Improving Information Security Training: An Intercultural Perspective

Miloslava Plachkinova, Center for Information Systems and Technology, Claremont Graduate University, CA, USA, miloslava.plachkinova@cgu.edu

Steven Andrés, Center for Information Systems and Technology, Claremont Graduate University, CA, USA, steven.andres@cgu.edu

Abstract

To ensure successful compliance with information security (InfoSec) policy and standards, organisations must harmonise their InfoSec training programmes with the national culture of the local workforce. A successful InfoSec policy must demonstrate the value of security, not just the requirement for security. We conducted a quantitative study of 177 professionals across 35 national cultures to investigate whether national culture influences InfoSec training and best practices using Hofstede's six cultural dimensions. Our findings indicate that training programmes should more directly address the variances in perception of InfoSec across cultures. These training programmes should also reflect the significance of the organisation's InfoSec policies in the context of the local employee, while maintaining unified corporate governance. By increasing training comprehension, organisations can reduce security incidents resulting from unintentional policy violations and, in turn, avoid costly remediation efforts.

Keywords: Information Security, Training, Education, Compliance, National culture, Insider threat, Corporate governance.

1 INTRODUCTION

Increasing globalisation trends (Rugman et al. 2004) and the decreasing costs of technologies and communication (Brynjolfsson et al. 2000) make global expansion a viable solution for many information technology (IT) organisations. It is crucial for companies with multiple worldwide locations to take an intercultural perspective in order to address employee needs and attitudes towards information security (InfoSec) training programmes and compliance with InfoSec best practices. If cultural differences are well understood in advance, the organisation can tailor its security training to increase comprehension and adoption by a global workforce.

While many of the insider threats are intentional, accidental insider security incidents happen more often and could have greater potential for harm than malicious insider attacks (Colwill 2009; Grant 2009). The insider threat is a growing problem in InfoSec, because unlike technical issues which can be resolved in a unified fashion, human behaviour is complex and requires a more specific and individual approach. Crossler et al. (2013) identify the need for more cross-cultural InfoSec behaviour research that goes beyond Western cultures.

Developing sustainable InfoSec training programmes can prevent many insider threats and can add value to global IT services (Olusegun et al. 2013). Prior research has established a strong relationship between InfoSec training and employee compliance with InfoSec best practices (Bulgurcu et al. 2010; Puhakainen et al. 2010; Warkentin et al. 2011). However, many of the existing training programmes make sweeping generalisations and do not focus on employees' local culture. Even with InfoSec training programmes, the number of insider threats is growing (Colwill 2009) which demonstrates the need for a more extensive analysis of the cultural differences in InfoSec training programmes. Providing more insight to this problem can potentially improve the existing educational approach and can minimise the number of unintentional insider threats.

The goal of this study was to establish a relationship between national culture, and employee attitudes towards InfoSec training and best practices. We developed a theoretical model to further investigate these hypothesised connections. We employed an anonymous online survey to test our model and quantitatively collected data from 177 respondents across 35 national cultures.

The results of our study provide several important contributions to Information Systems (IS) research. Specifically, we demonstrate that there is a strong correlation between national culture and attitude towards InfoSec training. The results also confirmed the previously established positive relationship between attitudes towards InfoSec training and best practices. The analysis demonstrates that although national culture is an important aspect in shaping employee perceptions, it is not yet perceived as a major factor in creating successful InfoSec training programmes. Further, our findings suggest that a significant number of employees do not receive any training although their organisation has written InfoSec policies and guidelines.

This study explores the relationship between national culture, InfoSec training programmes and adhering to best practices. We argue that national culture is not taken into consideration when designing InfoSec training programmes which leads to poor outcomes such as a lack of compliance with InfoSec best practices and a growing number of insider threats. We suggest that the insider threat can be minimised if InfoSec training reflects the cultural specifics of the employees, rather than using a more general approach and addressing universal principles. The current paper proposes recommendations to establish sustainable InfoSec training programmes by taking an intercultural approach which explores the attitudes of employees in different cultures.

2 RELATED WORK

In a recent study, Crossler et al. (2013) suggest that one of the biggest issues and limitations of behavioural InfoSec research is that the majority of it has been conducted in Western cultures and that the rest of the world has been overlooked. More specifically, they emphasise the need to examine cross-cultural considerations involved in insider threat behaviour. The current study aims to respond to their call for more rigorous research investigating differences in terms of uncertainty avoidance, collectivism-individualism, and power distance relationships. We take a broader approach and include in our work other dimensions of national culture such as distribution of roles between the genders, control of desires and impulses, as well as long- vs. short-term orientation in the culture. We use the definitions of these six cultural dimensions provided by Hofstede (1984) and Hofstede et al. (2010) to demonstrate their relevancy to the InfoSec context.

2.1 Hofstede's Six Cultural Dimensions

Classifying or measuring national culture is a great challenge, not least in part because it is an entity comprised of various aspects of individual behaviour. In this study we use Hofstede's cultural dimensions to understand how an intercultural approach can be used to improve InfoSec training and compliance with InfoSec best practices. We chose the Hofstede model over others because it encompasses over 30 years of experience and has been used worldwide in cross-cultural training programmes (Hofstede 2010). Furthermore, theory in IS has not taken into account the dimensions of national culture outlined by Hofstede (Bagchi et al. 2004) and the current study responds to the call for a stronger intercultural perspective to IS and InfoSec in particular.

