Association for Information Systems
AIS Electronic Library (AISeL)

ACIS 2009 Proceedings | Australasian (ACIS)

12-2009

An Investigation of the Impact of Corporate Culture on Employee Information Systems Security Behaviour

Brydie McCoy
School of Information Systems, Technology & Management, University of New South Wales, b.mccoy@unsw.edu.au

Greg Stephens
School of Information Systems, Technology & Management, University of New South Wales, g.stephens@unsw.edu.au

Kenneth J. Stevens
School of Information Systems, Technology & Management, University of New South Wales, k.stevens@unsw.edu.au

An Investigation of the Impact of Corporate Culture on Employee Information Systems Security Behaviour

Brydie McCoy
School of Information Systems, Technology & Management
University of New South Wales

Greg Stephens
School of Information Systems, Technology & Management
University of New South Wales
g.stephens@unsw.edu.au

Kenneth J Stevens
School of Information Systems, Technology & Management
University of New South Wales
k.stevens@unsw.edu.au

Abstract

Information security poses a variety of challenges for any organisation. One such challenge, though often overlooked, is that of the threat posed by users. Whilst a variety of methods are available to control this, none have been particularly successful. An alternative suggested in the literature is the use of organisational culture via corporate governance to improve the security behaviours of individuals (Thomson & von Solms, 2005; von Solms & von Solms, 2004; Mishra & Dhillon, 2006). At the core of these alternative theories is the assumption that culture affects information security, though no literature could be found that tests this relationship. Previous research into the effects of organisational culture on other aspects of an organisation has lead to uncertainty as to the existence of such a relationship, and therefore it needs to be evaluated before these theories can be tested or further utilised. The purpose of this study is twofold, viz, to test the relationship between organisational culture and information security behaviour, and to test the viability of using the Partial Least Squares (PLS) method advocated by Chin & Newstead (1999) for this type of research. A model was developed to represent information security attitudes, which, combined with Hofstede's (1990) model of culture, was used to develop the survey. The model and survey were piloted via interview in the organisations. The results lead us to question the existence of a relationship between organisational culture and information security attitudes.

Keywords

Information security, organization culture, PLS, user attitudes, IT governance

OVERVIEW

Information systems security is a key concern in many organizations. One challenge often overlooked in both academe and practice is the role of users' in IS security (Stanton et al., 2004). The Users' involvement in security is seen to create vulnerabilities in an organisations' IS security, which can never be truly eliminated by technical controls (Besnard & Arief, 2004). A variety of methods, including training and education, have been adopted to address the problems of user involvement, but with limited success (Stanton et al., 2004). In response to these problems, it has been suggested that corporate governance should take responsibility for information security, using the informal component of governance to address the 'user issue' in security (Mishra & Dhillon, 2006), through means such as organisational culture (Thomson & von Solms, 2005, von Solms & von Solms, 2004, Mishra and Dhillon, 2006).

Thomson and von Solms (2005) high level model outlines the theorised relationship between Information Systems Security, Corporate Governance and Corporate Culture, as set out in Figure 1 below.

Relationship A (information security/corporate governance) signifies the role governance should take in information security involving the more formal controls such as security policies. Relationship B (culture/information security), suggests that individual behaviours may be instilled through organisational culture, ensuring acceptable behaviours becomes common practice. Relationship C is the proposed extra step required by organisations, attempting to affect organisational culture to ensure that the desired behaviours and values are adopted by employees. Relationship D is defined as 'information security obedience', signifying that only when each of these factors align and support each other can there be successful information security.

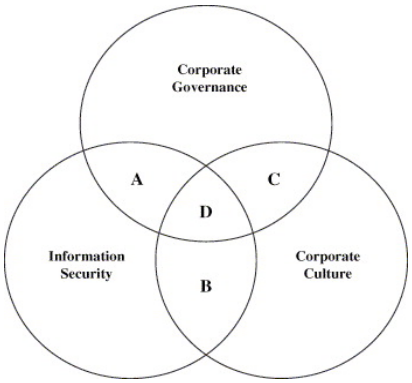

Figure 24: Interactions of the concepts, Thomson & von Solms (2005)

The relationship between culture and various aspects of organisations have been researched in considerable depth, across areas such as financial performance, marketing, customer service, employee satisfaction (Leidner & Kayworth, 2006). Culture has also been used within the field of information technology to explain the contradictory consequences of IT within firms, system methodologies and design, IS development and cultures influence on use and adoption. A review of culture in information systems by Leidner & Kayworth (2006) highlights that information flows and information technologies are often closely intertwined with culture and that IT is symbolic and therefore subject to the various cultural interpretations of those using it. However, the studies that these observations have been based upon have yielded mixed results and received a lot of criticism (Martin, 2002).

