regions, which provided a rough indicator of security concerns for countries in each region. A full list of participating countries 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.

The DTTL report [16] also included the highlights provided below (bulleted points); however, the information does not provide an indication of influences arising from cultural norms and values. This study's 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.

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

No	Threats and Controls	APAC	Japan	EMEA	LACRO	UK	USA	Canada
#1	Respondents believe there is an increase in their information security budget	73	14	55	62	56	94	46
#2	Respondents believe their information security expenditure is on or above plan	50	27	50	50	44	50	31
#3	Respondents who believe identity access management being 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: The entries are indicated in percentages (%).

2.3 National Culture

Hofstede [23] asserted that cultural norms influence the way individuals relate to their environment. Culture is the collective programming of the mind, which distinguishes the members of one group from another [23]; it represents the fabric of meaning through which a society interprets the events around it. National culture tends not only to be ingrained it also influences individuals and group behavior with regard to how they interpret and implement practices within their contexts [6, 44].

Cross-cultural factors have been studied using differing models. The three most commonly used models are: Hofstede [23], Schwartz [47], and GLOBE [24]. There is considerable controversy regarding the rigor and content of each model; nonetheless, there is an overlap among the models. Hofstede's perspective [23] has been widely recognized as the most dominant framework for theory development and validation in cross-cultural studies (e.g. [6, 44, 50]).

The four main cultural dimensions in Hofstede's typology are Power Distance (PDI), Individualism versus Collectivism (IDV), Masculinity versus Femininity (MAS), and Uncertainty Avoidance (UAI); their meanings are provided in Table 2. It is worth noting that two other dimensions i.e. Long-Term Orientation and Indulgence versus Restraint were later added to Hofstede's typology [37, 38]. However, these new dimensions will not be included in this study as data for some of the selected countries in this study do not have scores on those dimensions yet.

2.3.1 National culture and IS security and Related Concerns

Previous research suggested that national cultural factors matter in the discourse of IS security and privacy issues [5, 9, 12, 32, 33, 46]. These prior studies argued that in order for business organizations to cope with IS security and privacy-related issues in their contexts, an understanding of national cultural norms and values are of critical importance. For instance, Bjorck and Jiang [5] found that the assessment of IS security implementations differed by cultural attributes. Schmidt et al. [46] in studying Chinese and American cultures found significant differences in their perceptions of relevant computer security threats.

Dinev et al. [12] showed that national cultural differences can be used to differentiate user behavior towards protective security technologies. Johnson and Warkentin [32] found national culture to be an important factor for understanding privacy concerns and organizational commitment. However, others have also suggested that national cultural values matter less in the assessment of IS security issues. For example, Milberg et al. [38] sampling the views of approximately 900 ISACA members in 30 countries on selected privacy concerns did not find any significant differences between the participants on three dimensions of national culture: PDI, UAI, and IND. Ifinedo [28] found that national culture has no

bearing of the perceptions of IS security concerns by GFSI respondents. A summary of the studies that have included both national culture and IS security and related issues is shown in Table 3.

Table 2: Hofstede's cultural dimensions

Dimension	Definition	Manifestations
Power Distance (PDI)	The extent to which less powerful members of a society accept and expect power to be distributed unequally.	People in large PDI societies accept a hierarchical order in which everybody has a place and needs no further justification. In societies with low PDI, people strive to equalize the distribution of power and demand justification for inequalities in power [21, 23].
Individualism versus Collectivism (IDV)	The extent to which members of a society reinforce individual or collective achievement and interpersonal relationships	People in individualistic societies are expected to take care of themselves and their immediate families only. In collectivist societies, there is a preference for a tightly-knit framework in which individuals can expect their relatives or members of a particular in-group to look after them in exchange for unquestioning loyalty [21, 23].
Masculinity versus Femininity (MAS)	The extent to which members of a society differentiate and emphasize traditional gender and work roles.	In a masculine society, preference is placed on achievement, heroism, assertiveness, power, and material reward for success. In feminine societies, preference is for cooperation, modesty, caring for the weak and quality of life [21, 23].
Uncertainty Avoidance (UAI)	The extent to which members of a society feel uncomfortable with uncertainty and ambiguity.	Countries with strong UAI maintain rigid codes of beliefs and behaviors, and are intolerant of unorthodox ideas. In weak UAI societies, people are more flexible, tolerant of differing behaviors and opinions, and have risk taking behaviors [21, 23].

Table 3: Research with national culture and IS security and related issues as variables