Previous studies have only implicitly addressed some of the cultural dimensions for InfoSec. Zhang et al. (2008) define the *uncertainty avoidance index* (UAI) as the extent to which members of a culture feel threatened by uncertain or unknown situations. More specifically, they use Denmark and Singapore as examples of low uncertainty-avoidance national cultures; whereas Japan is an example of high uncertainty avoidance. If we transfer this concept to an InfoSec context, it suggests that Japanese end-users will be less likely to fall prey to phishing emails due to their uncertainty. Conversely, Singaporean users are less likely to by the uncertainty involved in phishing solicitations.

Another dimension of national culture is *individualism* (IDV) or the loose ties between individuals compared to more collectivistic countries where people are integrated into strong, cohesive groups that protect individuals in exchange for unquestioning loyalty (Zhang et al. 2008). The United States is an example of high individualism in contrast to China that is highly collectivistic. These differences could have an impact on users' InfoSec behaviours. Zhang et al. (2008) suggest that stronger loyalty in collectivistic individuals may lead to stronger adherence to InfoSec policies. However, a negative aspect is that the same person might be less likely to report InfoSec violations of people to whom they are loyal. In individualistic cultures, employees should be more likely to whistle-blow substantial InfoSec violations regardless of existing loyalty and relationships.

Power distance (PDI) is the extent to which the less powerful members of institutions and organisations within a country expect and accept that power is distributed unequally (Zhang et al. 2008). Thus, it is more likely those in high power distance cultures such as China, would more willingly comply with new policy requirements, while those in low power distance cultures such as Canada, may be more likely to question new InfoSec policies.

Another dimension of national culture is *long- and short-term orientation* (LTO) as perceived by Confucian dynamism. Such differences may have a significant impact on how leaders in organisations strategically plan their InfoSec architecture. It would be expected that InfoSec managers with a longer view such as Chinese and Japanese, would engage in more advanced, long-term planning that would focus on a scalable, highly secure architecture and policies for improving InfoSec. Those with a short-term view such as

Americans or Canadians, might have a less broad vision and be more narrowly-oriented towards short-term goals.

National cultures can be also differentiated by a dichotomy of *masculinity vs. femininity* (MAS). To the extent that a culture is feminine, the values of human relationships and concern for others are high. On the other hand, masculine cultures are more assertive and value materialism (Bagchi et al. 2004). We can expect that individuals in masculine cultures such as the US, would be more likely to disobey the InfoSec policies in order to achieve success and demonstrate their superiority, while individuals in feminine cultures such as Denmark, would be more concerned about the consequences of their actions and thus would be less likely to break the rules.

Indulgence vs. restraint (IVR) is a relatively new dimension proposed by Hofstede et al. (2010). Indulgence is a tendency to allow relatively free gratification of basic and natural human desires related to enjoying life and having fun. On the other side, restraint is defined as having less desire. Including this dimension in our study allows us to more precisely explain InfoSec behaviour and to account for some of the variance in employee perceptions. Not surprising, most attacks that are named after their designers also coincide with indulgent societies such as the US. For example, the Kaminsky bug and the Morris worm were both authored by Americans, one of the more indulgent societies (Sample 2013).

2.2 Human Behaviour and the Insider Threat

An insider has the potential to cause more damage to the organisation and has many advantages over an outside attacker: they have legitimate and often privileged access to facilities and information, have knowledge of the organisation and its processes and know the location of critical or valuable assets. It is usually far more cost-effective and quicker for an external threat source to place, or subvert, an insider to exploit vulnerabilities to steal information rather than launch an attack through multiple layers of protection. The situation is further complicated by the increase in the number of third parties given the same privileges as insiders (Colwill 2009). Although these insider threats are typically perceived as individuals with malicious intents, Grant (2009) provide evidence that 52% of insider incidents were accidental (including 6,244 incidents of unintentional data loss). Some examples of accidental damages include:

- Putting the organisation’s network and systems at risk of virus infections and malware;
- Potential lawsuits across a wide range of areas, for example, criminal action, copyright infringement and claims of sexual harassment, racism, bullying or defamation;
- Significant impact on the organisation’s reputation and future revenue.

A significant problem for InfoSec training programmes, standards and policies is a lack of differentiation between accidental and deliberate insider threats. Theoharidou et al. (2005) review the relevance of insider threats to ISO17799 which is a set of recommendations for InfoSec management. However, these guidelines equally treat both types of insider threats. Magklaras et al. (2006) discuss the insider threat in IT infrastructures and provide a taxonomy to predict insider threats but they also fail to take into consideration the difference between accidental and deliberate threats. We argue that some of these accidents can be prevented if employees receive more culturally sensitive training that is tailored to their own needs.

2.3 InfoSec Compliance

InfoSec policy is unlikely to be a successful tool unless organisations adhere to a number of important prescriptions in their policy implementation (Höne et al. 2002). Cultural factors should also be considered in order to design effective InfoSec policies, practices and training programmes in global networks where multiple cultures coexist (Dinev et al. 2009). Considerable efforts by the International Organisation for Standardisation (ISO) and the U.S. National Institute of Standards and Technology (NIST) have focused on developing international InfoSec standards. Yet these standards fail to acknowledge the influence of national culture on employee behaviour.