In general terms, research involving culture and organization typically proposes various cultural traits which a firm needs in order to gain improvements in the areas under consideration. Attempts by firms to implement these findings have met with limited success (Ogbonna & Harris, 2002, as cited in Buchanan & Huczynzki, 2004 p662). A review of these studies found that there was an emphasis on purely anecdotal evidence and the use of "dubious research methodologies" which linked qualitative beliefs with an organisation's performance and attributed any superior results to the cultural beliefs, without reference to the market or other environmental variables (Thompson & McHugh, 2002, as cited in Buchanan and Huczynski, 2004, p662 and Anonymous reviewer in Martin, 2002 p244), suggesting that this relationship simply cannot be assumed to exist, and is in need of further investigation.

Using a model of the interaction between information system and organization culture based on the models of Thompson and von Solms (2005) and Hofstede's (1990), a survey instrument was developed and administered to two cohorts of users across two organizations. The collected data was analysed using PLS, and the results find little in the way of a relationship between organizational culture and users' attitude towards information security, suggesting that the assumptions made about the existence of this relationship are, in fact, ill founded.

The outcomes of this research are useful to organizations seeking to improve user attitudes towards information security and better direct their IS security efforts. It assists organizations, as the greater the understanding of the influences on individuals' attitudes and behaviours towards information security, the more can be done to find appropriate tools to improve them and reduce the risk of this vulnerability in organisations.

RESEARCH FRAMEWORK AND QUESTIONS

The model proposed by Thomson and von Solms (2005) only depicts the various interactions of the concepts. To analyse the relationships, the model (Figure 1) has been re-factored to show the direct influences between the components based on the comments from the literature. Note that organisational culture, despite being able to be influenced by governance, can also influence governance.

Thomson and von Solms claim that good information security behaviours should be instilled through culture. However, there is little evidence that what is being proposed in these theories is possible. Previous research into the influence of culture has produced mixed results. This leads to scepticism over the existence of the relationship between organisational culture and information security attitudes which underlie these theories. This study seeks to examine this relationship.

To analyse this relationship a further decomposition of the model is required. Information security has been divided into two separate constructs: security attitudes and security behaviours. Culture is said to be the

backbone of peoples' values and beliefs and therefore will influence individual's attitudes without necessarily having direct effect on peoples' behaviours. Governance, on the other hand, is more inclined to have a direct impact on peoples' behaviours and only portrays an indirect link to attitudes via culture and behaviour as depicted in Figure 2. As highlighted by Thomson and von Solms (2005), governance influences security behaviours by means of implementing and gaining compliance to security policies.

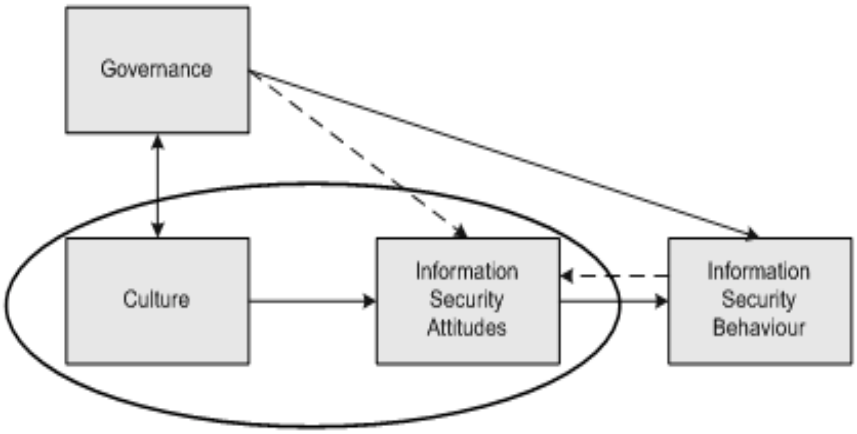

Figure 25: Conceptual Model

The last relationship, between culture and security attitudes is the one with lies at the foundations of the governance relationship proposed in the literature. Theoretically, culture will shape peoples' beliefs and values hence influencing their attitudes. It is believed that personal preferences are not restrained by systems of formal rules, authority and norms of rational behaviour but are instead controlled by cultural norms and values beliefs and assumptions (Ott, 1989). According to this theory, governance should not have a direct link to security attitudes with the influence, instead, being via culture. However, what kind of impact culture will have, on individual security attitudes, is unknown and uncertain and thus the relationship addressed by the proposed research question.