Research	Independent or moderating variable	Dependent variable	Publishing outlet
Dinev et al. [12]	PDI, UAI, MAS, IDV and LTO i.e. Hofstede's dimensions	Behavioral intention of security technologies	Information Systems Journal
Hovav and D'Arcy [25]	PDI, UAI, IDV and LTO i.e. Hofstede's dimensions	Information systems misuse	Information and Management
Bjorck and Jiang [5]	PDI, UAI, MAS, and IDV, i.e. Hofstede's dimensions	Effectiveness of IS security implementation	Master's thesis, Royal Institute of Technology, Stockholm, Sweden
Schmidt et al. [46]	PDI, UAI, MAS, IDV and LTO i.e. Hofstede's dimensions	Computer security awareness	Journal of Global Information Management
Alfawaz [1]	PDI, UAI, IDV and Hall's () Context	Information security management in organizations	PhD thesis, Queensland University of Technology, Australia
Ifinedo [28]	PDI, UAI, MAS, and IDV, i.e. Hofstede's dimensions	Information security management in GFSI	Information Management & Computer Security
Milberg et al. [38]	PDI, UAI, MAS	Information privacy concerns	Organization Science
Chen et al. [9]	PDI, UAI, MAS, and IDV, i.e. Hofstede's dimensions	Situational information security awareness programs	Information Management & Computer Security
Johnson et al. [33]	IDV, i.e. Hofstede's dimension	Information security assurance	Americas Conference on Information Systems (AMCIS) 2009 Conference
Johnson and Warkentin [32]	IDV, i.e. Hofstede's dimension	Privacy concerns and organizational commitment	International Federation for Information Processing (IFIP) 2009 Conference

3. HYPOTHESES FORMULATION

Hofstede's cultural index represented weak UAI countries with lower numerical scores; high UAI had higher scores. That said, individuals from cultures with weak UAI tend to accept higher levels of risk and uncertainty; they are more flexible in relation to unorthodox ideas and situations as they are socialized to accept such conditions [21, 23]. In contrast, people from strong UAI societies tend to exhibit high levels of anxiety and stress in dealing with uncertainty. Considering that emerging information security controls are innovative and may include new codes of beliefs and practices, it is to be expected the views of GFSI respondents from strong UAI cultures will be rigid while those from weak UAI societies will be more flexible. Moreover, information security threats are destabilizing [10, 16]; as such, it is to be expected that individuals from cultures averse to risks will not cope as well as counterparts from more risk tolerant societies [23, 24]. Past research on security and related issues has affirmed the foregoing insight [1]. Hence, it is predicted that:

H1: There will be a negative relationship between GFSI respondents' assessment of information security threats/controls and UAI, and this cultural dimension will have a significant effect on relevant items.

Hofstede [23] found that organizations in countries with high PDI tend to have centralized decision structures; their use of formal rules, as well as the flow of information, is constrained by hierarchy [6, 44, 50]. Hofstede also indicated that technological innovations' adoption is higher in countries with low PDI. As indicated, emerging information security controls are innovative in nature [10, 16, 42, 43]. Prior studies have supported the view indicating that new ideas and innovation diffuse faster in countries with a low PDI scores [48]. This may be due to the fact that individuals from such cultures operate in environments where decision making responsibility and authority is decentralized to allow them to take personal initiative in various issues [23, 24]. In contrast, individuals from high PDI cultures are expected to take their cues from those in authority. Björck and Jiang [5] found that individuals from differing power distance contexts assessed and related to IS security implementations differently, perhaps due to differences in organizational decision structures. Hence, it is predicted that:

H2: There will be a negative relationship between GFSI respondents' assessment of information security threats/controls and PDI, and this cultural dimension will have a significant effect on relevant items.

According to Hofstede [21, 23], feminine societies prefer solidarity, equality, cooperation, modesty, consensus seeking, and social relationships, while masculine societies placed more preference on achievement, heroism, ambition, competition, assertiveness, and power. It can be argued that behaviors and attitudes toward information security threats and controls would yield favorable outcomes where solidarity, cooperation, and consensus seeking are highly regarded. Often times, to effectively confront emerging threats and other security and privacy concerns, there is a need for organizations and their workers to build consensus and foster social relationships on such issues [16]. It is not suggested that attributes such as achievement, heroism, ambition, competition, and so forth mean little for the assessment of information security threats and controls; rather, it is stressed that the ideals contained in feminine cultures may seem more pertinent to eliciting favorable outcomes on such issues. Studies by Schmidt et al. [46], Milberg et al. [38], and Dinev et al. [12] confirmed that information security and privacy issues were better appreciated in feminine societies than in more masculine ones. Hence, it is predicted that:

H3: There will be a negative relationship between GFSI respondents' assessment of information security threats/controls and MAS, and this cultural dimension will have a significant effect on relevant items.

Hofstede's index represented high IDV countries with higher numerical scores; low IDV countries had lower scores. That said, people from individualistic cultures are driven by personal motivations and choices, whereas individuals from collectivistic countries are governed by group norms and aspirations [21, 23, 24]. In other words, people from individualistic societies often have more freedom to apply personal initiatives and act on their own; the same is not true for individuals from collectivistic cultures that are governed by collective decisions. It is possible that where group consensus is sought, delays in implementing needed courses of actions may ensue.

On the other hand, personal action and initiative are conducive to innovation. Waarts and van Everdingen [50] noted that perhaps such personal initiative has led to more patents being granted in individualistic countries than in collectivistic contexts. With respect to information security management and related issues, past evidence suggests that people from individualistic cultures act

more favorable toward to information security-related issues than counterparts from collectivist cultures [21, 24]. Against such a backdrop, it is expected that the assessment of relevant information threats and controls by GFSI respondents will have a similar outcome. Hence, it is predicted that:

H4: There will be a positive relationship between GFSI respondents' assessment of information security threats/controls and IDV, and this cultural dimension will have a significant effect on relevant items.