InfoSec standards and policies are applied to organisations globally, yet compliance is still an individual issue. Bulgurcu et al. (2010) provide evidence that an employee's compliance with stated InfoSec policies is highly influenced by beliefs about the consequences of non-compliance and the employee's attitude toward the policies. As a result, "security practitioners should design their InfoSec awareness programmes so employees' beliefs about intrinsic cost and benefit, safety, and vulnerability are reinforced" (p. 542). Thus, an intercultural perspective to InfoSec training within an organisation can have a positive impact on employee adherence to the InfoSec policy.

Compliance with InfoSec standards and policies is hard because they often times interfere with organisational workflow and may cause an "unacceptable" delay in performing tasks (Hunker et al. 2011). Thus, making compliance easy is critical for any successful effort to constrain insider threats. Compliance becomes more expensive when it gets InfoSec policies closer to the limit of staff tolerance for disruptions to their work and social interactions. A successful InfoSec policy needs to demonstrate to insiders the value of security, not just the requirement for security.

2.4 InfoSec Training

User awareness of security policies and security education and training programmes are among the practices deterring IS misuse (D'Arcy et al. 2009). Employees who comply with the InfoSec rules and regulations of the organisation are key to strengthening InfoSec (Bulgurcu et al. 2010). Thus understanding user attitudes, intentions and behaviour is essential for designing effective technologies and policies (Dinev et al. 2009). These findings correspond to the call for changes in InfoSec education and updates to curricula (Hentea et al. 2006), which can be done through developing multicultural education programmes, as they have a positive impact on learning outcomes and content integration (McGee Banks et al. 1995).

InfoSec training programmes are considered a fundamental part of an organisation's security function (Whitman 2003). As established by prior research (Colwill 2009), employees are the weakest link and pose a more serious threat than outsiders. Thus, raising employee awareness to InfoSec risks (D'Arcy et al. 2009) and ensuring compliance with policies and regulations is central to providing effective information security (Bulgurcu et al. 2010; Dinev et al. 2009). The current study is further motivated by the need of improving InfoSec policy compliance training identified by Puhakainen et al. (2010). The researchers demonstrate how employee noncompliance with InfoSec policies has become a key concern for organisations and focus on training is the most commonly suggested approach to solving this problem.

3 THEORETICAL MODEL

We develop a theoretical model (Figure 1) to explore if there is a relationship between national culture as expressed by Hofstede's six cultural dimensions and employee attitudes towards InfoSec training and best practices defined by global security standards and policies.

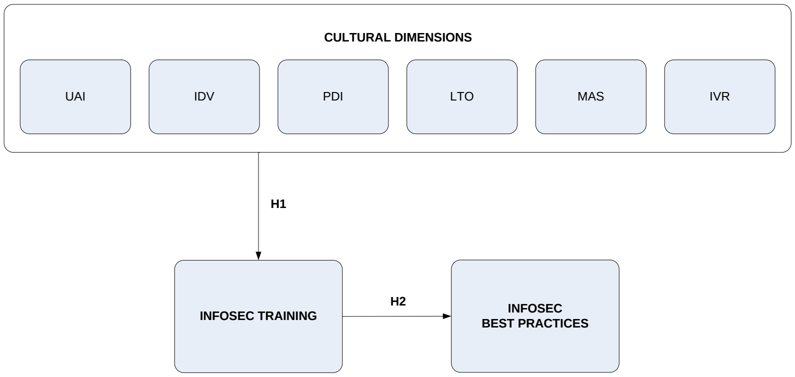

Figure 1. Theoretical Model

With the increasing number of sophisticated cyber-attacks and the decreasing cost of exploits (Choo 2011), it is inevitable that every organisation is a potential target. Employees are the weakest link (Sasse et al. 2001) and as “insiders” they pose substantial threat by virtue of their knowledge their ability to bypass existing security measures through legitimate means (Randazzo et al. 2005). Raising employee awareness to InfoSec risks (D'Arcy et al. 2009) and unintentional insider threats of data loss or corruption (Colwill 2009) through training is a fundamental part of an organisation’s security function (Whitman 2003). National culture has substantial significance in global information systems (Ein-Dor et al. 1993). Therefore, we expect to find that national culture, as measured by Hofstede’s six cultural dimensions, is related to InfoSec training programmes.

H1: *National culture exerts is related to InfoSec training programmes.*

Central to providing effective InfoSec is ensuring compliance with global security standards and policies, otherwise known as InfoSec best practices (Bulgurcu et al. 2010; Dinev et al. 2009). Training programmes that highlight the need of using best practices can significantly reduce the risk of data breach or theft (Liginlal et al. 2009) from unintentional insider threats and intentionally hostile outsiders. Successful InfoSec best practices should be able to demonstrate to insiders the importance and necessity of security measures and not just require individuals to blindly obey them (Hunker et al. 2011). Compliance with best practices is difficult to assess in a quantitative research study, but attitudes towards best practices can be more easily measured. We expect to find that InfoSec training affects attitudes towards best practices as a proxy for compliance:

H2: *Training programmes affect attitudes towards InfoSec best practices.*

4 METHODOLOGY

4.1 Study Design

We performed a quantitative study using an anonymous online survey. Our sampling frame consisted of global IT workers within multinational organisations. Since most strategic IT leaders are suspicious of clicking URLs from an unfamiliar source (Hall et al. 2011), we used two different approaches. First, we targeted Top 100 global IT services companies.[1] We successfully sent FAX letters to 80% of the corporate headquarters and 53% of the 521 remote offices. In total 1,382 FAX transmissions were attempted across 648 unique numbers, resulting in 359 successful deliveries across 60 countries. Second, we used the directory of ISACA chapters (an international professional association focused on IT governance) and reached out to 95 of the chapter presidents across the globe.[2] We applied the snowball method, asking the chapter presidents to send out the survey to their members. Due to the anonymous nature of the survey and the technique we used to recruit participants, we were not able to obtain a response rate for the ISACA members. We provided incentives for participation in the survey.