This research will therefore focus on the two components of this relationship: organisational culture and security attitudes. An analysis of the relationship depicted in the model is required to answer the specific research question:

Research Question: *Does organisational culture impact employees' attitudes to information security?*

Of key concern in answering this research question, and hence being able to conduct the study, is the ability to adequately operationalise the key constructs of 'organization culture' and 'employee attitude', as these have proven difficult to adequately define and measure in the past. However, as it demonstrated in the sub-sections below, both can be adequately operationalised.

Operationalising Organisational Culture

Culture generally refers to patterns of human activity and the symbolic structures that give such activities significance and importance. Organisational Culture is that culture belonging to the collective of the organisation.

Hofstede (1990) argued that organisational culture was measurable quantitatively and established a set of dimensions for which it could be measure and that values are the more stable element of culture so comparative research of culture presumes the measurement of values. He also notes however, that inferring values from people's actions only, is cumbersome and ambiguous. His research concluded that in organisations, it is the practices, rather than the values, that tend to vary the most. Van den Berg & Wilderom (2004) use this argument to compare practices among the organisations they studied and argue that values are not directly visible to employees. Hofstede (1990) found practices divided as follows:

- Process versus Results orientated - Companies can either be concerned with the means to reaching the goals or achieving the goals themselves.
- Employee versus Job - Organisations can either be focused on their employees or focused on getting the job done.

- Parochial versus professional - Employees can derive identity from the organisation or their particular role.
- Open versus closed - Organisation and people are open to newcomers and outsiders and almost anyone would fit in to the organisation or otherwise
- Loose versus tight control - This refers to the internal structuring of the organisation
- Normative versus pragmatic - Customer orientation is either market driven or rule driven. For example, it may be appropriate to break the rules of the company if it means making a customer happy.

Hofstede's dimensions have enjoyed considerable usage and success in Information Systems research and, as such, were adopted in this study.

Operationalising Information Security Attitudes

There is no universally accepted definition of 'attitudes', however, most researchers agree on certain constructs. Attitude can be seen to be made up of three components: cognitive, affective and behavioural, where the cognitive component can be described as an individual's ideas, thoughts, perceptions, beliefs, opinions or mental conceptualisations of the referent (Findler, Vilchinsky, and Werner, 2007). The affective component is said to reflect the emotional underpinnings of an attitude. The behavioural component relates to the individuals' intent or willingness to behave in a certain manner.

To measure information security attitudes a list of independent dimensions was required. These dimensions of attitudes can then be used to compare the dimensions of culture so to better identify any relationships between the two constructs. Some dimensions may be found to be affected by culture while others are not. No research was identified that addressed the measurement of attitudes towards information security so a model was developed from the literature. The following seven dimensions were identified:

- Understanding of how important security is
- Chance of a security incident occurring
- How bad the consequences will be if a security incident occurred
- Understanding the relevance to the individual
- Priority of information security to the individual
- Awareness of good security practices
- Awareness of internal standards and benchmarks (derived after piloting the interview)

These dimensions were developed based on Chan, Woon, Kankanhalli (2005), Dhillon and Backhouse (2000), and Stanton et al. (2004). The dimensions were developed by considering what characteristics of a person led to a good security attitude, assuming that someone with a bad security attitude would not have these characteristics. One note that needed to then be considered is the opposite of this, that there may be some extra attributes present in people with bad attitudes, but not present in those with good attitudes. Malicious intent (where a person may be a threat to the security of the organisation because they are attempting to compromise security for their own gain, (Besnard & Arief, 2004)) was not included because of perceived difficulties in its accurate measurement.

METHOD

A survey based approach, in which a survey would be administered to a number of separate groups throughout a number of different organizations, was seen as the most suitable way to pursue answers to the research questions as it allowed for consistent capture of the two constructs (culture and security awareness behaviour). This approach would allow both intra and inter organizational differences to be measured and analysed using a consistent approach.

Two large Australian financial sector organizations were purposefully recruited to the study and were chosen because of their similarities. These organisations are competing for the same market and deliver similar financial services to their customers, have very similar security needs and concerns within their work environment. The financial sector was chosen because of the importance that information security has to their operations. Within the organization, appropriate groups to which the survey could be administered were identified with the assistance of each organization's human resources department.