4. DATA AND RESEARCH METHODOLOGY

To examine the effects of national cultural attributes on the information security threats and controls, secondary data sources were used. As indicated, six (6) information security threats and controls in GFSI were taken from DTTL [16] (these are shown in Table 1). Appendix A shows Hofstede's cultural dimension scores for each country used in the study; the scores were taken from [21, 23]. The cultural dimensions were developed by Hofstede in a comprehensive study of how culture influences values in the workplace. He collected data from over 100,000 individuals in more than 70 countries. Four (4) countries i.e. Nicaragua, Dominican Republic, Honduras, and Iceland that were in the DTTL survey were not included in this study's data analysis as they did not score on Hofstede's cultural dimensions. With respect to Bosnia and Herzegovina, this study utilized data for the old Yugoslavia given that it was part of that country when Hofstede carried out his study.

Thus, data from 34 countries was used for analysis. Although a larger sample of countries would ideally be suitable for robust analysis; a sample of 34 diverse countries is sufficient for a preliminary study such as this one. For the purposes of this study, the analysis of data obtained from multiple sources does not pose a serious problem. The use of multiple-sourced data has been used in comparable research [3, 28, 29, 38]. It is worth noting that the information security threats and controls in the financial services industry reported in the 2012 DTTL survey compared reasonably well with those published by other global financial consultants e.g., PricewaterhouseCoopers [43]. Notably, security breaches, access controls, and cloud computing services are among the issues identified as important to the industry. Thus, to some degree, the content validity of the study's main data is assured.

5. DATA ANALYSIS AND PROCEDURE

SPSS 18.0 was used for data analysis. In providing an answer to question (Q1), correlation analysis, which provides an indication that two variables have some association (negative or positive), was used. However, correlation does not indicate that one variable causes the other (Hair et al., 1998). Person's correlation analysis was used to assess the strength of relationships between the study's variables. A correlation coefficient between 0.1 and 0.4 shows a weak association, 0.5 and above shows a fairly strong relationship [20].

The results of the correlation analysis are presented in Table 4. There were 9 significant relationships of out a total of 24 (approximately 40%). This is sufficient for this preliminary investigation as it suggested partial support for predictions made with the study's variables. For the purposes of this study, a significant, statistical relationship between at least one of the four (4) independent variables (i.e. cultural dimensions) and any of one of the six (6) information security threats and controls (dependent variables) is sufficient for preliminary insight.

For question (Q2), multiple regression analysis was used. The results are provided in Appendix B. Multiple regression models were estimated (please see Equation 1) with the goal of determining the effects of national cultural factors on assessment of information security threats and controls..

$$Yt = \alpha + \beta1(INDt) + \beta2\ (MASt) + \beta3(PDIt) + \beta4\ (UAI)t + et \quad \text{---------- Equation 1}$$

Where the subscript "t" stands for countries, α is the unknown intercept, β is the parameter to be estimated, "e" is the error term of the standard assumption, "Y" is each of the six (6) information security threats and controls considered in the study, PDI = Power Distance, MAS = Masculinity versus Femininity, IDV = Individualism versus Collectivism, and UAI = Uncertainty Avoidance

Figure 2: The study's regression equation

Table 4: The correlations matrix

		Issue #1	Issue #2	Issue #3	Issue #4	Issue #5	Issue #6
	N	34	34	34	34	34	34
PDI	Pearson Correlation	.152	.204	-.351*	.358*z	-.370*	-.217
	Sig. (2-tailed)	.390	.247	.042	.038	.031	.217
	N	34	34	34	34	34	34
IDV	Pearson Correlation	-.066	-.230	.524**	-.448**z	.666**	.451**
	Sig. (2-tailed)	.710	.190	.001	.008	.000	.007
	N	34	34	34	34	34	34
MAS	Pearson Correlation	-.148	-.387*	-.248	-.094	.137	.170
	Sig. (2-tailed)	.403	.024	.157	.596	.439	.335
	N	34	34	34	34	34	34
UAI	Pearson Correlation	-.475**	.020	.069	.094	-.446**	-.570**
	Sig. (2-tailed)	.005	.912	.698	.596	.008	.000
	N	34	34	34	34	34	34

Notes: ** = Correlation is significant at the 0.01 level (2-tailed); *= Correlation is significant at the 0.05 level (2-tailed); z = significant, but not considered due to direction; # = the issue for a specific number is provided in Table 1.

To enhance the results obtained with respect to Q1, it is recommended that assumptions in the regression analyses are tested [20]. In that regard, the two assumptions of relevance are multicollinearity and residual independence. Multicollinearity exists when two or more predictor variables in a multiple regression model are highly correlated. Multicollinearity was examined through Variance Inflation Factor (VIF) values; this does not appear to present any major problems for the study's data. The VIF for the study's variables ranged from 1.1 to 2.3, which is below the acceptable VIF's critical value of 10 for moderate multicollinearity [20].

To test for residual independence, the Durbin-Watson statistic [48] is recommended; it tests for autocorrelation in regression analysis residuals. The Durbin-Watson statistic is always between 0 and 4. A value of 2 indicates there is no autocorrelation in the data sample. Values approaching 0 indicate positive autocorrelation and values toward 4 indicate negative autocorrelation. The results show that residual independence is not a problem for the study's data as the results in this aspect ranged from 1.2 to 2.3 for all regression analyses except for #4 which had a value of 0.5.