To increase the internal validity of the constructs, the survey included filter questions and displayed answers to some of the questions in a randomised order. We adapted some of the measures developed by Chang and King (2003) to design our survey questions and followed construct validity procedures suggested by Moody et al. (2011). We performed a pilot test of the survey with 19 graduate students at a large public university in the western US. Additionally, we conducted three interviews to obtain feedback and suggestions for improvement: one with an expert in organisational psychology and two InfoSec officers of large multinational IT organisations.

[1] http://www.softwaretop100.org/global-software-top-100-edition-2011 (retrieved 21 Nov 2014).

[2] http://www.isaca.org/Membership/Local-Chapter-Information/Pages/Chapter-world-map.aspx (retrieved 21 Nov 2014)

4.2 Measures

4.2.1 Dependent Variables

We used IS success measures developed by DeLone & McLean (2003) to assess employee attitude towards the delivery of InfoSec training programmes and best practices, as derived from global security standards and policies. We only employed those measures that were relevant to InfoSec. Specifically, we conceptualised attitude towards best practices in terms of: understandability, accuracy, relevancy, applicability, clarity, believability, effectiveness and importance; and training programmes in terms of: understandability, accuracy, relevancy, applicability, clarity, believability, effectiveness, usefulness, value, and sufficiency.

These attributes were measured on a 4-point Likert scale. An even-numbered scale was selected to require respondents to provide a more useful non-neutral response to questions posed. An even scale was suggested in prior literature as a suitable measure to force participants to come down on one side of the central point (Boice et al. 1997). Further, answering the questions was optional and respondents were free to skip a question or withdraw from the survey at any time.

4.2.2 Independent Variables

Cultural dimensions for each participant's country were obtained from The Hofstede Center[3] using the year 2010 data set. In some cases, particular indexes were missing data for certain countries. In those instances, we referred to data from earlier studies, if available. Since long- vs. short-term orientation and indulgence vs. restraint were later added to Hofstede's typology, some of the participants' countries in this study do not have scores on those dimensions yet (Ifinedo 2014). In those instances we approximated the data based on geographically similar countries for which the scores were available.

4.2.3 Control Variables

Additionally, respondents were asked to identify their age, gender, years of education, position within the organisation, functional job area, and years of experience within the IT industry. These values were identified as control variables to ensure that the data we obtain is free from any age or gender bias and is applicable to inexperienced as well as veterans of the industry.

5 ANALYSIS AND RESULTS

A total of 197 respondents participated in the online survey. Twenty of the subjects were removed from the pool due to missing data, resulting in a final dataset sample of 177 participants across 35 national cultures. Four of the countries (Bulgaria, India, Uganda and the US) represent 64.4% of the responses. However, these four countries are located each on a different continent and they differ greatly in terms of culture as measured by Hofstede's cultural dimensions. Thus, they can be treated as sufficiently representative to test our model.

Table 1 presents the number of respondents and the independent variable data for each country. High PDI scores indicate more inequality in the power distribution. High IDV scores suggest more independence among members of the society. High UAI scores indicate less tolerance for uncertainty and ambiguity. High MAS scores indicate that the society will be driven by competition, achievement and success. A low MAS score means that the dominant values in society are caring for others and quality of life. High IVR scores mean people do not have the perception that their actions are restrained by social norms and there is

[3] http://geert-hofstede.com/countries.html (retrieved 21 Nov 2014).

significant emphasis on leisure time. High LTO scores indicate fostering of virtues oriented towards future rewards.

Country	**N**	**%**	**PDI**	**UAI**	**IDV**	**MAS**	**LTO**	**IVR**
Algeria	1	.6	80	68	38	26	32	36
Australia	3	1.7	51	90	61	21	71	71
Austria	2	1.1	70	55	79	60	63	63
Benin	1	.6	29	54	20	46	16	84
Bosnia and Herzegovina	1	.6	86	92	25	43	16	28
Brazil	1	.6	76	38	49	44	59	59
Bulgaria	34	19.2	41	85	30	40	69	16
China	2	1.1	40	30	20	66	87	24
Croatia	1	.6	80	33	40	58	33	33
Czech Republic	1	.6	74	58	57	70	29	29
Ecuador	2	1.1	67	8	63	63	65	97
Germany	5	2.8	65	67	66	83	40	40
Greece	1	.6	100	35	57	45	50	50
Hungary	1	.6	82	80	88	58	31	31
India	34	19.2	40	48	56	51	26	26
Iran	4	2.3	59	41	43	14	40	40
Ireland	5	2.8	35	70	68	24	65	65
Israel	4	2.3	81	54	47	38	45	52
Italy	2	1.1	75	76	70	61	30	30
Japan	1	.6	92	46	95	88	42	42
Kenya	2	1.1	50	25	60	60	25	84
Malaysia	1	.6	36	26	50	41	57	57
Namibia	1	.6	65	45	30	40	25	84
Netherlands	2	1.1	53	80	14	67	68	68
Pakistan	1	.6	70	14	50	50	40	40
Romania	2	1.1	90	30	42	52	20	20
Saudi Arabia	1	.6	80	68	38	36	52	52
Serbia	2	1.1	92	25	43	52	28	28
Singapore	2	1.1	8	20	48	72	46	46
Switzerland	1	.6	58	68	70	74	66	66
Uganda	12	6.8	38	56	30	57	20	84
United Kingdom	4	2.3	35	89	66	25	69	69
USA	34	19.2	46	91	62	26	68	68
Venezuela	5	2.8	76	12	73	16	100	100
Vietnam	1	.6	30	20	40	57	35	35