The survey instrument was developed to 'operationalise' the research model using the aspects of the constructs discussed above. The instrument made use of prior research using these constructs (such as Hofstede (1990,

Chan et al (2005), Dhillon and Backhouse (2000), and Stanton et al. (2004). The instrument was appropriately piloted before its use.

Four teams were sampled from the two organisations. The teams included two finance teams, a human resources team and a business support team. A whole population study was completed on each team. From the twenty four responses, 13 were male and 11 were female and the split of managers/team leaders to non team leaders was 50-50. Participants were dispersed relatively evenly over the various age groups, with the only one not well represented was the <25 group which had only one member. Most had some form or tertiary education be it an undergraduate degree, postgraduate degree or qualifications from a technical college, none, however, had not completed high school. This indicates that members of the teams were all well educated. The self assessed technical ability of participants ranged from very good (12.5%) to okay (25%) with the majority sitting on good (62.5%) and all participants had been using IT for a long time. Participants were considered to have the technical knowledge and abilities required to complete the survey correctly and to have well considered security expectations. Interestingly, the length of service of participants ranged from <1 to 38 years with 7 years being the longest anyone had been in their current position. With the measures for the number of years in the organisational unit and in the industry also displaying a diverse range (<1-13 and <1-38 respectively) a wide range of views on the organisation would have been encompassed within the study.

The data from this survey was analysed using a variety of methods. SPSS 15.0 was used for descriptive statistics and to run a series of validation tests. To explore the relationship between the two constructs a form of Structured Equation Modelling (SEM) known as PLS (Partial Least Squares) was used. PLS was also used to measure the reliability of the research method and for other validation techniques as outlined below.

Despite the fact that data was obtained from two different organisations, a lack of responses required the data to be pooled to create a single set of data. Data was screened for inconsistencies and invalid responses. All data was found to be valid.

PLS was selected as the data analysis tool for this study because of its ability to handle small datasets and weak linkages between constructs. Although the suitability of PLS for small sample sizes has been questioned (Goodhue, Lewis & Thompson, 2006; Marcoulides & Saunders, 2006) a major proponent of this analysis technique supports its use for small samples (Chin & Newsted, 1999). In addition the data collected had a small sample size (twenty four cases) and the results did not follow a standard distribution making the use of parametric analysis techniques unsuitable. The theoretical information regarding the relationship in this study is weak and hence this is more exploratory than confirmatory analysis for which PLS is more suitable than other data analysis techniques.

ANALYSIS AND RESULTS

Each core construct in the model (as depicted in Figure 3) is reflective of each of the dimensions studied. 'Organisation' was added as a control as it is the indicator most likely to have an effect on the organisational culture.

The first stage of the analysis required the screening of each indicator based on the loadings. Despite the testing of the instrument, it was found that there was little correlation between answers belonging to the same construct (i.e. the answers to the various questions for each construct were not consistent). The various loadings for the indicators were analysed and those with loadings less than 0.707 were reconsidered as part of the model. In some cases loadings of 0.5 or 0.6 were kept because there were other supporting indicators otherwise the indicators were removed. Low loadings occur due to the lack of consistency between answers. After the first round of culling the loadings were recalculated to ensure that they were still acceptable. During this process some loadings were increased and others decreased. Those that dropped below the benchmark of 0.7 were then removed. All loadings for indicators kept are significant at the 0.05 level (T-stat > 2.048) with the majority being significant at the 0.01 level (T-stat > 2.763). These high loadings suggest that the remaining items tend to strongly reflect their respective constraints.

Using the resulting indicators, the internal consistency of the constructs was examined. Firstly the composite reliability was examined using the composite reliability measure in PLS. As Cronbach's alpha will generate particularly low scores when there are a small number of items within each construct it was not used. The composite reliability variable was required to be greater than 0.70 to indicate internal consistency. As all reliability scores were well above 0.7, with the exception of the culture dimension of Open versus Closed (which only had a score of 0.701). Composite reliability was assumed.

The discriminant validity was then analysed via both available methods. These were calculated between the constructs of latent variables component scores and other indicators not associated with that construct. Each indicator should load higher on its own construct over any other construct. Only one potential problem was

identified, this being the indicator labelled Q4S1C17 which loads higher with Security Dimension 5 (Internal Standard) than it does with its own dimension (Security Dimension - Relevance). However, as it is not higher than those indicators specific to dimension 5, this is seen as a borderline case and as such it was decided to let it be due the minimal numbers already.