6. RESULTS AND DISCUSSIONS

The absence of statistical significant relationships between variables or the lack of support for the effects of certain independent variables on the dependent variables may be attributable to research design problems. It can be equally argued that the lack of support may be a reflection of reality. The scope of this study does not extend to explaining why certain aspects of the results were obtained. That said, the study's significant results will be discussed in two parts. With respect to Q1, the data analysis provided the following elucidating insights:

1. The data indicated weak negative correlations between information security threats and controls indicated by "Respondents who believe identity access management being the top security initiative" (Issue #3) and "Respondents that implemented or purchased cloud computing services" (Issue #5) and PDI. That is, GFSI respondents from weak PDI societies seemed to appreciate the need to acquire and implement security tools such as identity access management and cloud computing services in their environments more than counterparts from high PDI contexts. It is possible that the disparity is due to the fact that individuals from high PDI contexts may not enjoy as much freedom as their colleagues from weak PDI societies when it comes to contributing to decision making related to adopting facilities to better manage and control IS security issues.
2. The data showed fairly strong positive correlations between information security threats and controls indicated by "Respondents who believe identity access management being the top security initiative" (Issue #3), "Respondents that implemented or purchased cloud computing services" (Issue #5), and "Respondents who experienced privacy-related breaches in the past year" (Issue #6) on one hand, and IDV on the other. That is, GFSI respondents from strong IDV countries seemed to appreciate the need to acquire and implement security tools, i.e., identity access management and cloud computing services, in their environments than counterparts from high PDI contexts; they are also more likely to have experienced privacy-related breaches in the recent past. It comes as no surprise that the foregoing results were observed given that personal initiative boded well for the acceptance of

technological innovations, in general, and IS security-related ones as well [23, 24, 50]. Additionally, the pressure of stigmatization from group or societal members may be less pronounce or absent in individualistic societies compared to cultural groups that demand conformity, thereby making it easier for people from individualistic contexts to be more forthright in reporting security breaches in their contexts..

3. The data indicated weak negative correlations between information security threat and control indicated by "Respondents believe their information security expenditure is on or above plan" (Issue #2) and MAS. That is, GFSI respondents from weak MAS countries seemed to believe that their financial commitment toward information security was up to par. Perhaps such cultures realize a greater need to effectively combat information security concerns with financial resources. In the context of this study, the views from more masculine countries appeared to be different. Consistent with past findings in the area, the result in this regard affirmed the notion that information security and privacy issues, including resource allocation for IS security management, are better appreciated in feminine societies [12, 38, 46] perhaps due to influences arising from their cultural norms and practices.
4. The data showed fairly strong positive correlations between information security threats and controls indicated by "Respondents believe there is an increase in their information security budget" (Issue #1), "Respondents that implemented or purchased cloud computing services" (Issue #5), and "Respondents who experienced privacy-related breaches in the past year" (Issue #6) on the one hand, and PDI on the other. That is, GFSI respondents with weak UAI tended to accept higher levels of uncertainty associated with the management of IS security threats in their organizations. The result indicated that GFSI respondents in weak UAI contexts have observed an increase in their IS security budgets, and have spent more to acquire and implement security tools such as cloud computing services than their counterparts from strong UAI cultures, which are rigid to uncertain ideas or in this instance, IS security issues. As IS threats can be destabilizing, it comes as no surprise that GFSI workers more tolerant of risks and uncertainties are better poised in committing resources and deploying facilities capable of militating against such concerns. They also appear also more willing to report threat incidents in their contexts than counterparts from elsewhere.

With respect to Q2, the following insights are offered: the regression result showed that only UAI had a significant effect on information security threats and controls indicated by "Respondents believe there is an increase in their information security budget" (Issue #1) (β = -0.551, $p < 0.05$). Namely, the assessment of this item by GFSI respondents is strongly influenced by their degree of tolerance for uncertainties, ambiguities, and risks (or threats). As discussed above, those from weak UAI contexts tended to see more need to allocate financial resources to IS security management in their organizations. Regarding information security threats and controls indicated by "Respondents believe their information security expenditure is on or above plan" (Issue #2), the data showed that only MAS had a significant effect on this item (β = -0.381, $p < 0.05$). That is, the views of GFSI respondents with respect to the allocation of financial resources for IS security management is strongly influenced by societal values characterized by the value given to masculinity and femininity concerns. The results above showed that feminine values and concerns augured for IS security issues.

Two cultural dimensions of IDV and MAS were found to have significant effects on information security threat and control indicated by "Respondents who believe identity access management being the top security initiative" (Issue #3). These results affirmed that the cultural dimensions of IDV (β = 0.792, $p < 0.05$) and MAS (β = -0.425, $p < 0.05$) strongly mattered in shaping the views of GFSI respondents with regard to the assessment of identity access management as a key IS security tool in their organizations. Previous results showed that GFSI respondents from countries with strong individualistic norms appreciated the potential of identity access management for information security management in their organizations more than counterparts from collectivist societies. In addition, the need for such tools were found be in higher in feminine contexts as well.