Table 1. Descriptive Statistics for Participant Cultures

The majority of our respondents (79%) were male and possessed either a four-year college (22%) or Master’s degree (49%). The majority of the survey respondents had a job role related to Computers & IS (54%), at a management- (41%) or professional-level (43%), with 5-19 years (55%) of experience in the IT industry.

All reflective survey items were entered into a confirmatory factor analysis. From this, only factors with an eigenvalue equal or greater to 1.0 were retained. Results were then rotated using Varimax rotation to ascertain the loadings of each indicator on its respective construct. Only highly loaded items were used in construct calculation (i.e., > .70, representing that over 50% of the variance was captured for the indicator in the rotation).

Based on these factor groupings, the Cronbach's Alpha scores for InfoSec best practices and InfoSec training were obtained to demonstrate construct validity (Table 2). Due to page limitations. measurement items and raw data are available upon request.

Grouping	Subconstructs	Cronbach's Alpha
InfoSec Training	Value Applicability Effectiveness Accuracy Clarity Understandability Sufficiency Believability Usefulness	.947
InfoSec Best Practices	Understandability Accuracy Relevancy Applicability Clarity Believability Effectiveness	.914

Table 2. Factor Analysis

Then we investigated the correlation between each of the six cultural dimensions to demonstrate their relationship and to justify the computation and use of a single variable ("Culture") in our theoretical model (Table 3). This concept is based on Hofstede's previous studies on national culture (Hofstede 1984; Hofstede 2010; Hofstede et al. 2010).

		PDI	UAI	IDV	MAS	LTO	IVR
PDI	Pearson Correlation	1					
	Sig. (2-tailed)						
	N	177					
UAI	Pearson Correlation	-.429**	1				
	Sig. (2-tailed)	.000					
	N	177	177				
IDV	Pearson Correlation	-.245**	.333**	1			
	Sig. (2-tailed)	.001	.000				
	N	177	177	177			
MAS	Pearson Correlation	.350**	-.559**	-.381**	1		
	Sig. (2-tailed)	.000	.000	.000			
	N	177	177	177	177		
LTO	Pearson Correlation	-.252**	.536**	.604**	-.741**	1	
	Sig. (2-tailed)	.001	.000	.000	.000		
	N	177	177	177	177	177	
IVR	Pearson Correlation	-.390**	.437**	.227**	-.578**	.722**	1
	Sig. (2-tailed)	.000	.000	.002	.000	.000	
	N	177	177	177	177	177	177

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

Table 3. Correlation Matrix of Hofstede's Cultural Dimensions

Next, we investigated the correlation between the new computed variable Culture and InfoSec Training and Best Practices based on the items suggested in the factor analysis. This was important in order to establish the relationships and test our theoretical model (Table 4).

		Culture	**InfoSec Training**	**InfoSec Best Practices**
Culture	Pearson Correlation	1		
	Sig. (2-tailed)			
	N	177		
InfoSec Training	Pearson Correlation	.350**	1	
	Sig. (2-tailed)	.001		
	N	89	89	
InfoSec Best Practices	Pearson Correlation	.216*	.705**	1
	Sig. (2-tailed)	.021	.000	
	N	114	81	114

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

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

Table 4. Correlation Matrix of Culture, InfoSec Training and Best Practices

We performed a regression analysis to test our two hypotheses. Such an analysis is suitable to measure how well the data we collected fits the proposed theoretical model. The results indicate that Hofstede's six cultural dimensions explain 18% of the variance in InfoSec training attitudes ($R^2 = 0.180$) and InfoSec Training attitudes explain about 50% of the variance in attitudes towards InfoSec Best Practices ($R^2 = 0.497$).