The square root of the average variance extracted for each construct with reflective indicators is greater than the correlations. The only exception to this is the two second order constructs. However, seeing as though these constructs are comprised of the same indicators as the conflicting constructs, this correlation is to be expected. Based on these results, and those of the cross loadings test, high discriminant validity was indicated.

The AVE value of all constructs sits above 0.5 implying that the construct accounts for at least 50% of the variance. Once again the only construct which only just reaches the 0.5 level is the culture dimension of Open versus Closed. This, as well as the composite reliability scores, indicates a high convergent validity.

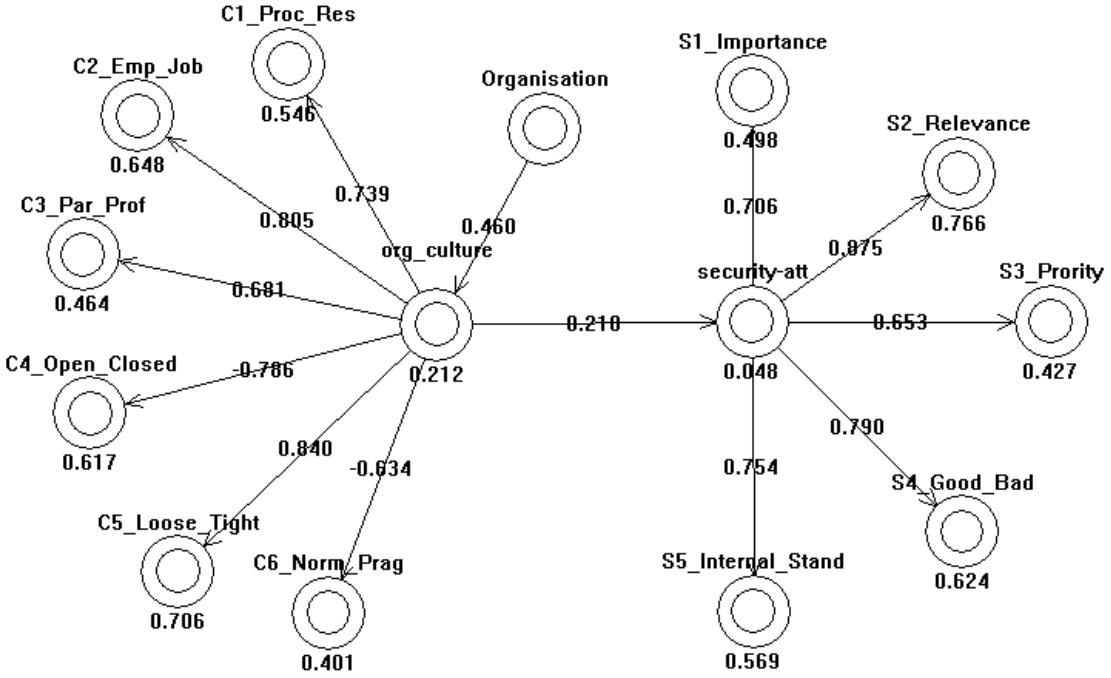

Figure 26: PLS output for model (inc. path coef. and R-square)

As can be seen in Figure 3, all of the dimensions of culture have a relatively high path coefficient excluding the dimension of Loose versus Tight control. All of these paths were significant (based on the T-statistic generated by running the bootstrap technique with 500 cases). A score was considered significant at the 0.01 level if greater than 2.763, which all of these values are. It can also be noted that organisation had an impact on the organisational culture, with a significance of 2.8016 which was to be expected. These figures suggest that the most important factors influencing the total organisational culture are those of Loose versus Tight control and Employee versus Job oriented. On the security construct it appears that the most influencing factor to employees' attitudes to security is the relevance to the individual. These results indicate support for the two components of the model.

If the relationship between the two core constructs is considered, the path coefficient is only 0.210 with an R-square of 0.048. Thus, very little variance explained by culture. Examination of the T-statistics provided by the bootstrap analysis suggests that this relationship is not significant at any level with a T statistic of 1.1275 which indicates that there is little or no relationship between these two constructs.

Based on these results it is assumed that the measurement model is correct. These tests were independently checked by colleagues to ensure the validity of the results. The analysis of the structural model displayed high significance of each of the various dimensions in each construct, thus indicating that for each construct the theoretical model is correct. However, the relationship between the two core constructs was found to be small (culture accounting for only 0.048 of the variance in attitudes) and insignificant with a T-value of 1.1275 (1.701

was required for a significance level of 0.1). This indicates that there is no relationship in this sample between culture and information security attitudes and the research question is rejected.