The information security threats and controls indicated by "Respondents who believe IS governance as the top security initiative" (Issue #4) did not yield any meaningful results. As per. "Respondents that implemented or purchased cloud computing services" (Issue #5), the regression result in this aspect showed that IDV (β = 0.763, $p < 0.001$) and UAI (β = -0.312, $p < 0.05$) significantly affected this item. Namely, the assessment of this item by GFSI respondents is strongly influenced by their degree of tolerance for uncertainties and the extent to which their societies value individualistic or group aspirations. As previously noted, GFSI respondents in strong IDV countries tend to see more need to acquire cloud computing services in managing IS security. Likewise, GFSI respondents from societies more

tolerant of risks tended to appreciate the benefits of implementing IS security tools such as cloud computing services in their organizations than others from societies averse of risks and uncertainties.

The regression result showed that IDV (β = 0.449, $p < 0.05$) and UAI (β = -0.448, $p < 0.05$) had significant effects on information security threat and control indicated by "Respondents who experienced privacy-related breaches in the past year" (Issue #6). That is, the assessment of this item by GFSI respondents is strongly influenced by the extent to which their societies value individualistic or group values and their aversions to uncertainties, ambiguities, and risks (or threats). As indicated above, GFSI respondents in individualistic contexts reported more incidents of security breaches in their organizations than those from collectivist societies. Similarly, GFSI respondents from countries with weak UAI who are conditioned to accept higher levels of uncertainties tended to report more incidents of security breaches in their organizations.

6.1 Limitations and Directions for Future research

This study clearly has its limitations. For example, it used data obtained mainly from secondary sources. As a result, it might have inherited all limitations from the DTTL survey as well those from the other sources used. One example is the absence of demographic information in the DTTL survey; this is limiting. The reliability and validity of items used in composing various measures in secondary sources cannot be assured. 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. Data analysis might have been more robust had the DTTL data been presented on the Likert scale rather than in percentages.

It is worth noting that an attempt was made to perform a longitudinal analysis of the data that has 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. This reality is consistent with the reality indicating that IS security concerns in organizations never remain static [29]. As a consequence, this study had to use cross-sectional data i.e. data from 2012, to fulfill its stated objectives. The respondents in the DTTL surveys were mainly management personnel; the views of lower level personnel were not considered. It is accepted that both employers' and employees' views of security differ [26, 39]. Thus, it is difficult to say with certainty whether or not the findings in the DTTL study can be generalized across all work groups. More useful insights would emerge if national summaries were used instead of regional aggregates. A larger sample of countries (more than 34) might also permit deeper insights. This present effort has opened up future areas of inquiry even though some of its apparent limitations have been noted. To that end, it is advised that the interpretations of this research study be applied with caution.

Future researchers could improve understanding by addressing some of this study's limitations. To add more meaning to the insights uncovered in this current 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 as the use of data from multiple sources may have its shortcomings. The Likert scale should be used to facilitate research replication. Future studies should employ a longitudinal study approach to understand the dynamic nature of information security threats and controls in GFSI and in comparable organizations. Viewpoints of both end users i.e. workers and managers should be considered in future research. The relationships between information security threats and controls and other relevant contextual factors such as national technological capability, educational standards, legislation, and organizational managerial practices, could also be investigated.

6.2 Contributions to Scholarship and Practical Implications

This preliminary study offers implications for both researchers and practitioners. From a theoretical perspective, this study added insight regarding the effects of selected cultural dimensions on information security threats and controls in GFSI. This study adds to the body of work focusing on information security assessment in financial organizations [7, 9, 28, 29] and lends support to observations in the extant literature that signify the pertinence of cross-cultural factors to information and security management in organizations [1, 3, 4, 5, 9, 28, 33, 38, 46].

This study's analysis has enriched the information provided in the 2012 DTTL survey. This study has responded to calls in the literature for IS security researchers to adequately focus on the financial services industry. Information garnered from this effort could provide useful input or serve as a foundation for future studies in the area. Above all, this study provides partial support to the fact that it would be erroneous to accept that all respondents across GFIS hold exactly the same view of information security threats and controls in their industry, and that environmental factors such as national culture do not matter.

The benefits to practitioners are as follows: For GSFI managers, attention is drawn to the importance of contextual influences. Such additional information may offer a layer of insight that deepens industry-related perceptions of information security

threats and controls. The knowledge of the relationships between national cultural factors and the assessment of information security threats and controls might be valuable to GFSI managers as they manage workers' expectations across differing contexts.

This study provides information about information security and control issues likely to be affected by national cultural norms. As indicated, past studies confirmed that national cultural values significantly influence the views of stakeholders, i.e. employees, management, and the entire organization on IS security and privacy-related issues [1, 3, 4, 5, 9, 28, 33, 38, 46]. When such an influential contextual factor is not adequately considered by GFSI operators, unfavorable consequences could ensue. For example, they could suffer serious, negative business impact such as loss credibility, revenue, and bad publicity if their data/information resources are compromised due to workers' cultural underpinnings or conditioning.

Practitioners benefit from this study's findings by taking note of the critical role national cultural values play in the assessment of information security and controls, especially where global operations are in place. Another way managers can benefit from this study's findings is by promoting organizational IS security policies and acceptable practices and procedures that take into account regional differences (and similarities). For example, inhibiting cultural attributes that may hinder the deployment and implementation of IS security tools and procedures could be re-examined and appropriate countermeasures suitable for each contexts be proposed. It may be advisable for management of GFSI to proactively look into ways of re-sensitizing and re-training workers from any part of the world where prevailing environments might have conditioned employees to act in ways not in agreement with organizational information security postures.