6 DISCUSSION

6.1 Findings

The primary goal of this study was to determine whether national culture has influence on InfoSec training programmes. We found and measured several variables with differing levels of significance. Our data indicate that national culture, although significantly correlated to InfoSec training, can only partially explain the variance in training programmes. InfoSec training programmes, however, are significantly correlated and explain about half of the variance in attitudes towards InfoSec best practices. Figure 2 demonstrates our results:

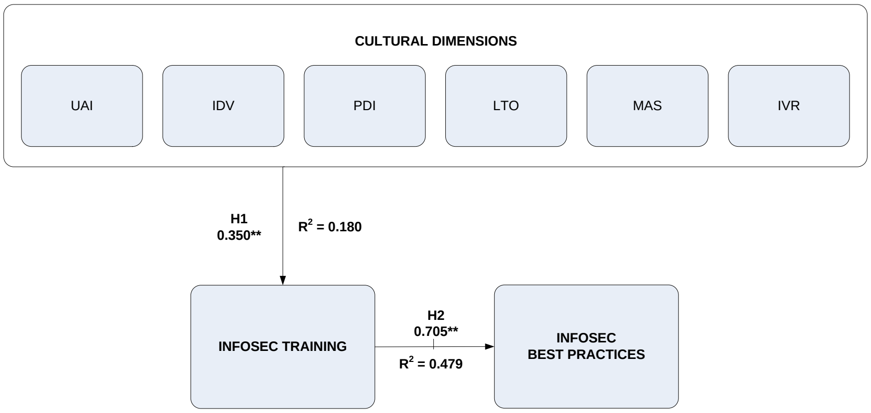

Figure 2. Results

We found partial support for H1. National culture is significantly correlated with InfoSec training. However, it explains about 18% of the variance in employee attitudes towards InfoSec training. This finding presents an opportunity for organisations to revise their education programmes to be more culturally sensitive in the delivery of InfoSec concepts. Further, the relatively low R^2 value can be explained by the fact that currently most training programmes are focused on ensuring compliance for global InfoSec standards. As such, they allow very little variation in the content and educational methods of delivery. However, such a unified training approach does not seem to be very successful if we consider the growing number of unintentional insider threats (Colwill 2009).

We found support for H2, with training being highly correlated to InfoSec best practices and explaining nearly half of the effect upon attitudes towards best practices. This result indicates that employees who receive more training are more likely to have positive attitudes towards best practices. Our finding is consistent with previous studies (Bulgurcu et al. 2010; D'Arcy et al. 2009; Dinev et al. 2009) and confirms the positive influence of training programmes on InfoSec. Our research extends these past studies, as our results are based on a large sample of data obtained from a highly diverse population across the world. The cultural dimensions do not directly affect following InfoSec best practices as those are usually based on international standards and allow for little modification on a local level. Adherence to such standards may be more related to personal characteristics rather than nationwide perceptions.

Another finding was that 64.40% of the respondents indicated their organisation had a written InfoSec policy or guidelines and of those only 70.05% admitted to have attended some form of InfoSec training provided by their current employer. This alarming trend suggests a major disconnect between training programmes and compliance with standards and best practices. Employees often lack motivation to follow InfoSec best practices and knowledge of InfoSec risks and how they can handle these risks (Albrechtsen 2007). Thus, the lack of InfoSec training can further increase the possibility of unintentional insider threats and create a significant vulnerability in the organisation’s security.

These findings demonstrate that training programmes are ignoring the very real differences in InfoSec perception from each national culture. These localised variances of best practices could produce greater appreciation for the concepts and improved attitudes. For example, in cultures that are more collectivistic, the threats and risks associated with sharing passwords should be explained differently to counteract the innate predilection to share information in collectivistic societies. Additionally, these results suggest a potential problem in organisations that have a bring-your-own-device (BYOD) policy, as malware could migrate from the personal device into the company’s machines and over the company’s networks (Miller et al. 2012). Our results also support the calls for changes in InfoSec education (Hentea et al. 2006) and for adopting different approaches to teaching InfoSec (Yurcik et al. 2001).

6.2 Implications for Practice

Our results suggest there is untapped potential for improving InfoSec training programmes to create more positive attitudes towards best practices. Although national and international standards on InfoSec exist, individuals in different countries perceive these standards differently. InfoSec best practices can and should be explained in a culturally sensitive manner, tuned to each local population.

Global citizens react differently to InfoSec awareness training due to differing cultures (Chen et al. 2008). If national culture is used as a prism (Figure 3) through which to describe one set of policies and IT controls in place to protect the organisation and its employees, a higher level of comprehension and relevance can be attained. With more effective training programmes, organisations may decrease policy violations caused by unintentional insider threats and avoid costly remediation efforts.