Limitations of Results

There are several factors that could lead to finding no relationship when one may exist. These include problems with the culture measurement tool, problems with the security measurement tool or problems with participants, all of which have significant implications for the research.

While the statistical analysis showed that the model of culture was indeed fitting of the organisations, it may be that it was inadequate to pick up the differences and characteristics in the culture that have an influence on the information security attitudes of employees. Culture was identified through the literature to be a particularly difficult concept to measure accurately. The particular model used in this study was chosen due to its extensive testing and reuse, however it was developed in the 1980's and it may well be out of date. It also should be noted that Hofstede never intended for the cultural measurement instrument he developed to be generalisable (Hofstede & Hofstede, 2005). However, this was accommodated for during the pilot by altering the questions to suit the companies so it is unlikely that this is the case. Previous studies have found organisations within the Australian financial industry to display very similar cultures (Kabanoff, 1992), so it may actually be that there were limited differences in the cultures to be analysed.

Another issue may have been with the tool itself as there is the possibility that it has not worked correctly and that the specific questions asked could not be properly answered by the participant. Kabanoff (1992) states, questionnaires can distort what members report on their culture. People may not naturally think about their organisational culture in terms of the researcher's survey questions. Employees may have never thought extensively about their work environment or have never had to make such evaluations before, so struggled to convert what they saw in the organisation into answers. While these concerns can never be completely eliminated, due care was taken when piloting the survey to reduce these issues.

The participants selected for this study may have had an influence on these results. The sample was representative of the various demographics, including managers and non managers; however, it was not necessarily representative of the organisation as a whole. The culture can differ from one place in the organisation to another and it is possible that the two cultures analysed within each organisation did not have a culture that effected security whilst others might. However, four separate groups were selected in each from several different business units and not one of the groups showed any sign of a correlation between the constructs, therefore indicating that it is unlikely to find a correlation in any of the other groups in similar business units. Furthermore, if this theorised relationship does exist, it should show up no matter where it was tested for in that area of business, regardless of whether it is a positive or a negative relationship. These forms of bias are difficult to account for however, where anonymity is ensured and honesty requested, there is little that can be done to ensure that participants are providing accurate responses. If these cases did occur, then the numbers should be minimal (otherwise it probably is reflective of the culture) and would have been picked up as outliers during the statistical analysis, therefore having minimal effect.

DISCUSSION

The results of the statistical analysis imply that there is no relationship between the organisational culture and information security attitudes in the data sample. This result is contrary to theories proposing the use of organisational culture with regards to information security. The initial scepticism about the relationship due to mixed results in previous research and external reviews of the conclusions reached in previous research. The following discussion explores the various possible explanations for the lack of a relationship to provide some further understanding to the results.

Security is still immature

The first possible reason for the lack of a relationship is timing. Organisational culture is something that takes a lot of time to develop. It takes time for values and practices to become ingrained into the culture. Information security is still a relatively new concept to a lot of organisations, especially the various methods for controlling possible threats. It is possible that it is still too early to find information security values and beliefs as part of an organisation's culture. Changes in an organisation's culture can be slow and painful, as various shifts in the sources of the culture gradually seep in and these changes are often resisted (Ott, 1989). For security to become part of an organisation's culture, these ideas must be somehow imparted on the organisation, accepted, and then propagated throughout the organisation. The fact that there are still arguments over what is 'best' for information security is possibly enough reason for these ideas to be resisted and struggle to impart themselves on the culture of an organisation. However, if it is in fact the case that security has not had the time to fuse into

culture, it leads to questions as to whether or not governance can truly alter or manipulate culture to cause desired changes in people's attitudes and beliefs. Any attempts to do so would, a) be met with resistance, and b) take significant time to become accepted and propagate before becoming a true part of the culture, thus also giving reason to doubt the practicality of the original theories underpinning this research.

Culture is too weak

As mentioned earlier, there appeared to be little consistency in the perceptions of individuals regarding the culture in their organisation. This further propagates to show little consensus within each of the sub groups. This may have been due to problems with the instrument itself but it could also be indicative of a few underlying culture issues, each of which have interesting implications to the theories.