7. CONCLUSION

This study has deepened the breadth of information provided in the 2012 Deloitte Touche Tohmatsu Limited (DTTL) report that surveyed IS security threats in the global financial services industry. The main contribution of this current study is it signified the critical importance of cultural dimensions related to uncertainty avoidance (UAI), individualism versus collectivism (IDV), and masculinity versus femininity (MAS) to the perceptions of IS threats and controls in GFSI. It is hoped that this study's findings will spur on further research and inquiries in the area. Practitioners could use the information provided in this study to better manage their workers' take on IS security and privacy concerns across differing global settings.

ACKNOWLEDGEMENTS

The author is grateful for the assistance received from contacts in DTTL.

REFERENCES

1. Alfawaz, S. M., 2011, "Information security management: a case study of an information security culture," *Queensland University of Technology, PhD thesis*.
2. Arestis, P., Baddeley, M. and McCombie, J., 2003, *Globalisation, Regionalism and Economic Activity*, Edward Elgar Publishing, Cheltenham, UK.
3. Bagchi, K., Kirs, P. and Cerveny, R., 2006, "Global software piracy: Can economic factors alone explain the trend?" *Communications of the ACM*, Vol. 49, No. 6, pp. 70-75.
4. Bia, M. and Kalika, M., 2007, "Adopting an ICT code of conduct: an empirical study of organizational factors," *Journal of Enterprise Information Management*, Vol. 20, No. 4, pp. 432-446.
5. Björck, J. and Jiang, K. W. B., 2006, "Information security and national culture: Comparison between ERP system security implementations in Singapore and Sweden," *Master Degree Thesis Submitted at the Royal Institute of Technology*, Sweden.
6. Černe, M., Jaklič, M. and Škerlavaj, M., 2013, "Decoupling management and technological innovations: Resolving the individualism–collectivism controversy," *Journal of International Management*, Vol. 19, No. 2, pp. 103-117.
7. Chang, A. J. and Yeh, Q., 2006, "On security preparations against possible is threats across industries," *Information Management & Computer Security*, Vol. 14, No. 4, pp. 343-360.
8. Chang, I. C., Hwang, H. G., Yen, D. C. and Huang, H. Y., 2006, "An empirical study of the factors affecting Internet security for the financial industry in Taiwan," *Telematics and Informatics*, Vol. 23, No. 4, pp. 343-364.
9. Chen, C. C., Medlin, B. D. and Shaw, R. S., 2008, "A cross-cultural investigation of situational information security awareness programs," *Information Management & Computer Security*, Vol. 16, No. 4, pp. 360-376.
10. Cretan, A., da Silva, C. F., Coutinho, C., Jardim-Goncalves, R., and Ghodous, P., 2013, "Framework for ontology-based negotiation to support enterprise interoperability in