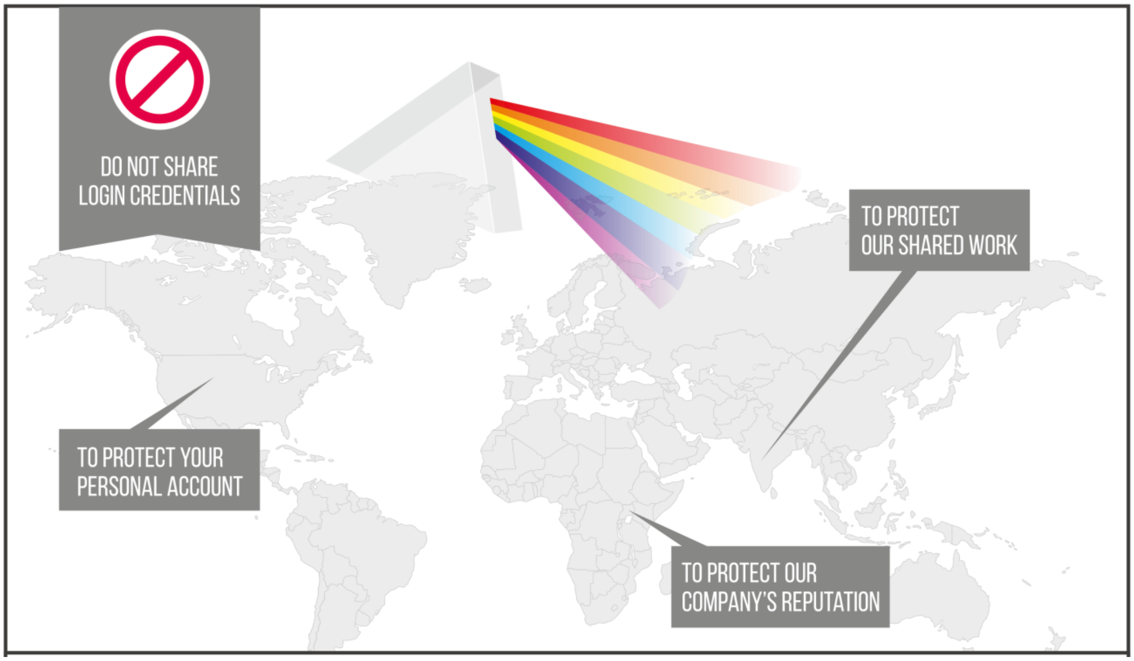

Figure 3. Culturally Sensitive Prism in InfoSec Training Programmes

6.3 Future Research and Limitations

The current study is the first step towards gaining a better understanding of the influence of national culture on InfoSec. Our next goal would be to conduct qualitative analysis and gain a deeper and more meaningful perception of employee attitudes towards InfoSec training and compliance with best practices. Such a qualitative study can answer the question: “How does culture influence InfoSec training?” which would explain in further detail the impact of national culture on attitude towards InfoSec training and perception of implementing best practices. As an exploratory study of such a broad topic, our first step was to demonstrate a correlation between the different variables and our future research will focus on explaining how the motivations of participants are determined by national culture.

We encourage others to do further research and expand upon our work. By its nature, survey respondents were those that valued research in InfoSec concepts and thus could colour the data provided, especially in instances when there was only a single participant to represent an entire country. With a more inclusive study of all workers within one global IT organisation, a stronger influence of national culture might be observed.

In this study we rely on the participants to self-identify with a single national culture. However, a person can have a multicultural background and this implication should also be taken into account when developing training programmes. The use of Reinecke & Bernstein’s (2013) algorithm to approximate individuals’ cultural backgrounds can be a good starting point for such a process.

Training programmes can employ greater cultural intelligence by working with local offices to culturally translate InfoSec concepts into easily accessible contexts. Beyond the modification of consequences of deviating from best practices, training should concentrate on motivations behind practices, to encourage greater acceptance from the target population. We encourage others to perform double-blind testing where an organisation provides culturally sensitive InfoSec training to one group while a control group receives the standard training. By measuring the number of security incidents in both groups over the course of several years, future researchers may confirm the benefits of an intercultural perspective to InfoSec training.

7 CONCLUSIONS

Global InfoSec standards and policies exist in an idealised vacuum, apart from the realities of national culture and its influence on attitudes towards best practices. This paper explores whether culture is related to InfoSec programmes and, in turn, if those programmes influence attitudes towards best practices. Our results suggest that national culture is important and highly correlated with InfoSec training but it is not well understood and properly implemented by InfoSec managers and experts. Further, lack of proper training or any training at all can potentially lead to noncompliance and an increase in unintentional insider threats. We aim to shed more light into these issues and raise awareness of the current methods for training delivery.

This study contributes to literature in several aspects. First, we offer an intercultural perspective to InfoSec. Although prior research has addressed this factor, ours is the first study to include a comprehensive list of all six of Hofstede's cultural dimensions. We demonstrate the importance of understanding cross-cultural issues in InfoSec, as they directly influence training delivery and impact policy compliance. Second, unlike previous research, we do not rely on data predominantly from Western cultures. In fact, over 2/3 of our data are collected from cultures other than Western. This is a response to a previous call on taking a more diverse approach to InfoSec (Crossler et al. 2013). Third, this study offers a possible explanation for the current phenomenon of the growing unintentional insider threats in spite of the increased InfoSec training provided to employees (Colwill 2009). We demonstrate the need to change the educational approach and develop more culturally sensitive training in order to limit the accidental damages. And lastly, the study offers some practical implications which can be addressed by InfoSec experts. We outline some actions which can help to tailor the existing InfoSec training programmes to meet the real needs of the employees in multinational organisations. In an interconnected world with an increasingly global workforce, culturally sensitive InfoSec training programmes can help overcome cross-cultural barriers in InfoSec through harmonisation of local cultural dimensions and worldwide corporate governance.

References

Albrechtsen, E. (2007). "A qualitative study of users' view on information security," *Computers & security* (26:4), pp 276-289.

Bagchi, K., Hart, P., and Peterson, M. F. (2004). "National culture and information technology product adoption," *Journal of Global Information Technology Management* (7:4), pp 29-46.

Boice, D. F., and Kleiner, B. H. (1997). "Designing effective performance appraisal systems," *Work Study* (46:6), pp 197-201.

Brynjolfsson, E., and Hitt, L. M. (2000). "Beyond computation: Information technology, organizational transformation and business performance," *The Journal of Economic Perspectives*), pp 23-48.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. (2010). "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *MIS Quarterly* (34:3).

Chang, J. C.-J., and King, W. R. (2003). "Measuring the performance of information systems: a functional scorecard," *Journal of Management Information Systems* (22:1), pp 85-115.