The first of these issues is culture 'strength'. The literature often interprets culture strength to be the level of consensus between members of the organisation. A strong culture is one which is considered to be homogenous, where all respondents will give the same answers on key cultural questions (Hofstede & Hofstede, 2005). Weak cultures, on the other hand, provide answers that vary widely between members of the same unit. These results could therefore indicate that in fact the culture in both of these organisations is relatively weak or non-existent. If the cultures were too weak to be picked up, then the culture would therefore also be too weak to be used as a method of influence by corporate governance.

There are also some interesting perspectives regarding the existence of culture in organisations today. If culture takes such a long time to develop, then what happens in the unstable shifting business environment we have today? With higher and higher turnover rates, an organisation would have a situation where culture would not form because values would be consistently changing (Millman, 2007). As organisations and people's commitments to them become more short term and transient, it is suggested that people may get their workplace norms and values not from organisational culture, but from their profession. Organisation wide harmony and homogeneity is difficult to sustain given the salience of inconsistencies, disruptions, conflicts and ambiguities in contemporary organisations (Martin, 2002). The impact of technology on organisations has lead to more distributed business (for example, more people working from home) which could also reduce the influence of the organisation itself on employees. Thus, organisations would be unable to use their culture to influence employees, ruling out its usefulness as a means to improve information security.

Culture is fragmented

Another issue which may also be highlighted by the inconsistency in the results lies in the foundations of the fragmented view of culture. The fragmented view of culture sees consensus as transient and issue specific in which every time a particular issue is brought forward there is always some who are for the issue, some against, and others who are ambivalent or indifferent. A lack of consensus in the results could indicate that this view of culture is indeed the accurate one. However, if it is the accurate view of culture, then any attempts to influence the culture of the organisation by governance will also end in mixed results and therefore have little effect on the overall security behaviours.

Culture has no influence

The last explanation for the lack of a relationship is the simple fact that the relationship does not exist and never will exist. Perhaps culture has no influence whatsoever on people's attitudes and opinions, and henceforth their behaviours to information security? This lack of a relationship may only be with information security, or could extend further to a greater set of people's attitudes and opinions. If this is the case, then looking to culture as a means of improving user security behaviours will prove unfruitful and alternative methods will need to be explored. Looking at the results, there was a relative consistency in the security attitudes of employees, leading to the belief that there is indeed another factor which is having an influence

CONCLUSION

Information technology is advancing at a rapid rate and with this comes changes to the challenges of information security. A challenge which is often overlooked, both in the literature and in practice, is that of the threat posed by users to information security (Stanton et al., 2004). A variety of methods, including training and awareness, are used in an attempt to alleviate the problems of user involvement, but these can have adverse consequences. Instead it is proposed that corporate governance should take responsibility for information security.

There are several forms of information security governance, consisting of the technical, formal and informal. Research has recommended the use of the informal component to address the user issue in security (Mishra & Dhillon, 2006), and in particular the use of culture (Thomson & von Solms, 2005; von Solms & von Solms,

2004). All of these theories are based on the core assumption that a relationship exists between organisational culture and information security attitudes. However, no research could be identified that tested the existence of such a correlation. Tests for the effects of culture on other aspects (other than information security) of organisations have yielded mixed results (Martin, 2002). Various reviews of culture research found that its conclusions were often derived through inadequate methodology or from anecdotal evidence (Buchanan & Huczynski, 2004). This current knowledge leads to uncertainty about the existence of a relationship between organisational culture and information security attitudes. The relationship therefore needs to be evaluated before these theories can be tested or further utilised.

To test the relationship, a quantitative analysis was performed on two teams within each of two organisations from the financial industry. A survey was developed to analyse both the perceptions of the organisational culture and the attitudes to information security of employees in the organisation. This was based on the model of culture by Hofstede et al. (1990) and an information security attitude model developed through the research process. The model and survey were piloted via interview with the two organisations. The survey was then distributed via face to face methods and online, receiving twenty four responses. The data was analysed using Partial Least Squares (a method of Structural Equation Modelling). Both constructs appeared to be well-defined by their dimensions; however no relationship was found between organisational culture and information security attitudes. A secondary analysis was performed to examine the influence of governance measures on information security, and a positive relationship was discovered.

These results highlight the possibility that the relationship between organisational culture and attitudes to information security does not exist and also that perhaps a global culture model is not adequate. Possible explanations for the non-existence of the relationship have been provided. These include the nature of culture in today's organisations and the nature of culture itself, as well as the notion that information security has not yet had time to become part of the culture. The results also suggest that it is in fact the more common forms of governance which have an influence on information security attitudes.