cloud-based environments," *International Journal of Electronic Business Management*, Vol. 11, No. 3, pp. 168-177.
11. Delimatsis, P., 2013, "Transparent financial innovation in a post-crisis environment," *Journal of International Economic Law*, Vol. 16, No. 1, pp. 159-210.
12. Dinev, T., Goo, J., Hu, Q. and Nam, K., 2009, "User behaviour towards protective information technologies: The role of national cultural differences," *Information Systems Journal*, Vol. 19, No. 4, pp. 391-412.
13. DTT-Global Security Survey, 2005, "The global security survey, 2004, Deloitte Touche Tohmatsu (DTT)," http://www.deloitte.com/assets/Dcom-Argentina/Local%20Assets/Documents/global_security.pdf.
14. DTT-Global Security Survey, 2008, "The global security survey, 2007, Deloitte Touche Tohmatsu (DTT)," http://www.deloitte.com/assets/Dcom-Shared%20Assets/Documents/dtt_gfsi_GlobalSecuritySurvey_20070901.pdf.
15. DTT-Global Security Survey, 2009, "The global security survey, 2008, Deloitte Touche Tohmatsu (DTT)," https://www.deloitte.com/assets/Dcom-Serbia/Local%20Assets/Documents/rs_gfsi_globalsecuritysurvey_0901%282%29.pdf.
16. DTTL, 2012, "2012 DTTL global financial services industry security study breaking barriers," http://www.deloitte.com/view/en_GX/global/industries/financial-services/42a6436f82559310VgnVCM2000001b56f00aRCRD.htm#.Ukxb34aTjmc.
17. Durbin, J. and Watson, G .S., 1971, "Testing for serial correlation in least squares regression.III," *Biometrika*, Vol. 58, No. 1, pp. 1–19.
18. ENISA, 2013, "European Union Agency for Network and Information Security." http://www.enisa.europa.eu/.
19. Goodhue, D. L. and Straub, D. W., 1991, "Security concerns of system users: a study of the perceptions of the adequacy of security," *Information and Management*, Vol. 20, No. 1, pp. 13-22.
20. Hair, J. F. Jr., Anderson, R. E., Thatham, R. L. and Black, W. C., 1998, *Multivariate Data Analysis*, Prentice-Hall International, Inc., Upper Saddle River, NJ.
21. Hofstede, G., 2013, "The Hofstede centre - National culture, countries," http://geert-hofstede.com/. Retrieved October 3, 2013.
22. Hofstede, G. and Bond, M. H., 1988, "The Confucius connection: from cultural roots to economic growth," *Organizational Dynamics*, Vol. 16, pp. 4-21.
23. Hoftstede, G., 2001, "Culture's Consequences," Second edition, Sage Publications, Thousand Oaks, CA.
24. House, R., Hanges, P., Javidan,M., Dorfman, P. and Gupta, V., 2004, "Leadership, Culture, and Organizations: The GLOBE Study of 62 Societies," Sage Publications, Beverly Hills, CA.
25. Hovav, A. and D'Arcy, J., 2012, "Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U.S. and South Korea," *Information & Management*, Vol. 49, No. 2, pp. 99-110.
26. Ifinedo, P., 2007, "An empirical study of ERP success evaluations by business and IT managers," *Information Management & Computer Security*, Vol. 15, No. 4, pp. 270-282.
27. Ifinedo, P., 2009a, "Information technology security concerns in global financial services institutions: do socio-economic factors differentiate perceptions?" *International Journal of Information Security and Privacy*, Vol. 3, No. 2, pp. 68-83.
28. Ifinedo, P., 2009b, "Information technology security management concerns in global financial services institutions: is national culture a differentiator?" *Information Management & Computer Security*, Vol. 17, No. 5, pp. 372-387.
29. Ifinedo, P., 2013, "Relationships between relevant contextual influences and information security threats and controls in global financial services industry," *Journal of Computing and Information Technology*, Vol. 21, No. 4, pp. 235-246.
30. ISO/IEC – 27005, "Information Technology -- Security Techniques-Information Security Risk Management.' Retrieved October 3, 2013. http://www.iso.org/iso/catalogue_detail?csnumber=56742.
31. ISO/IEC- 27001, "Information technology -- Security Techniques -- Information Security Management Systems – Requirements," Retrieved October 3, 2013. http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54534.
32. Johnston, A. C. and Warkentin, M., 2009, "National culture and information privacy: the influential effects of individualism and collectivism on privacy concerns and organizational commitment," *In Proceedings of the International Federation of Information Processing (IFIP), International Workshop on Information Systems Security Research*, Cape Town, South Africa, pp. 88-104.
33. Johnston, A., Warkentin, M. and Luo, R., 2009, "The impact of national culture on workplace privacy expectations in the context of information security assurance," *In*

Proceedings of the 2009 Americas Conference on Information Systems, pp. 3939-3944.
34. Lee, S. G., Trimi, S. and Kim, C., 2013, "The impact of cultural differences on technology adoption," *Journal of World Business*, Vol. 48, pp. 20-29.
35. Leidner, D. E. and Kayworth, T., 2006, "Review: a review of culture in information systems research: toward a theory of information technology culture conflict," *MIS Quarterly*, Vol. 30, No. 2, pp. 357-399.
36. Liu, A., Chang, H. K., Lo, Y. and Wang, S., 2012, "The increase of RFID privacy and security with mutual authentication mechanism in supply chain management," *International Journal of Electronic Business Management*, Vol. 10, No. 1, pp. 1-7.
37. Liu, Z., Lin, F. and Fang, L., 2009, "A study of applying DEA to measure the performance on bank implementing financial electronic data interchange," *International Journal of Electronic Business Management*, Vol. 7, No. 4, pp. 268-277.
38. Milberg, S., Smith, H. J. and Burke, S., 2000, "Information privacy: corporate management and national regulation, *Organization Science*, Vol. 11, No. 1, pp. 35-57.
39. Mitrou, L. and Karyda, M., 2006, "Employees' privacy vs. employers' security: Can they be balanced?" *Telematics and Informatics*, Vol. 25, pp. 164-178.
40. Moshirian, F., 2007. "Financial services and a global single currency," *Journal of Banking and Finance*, Vol. 31, No. 1, pp. 3-9.
41. Open web application security project (OWASP). T10-ArchitectureDiagram 2013. Retrieved October 3, 2013. https://www.owasp.org/index.php/ASVS.
42. Ouedraogo, W. F., Biennier, F. and Ghodous, P., 2013, "Model driven security in a multi-cloud context," *International Journal of Electronic Business Management*, Vol. 11, No. 3, pp. 178-190.
43. Price Waterhouse Coopers, 2012, "The Global State of Information Security Survey 2012," http://www.pwc.com/jg/en/media-article/2012-global-state-of-information-security-survey.jhtml. Retrieved October 17, 2013.
44. Sagiv, L., Schwartz, S. H. and Arieli, S., 2011, Personal values, national culture and organizations: Insights applying the Schwartz value framework, in Ashkanashy, N.M., Wilderom, P.M., Peterson, M.F. (Eds.), The *Handbook of Organizational Culture and Climate*, 2nd ed. Sage, Thousand Oaks, CA, pp. 515-537.
45. Schatz, D., 2008, "Setting priorities in your security program", In H. F. Tipton and K. Krause (Eds), *Information Security Management Handbook*, Taylor & Francis Group, Boca Raton, FL, pp. 93-107.
46. Schmidt, M. B., Johnston, A. C., Arnett, K. P. Chen, J. Q. and Xi'an, S. L., 2008, "A cross-cultural comparison of US and Chinese computer security awareness," *Journal of Global Information Management*, Vol. 16, No. 2, pp. 91-103.
47. Schwartz, S., 2006, "A theory of cultural value orientations: explication and applications," *Comparative Sociology*, Vol. 2, pp. 137–182.
48. Shane, S. A., 1993, "Cultural influences on national rates of innovation," *Journal of Business Venturing*, Vol. 8 No. 1, pp. 59-73.
49. Velmurugan, M. S., 2009, "Security and trust in e-business: problems and prospects," *International Journal of Electronic Business Management*, Vol. 7, No. 3, pp. 151-158.
50. Waarts, E. and van Everdingen, Y., 2005, "The influence of national culture on the adoption status of innovations: an empirical study of firms across Europe," *European Management Journal*, Vol. 25, No. 6, pp. 601-610.