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

Choo, K.-K. R. (2011). "The cyber threat landscape: Challenges and future research directions," *Computers & Security* (30:8), pp 719-731.

Colwill, C. (2009). "Human factors in information security: The insider threat–Who can you trust these days?," *Information security technical report* (14:4), pp 186-196.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., and Baskerville, R. (2013). "Future directions for behavioral information security research," *computers & security* (32), pp 90-101.

D'Arcy, J., Hovav, A., and Galletta, D. (2009). "User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach," *Information Systems Research* (20:1), pp 79-98.

Delone, W. H., and McLean, E. R. (2003). "The DeLone and McLean model of information systems success: a ten-year update," *Journal of Management Information Systems* (19:4), pp 9-30.

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* (19:4), pp 391-412.

Ein-Dor, P., Segev, E., and Orgad, M. (1993). "The effect of national culture on IS: Implications for international information systems," *Journal of Global Information Management (JGIM)* (1:1), pp 33-44.

Grant, I. (2009). "Insiders cause most IT security breaches, study reveals," ComputerWeekly.

Hall, J. H., Sarkani, S., and Mazzuchi, T. A. 2011. "Impacts of organizational capabilities in information security," *Information Management & Computer Security* (19:3), pp 155-176.

Hentea, M., Dhillon, H. S., and Dhillon, M. (2006). "Towards changes in information security education," *Journal of Information Technology Education* (5), pp 221-233.

Hofstede, G. (1984). *Culture's consequences: International differences in work-related values*, (sage.

Hofstede, G. (2010). "The GLOBE debate: Back to relevance," *Journal of International Business Studies* (41:8), pp 1339-1346.

Hofstede, G., Hofstede, G. J., and Minkov, M. (2010). *Cultures and organizations: Software of the mind*, (McGraw-Hill London).

Höne, K., and Eloff, J. (2002). "What makes an effective information security policy?," *Network Security* (2002:6), pp 14-16.

Hunker, J., and Probst, C. W. (2011). "Insiders and insider threats—an overview of definitions and mitigation techniques," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications* (2:1), pp 4-27.

Ifinedo, P. (2014). "The effects of national culture on the assessment of information security threats and controls in financial services industry," *International Journal of Electronic Business* (12:2), pp 75-89.

Liginlal, D., Sim, I., and Khansa, L. 2009. "How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management," *computers & security* (28:3), pp 215-228.

Magklaras, G., Furnell, S., and Brooke, P. J. (2006). "Towards an insider threat prediction specification language," *Information management & computer security* (14:4), pp 361-381.

McGee Banks, C. A., and Banks, J. A. (1995). "Equity pedagogy: An essential component of multicultural education," *Theory into practice* (34:3), pp 152-158.

Miller, K. W., Voas, J., and Hurlburt, G. F. (2012). "BYOD: security and privacy considerations," *It Professional* (14:5), pp 0053-0055.

Moody, G., Galletta, D., Walker, J., and Dunn, B. 2011. "Which Phish Get Caught? An Exploratory Study of Individual Susceptibility to Phishing," ICIS 2011 Proceedings.

Olusegun, O. J., and Ithnin, N. B. (2013). "People are the answer to security: Establishing a Sustainable Information Security Awareness Training (ISAT) program in organization," *arXiv preprint arXiv:1309.0188*).

Puhakainen, P., and Siponen, M. (2010). "Improving employees' compliance through information systems security training: an action research study," *MIS Quarterly* (34:4), pp 757-778.

Randazzo, M. R., Keeney, M., Kowalski, E., Cappelli, D., and Moore, A. (2005). "Insider threat study: Illicit cyber activity in the banking and finance sector," DTIC Document.

Reinecke, K., and Bernstein, A. (2013). "Knowing What a User Likes: A Design Science Approach to Interfaces that Automatically Adapt to Culture," *MIS Quarterly* (37:2).

Rugman, A. M., and Verbeke, A. (2004). "A perspective on regional and global strategies of multinational enterprises," *Journal of International Business Studies* (35:1), pp 3-18.

Sample, C. (2013). "Applicability of Cultural Markers in Computer Network Attack Attribution," Proceedings of the 12th European Conference on Information Warfare and Security, pp. 11-12.

Sasse, M. A., Brostoff, S., and Weirich, D. (2001). "Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security," *BT technology journal* (19:3), pp 122-131.

Theoharidou, M., Kokolakis, S., Karyda, M., and Kiountouzis, E. 2005. "The insider threat to information systems and the effectiveness of ISO17799," *Computers & Security* (24:6), pp 472-484.

Warkentin, M., Johnston, A. C., and Shropshire, J. (2011). "The influence of the informal social learning environment on information privacy policy compliance efficacy and intention," *European Journal of Information Systems* (20:3), pp 267-284.

Whitman, M. E. (2003). "Enemy at the gate: threats to information security," *Communications of the ACM* (46:8), pp 91-95.

Yurcik, W., and Doss, D. (2001). "Different approaches in the teaching of information systems security," Proceedings of the Information Systems Education Conference.

Zhang, D., and Lowry, P. B. (2008). "Issues, limitations, and opportunities in cross-cultural research on collaborative software in information systems," *Journal of Global Information Management (JGIM)* (16:1), pp 61-84.