A number of possible inadequacies of the analysis have been identified and addressed. The data passed all the validity and reliability tests and the results were independently checked to ensure their robustness. The resulting limitations that could not be addressed were identified.

Based on the results, the hypothesis that organisational culture does not have an influence on information security attitudes and behaviours was supported. However, due to the scope of the study it cannot be conclusively established that no relationship exists. Nevertheless, the results of the research have implications for both theory and practice. These results give us an insight into the relationship between organisational culture and information security through empirical testing, and lead us to question the proposed theories regarding information security and culture. These results can be used to guide further research toward alternate measures for improvement, which may provide more successful outcomes. Areas identified for future research include assessing further the influence of culture on information security, advancing the measurement tools, and examining more generally ways in which organisations can improve their information security via governance and thereby address the security vulnerabilities that arise from user interaction.

REFERENCES

Besnard D. & Arief B. (2004) Computer security impaired by legitimate users, *Computers & Security*, 23, 3, May 2004, Pages 253-264

Buchanan D. & Huczynski A. (2004) *Organisational Behaviour an Introductory Text*, 5th Ed., Prentice Hall

Chan M., Woon I. & Kankanhalli A. (2005) Perceptions of Information Security in the workplace: Linking Information Climate to Compliant Behaviour, *Journal of Information Privacy and Security*, 1, 3

Chin W. & Newstead P. (1999) Structural Equation Modelling Analysis with Small Samples Using Partial Least Squares, in Hoyle R. H. (Ed.), *Statistical Analysis for Small Sample Research*, SAGE Publications, California

Chin W. (1998a) Issues and Opinions on Structural Equation Modelling, *MIS Quarterly*, March

Chin W. (1998b) The Partial Least Squares Approach to Structural Equation Modelling, in Marcoulides G. (Ed.), *Modern Methods for Business Research*, Mahwah, NJ: Lawrence Erlbaum Associates

Dhillon G. & Backhouse J. (2000) Information Systems in the New Millennium, Association for Computing Machinery, *Communications of the ACM*, 43

Findler L., Vilchinsky N. & Werner S. (2007) The Multidimensional Attitudes Scale Toward Persons with Disabilities (MAS), *RCB*, 50

Goodhue D., Lewis W. & Thompson R. (2006) PLS, small size and statistical power in MIS research, Proceedings of the 39th Hawaii International Conference on Systems Sciences.

Hofstede G. (2005) *How Universal are the Six Organizational Culture Dimensions*? Accompanying Letter for Survey Questions

Hofstede G. & Hofstede G. J. (2005) *Cultures and Organisations: Software of the Mind*, Second Edition, McGraw Hill

Hofstede G., Neuijen B., Ohayv D. D. & Sanders G. (1990) Measuring Organisational Cultures: A Qualitative and Quantitative Study Across 20 Cases, *Administrative Science Quarterly*, 35

Hopkins A. (2006) Studying Organizational Cultures and Their Effects on Safety, *Safety Science*, 44

Kabanoff B. (1992) An Exploration of Organisational Culture in Australia (with a closer look at the banking sector), The Centre for Corporate Change, University of New South Wales

Leidner D. E. & Kayworth T. (2006) Research: A Review of Culture in Information Systems; Research: Toward a Theory of Information Technology Culture Conflict, *MIS Quarterly*, 30

Marcoulides G. A. & Saunders C. (2006) PLS: A silver bullet? A commentary on sample size issues in PLS modeling, MIS Quarterly, 30(2), iii-x.

Martin J. (2002) *Organizational Culture: Mapping the Terrain*, Foundations for Organizational Science, SAGE Publications, California

Millman G. J. (2007) Corporate Culture: More Myth than Reality?, *Financial Executive*, July / August

Mishra S. & Dhillon G. (2006) Information Systems Security Governance Research: A Behavioral Perspective, *Annual NYS Cyber Security Conference*

Ott J. S. (1989) *The Organisational Culture Perspective*, Brooks/Cole Publishing, California

Stanton J. M., Starn K. R., Mastrangelo P. & Jolton J. (2004) Analysis of End User Security Behaviours, *Computers & Security*, 23

Thomson K. & von Solms R. (2005) Information Security Obedience: A Definition, *Computers & Security*, 24

van den Berg P. & Wilderom C. (2004) Defining, Measuring and Comparing Organisational Cultures, *Applied Psychology: An international review*, 53

von Solms R. & von Solms B. (2004) From Policies to Culture, *Computers & Security*, 23

COPYRIGHT