ABOUT THE AUTHOR

Princely Ifinedo is an Associate Professor in the Shannon School of Business at Cape Breton University, Canada. He holds a PhD in Information Systems (IS) from University of Jyväskylä, Finland, an MBA from the Royal Holloway, University of London, UK, a M.Sc. from Tallinn University of Technology, Estonia, a B.Sc. from University of Port-Harcourt, Nigeria, and a Diploma (Educ.) from University of British Columbia, Canada. His research includes ERP Success, Human--Computer Interaction, IS Security Management, IS adoption in businesses and healthcare, E-government, E-business, E-learning, and IS in developing countries and transiting economies. He has presented research at various international IS conferences, contributed chapters to several books/encyclopedias, and published in several reputable journals such as I&M, JCIS, C&S, JSS, DATA BASE, CHB, JOCEC, JITM, IMDS, EIS, IJITDM, ITD, JITM, JGTIM, EG, JISP, and Internet Research. He has authored about 100 peer-reviewed publications. He is affiliated with AIS, ACM, IEEE, ISACA, ASAC, and CIPS.

(Received January 2014, revised March 2014, accepted March 2014)

APPENDIX

Appendix A: Hofstede's cross-cultural dimension scores for countries used in this study

Country	Power Distance (PDI)	Individualism versus Collectivism (IDV)	Masculinity versus Femininity (MAS)	Uncertainty Avoidance (UAI)
Australia	36	90	61	51
New Zeeland	22	79	58	49
Indonesia	78	14	46	48
Malaysia	104	26	50	36
China	80	20	66	40
Philippines	94	32	64	44
Singapore	74	20	48	8
Thailand	64	20	34	64
Japan	54	46	95	92
Bosnia and Herzegovina	76	27	21	88
Belgium	65	75	54	94
Croatia	76	27	21	88
Finland	33	63	26	59
France	68	71	43	86
Germany	35	67	66	65
Greece	60	35	57	112
Luxembourg	40	60	50	70
Slovenia	71	27	19	88
Spain	57	51	42	86
Switzerland	34	68	70	58
South Africa	49	65	63	49
Turkey	66	37	45	85
United Kingdom	35	89	66	35
United States of America	40	91	62	46
Canada	39	80	52	48
Peru	64	16	42	87
Mexico	81	30	69	82
Brazil	69	38	49	76
Colombia	67	13	64	80
Costa Rica	35	15	21	86
Argentina	49	46	56	86
Panama	95	11	44	86
Venezuela	81	12	73	76
Uruguay	61	36	38	100

Appendix B: The results of the multiple regression models

Regression model		Unstandardized coefficients		Standardized	t	Sig.
Model – Issue #1		B	Std. Error	Coefficients (Beta)		
R^2 =0.33	(Constant)	84.858	15.227		5.573	.000
	PDI	.103	.135	.168	.761	.453
	IDV	-.001	.113	-.003	-.011	.991
	MAS	-.189	.119	-.259	-1.590	.123
	UAI	-.298	.087	-.551	-3.434	.002
Model - Issue #2						
R^2 = 0.18	(Constant)	54.020	6.822		7.918	.000
	PDI	.035	.060	.140	.577	.568
	IDV	-.008	.051	-.043	-.167	.869
	MAS	-.113	.053	-.381	-2.124	.042
	UAI	-.020	.039	-.092	-.521	.607
Model - Issue #3						
R^2 = 0.48	(Constant)	16.640	11.734		1.418	.167
	PDI	.084	.104	.157	.804	.428
	IDV	.337	.087	.792	3.860	.001
	MAS	-.271	.092	-.425	-2.958	.006
	UAI	.068	.067	.144	1.018	.317
Model - Issue #5						
R^2 = 0.56	(Constant)	40.968	14.294		2.866	.008
	PDI	.132	.127	.185	1.039	.308
	IDV	.431	.106	.763	4.054	.000
	MAS	-.115	.111	-.136	-1.029	.312
	UAI	-.196	.081	-.312	-2.407	.023
Model - Issue #6						
R^2 = 0.44	(Constant)	31.958	9.973		3.204	.003
	PDI	.060	.088	.137	.680	.502
	IDV	.157	.074	.449	2.118	.043
	MAS	-.031	.078	-.059	-.397	.694
	UAI	-.190	.057	-.488	-3.340	.002

Note: Issue # items are provided in Table 1.