The Effect of Organisational Culture on Employee Security Behaviour: A Qualitative Study

L. Connolly[1], M. Lang[1], J. Gathegi[2] and J.D. Tygar[3]

[1]Business Information Systems, National University of Ireland Galway, Ireland
[2]School of Information, University of South Florida, Tampa, USA
[3]Electrical Engineering and Computer Science, University of California, Berkeley, USA
e-mail: y.connolly1@nuigalway.ie

Abstract

An increasing number of information security breaches in organisations presents a serious threat to the confidentiality of personal and commercially sensitive data. Recent research shows that humans are the weakest link in the security chain and the root cause of a great portion of security breaches. This paper draws on prior research on organisational culture to examine how cultural factors affect employee security behaviour. Data for this research project were collected in 15 organisations in the United States and Ireland through qualitative interviews. Our findings demonstrate that organisational culture values of solidarity and people-orientation promote information security compliance, while sociability and task-orientation have a negative effect on employee security behaviour.

Keywords

Employee Security Behaviour, Organisational Culture, Information Security

1. Introduction

Historically, organisations have emphasised a technological approach in order to protect the security of their information assets. However, as many attackers have started to include social means in their malicious efforts, e.g. social engineering, the need for a holistic approach in addressing information security issues has emerged. The domain of behavioural information security (InfoSec) research highlights the importance of taking into consideration the "human" element when ensuring information security throughout the organisation. Research and practice have shown that technical tools are powerless when it comes to the enforcement of behavioural rules such as password sharing, reporting of security incidents, adherence to a clear desk policy, and the secure disposal of confidential documents. Commonly, compliance with these rules entirely depends on employees' motivation to conform.

Generally, Behavioural InfoSec research falls into two broad categories: those that focus on the effects of cognitive processes on employee security behaviour (Bulgurcu et al., 2010) as well as social controls (Chen et al., 2013). The two basic forms of social controls are formal and informal (Ross, 1896). This study concentrates on informal controls. Informal social controls include customs, traditions, norms, morality and other social values (Cheng et al., 2013). Researchers

from the IS discipline have examined the effect of various informal social controls on employee behaviour in organisational settings such as social bonds (Ifinedo, 2014), social pressure (Cheng et al., 2013; Guo and Yuan, 2012), influence of top management (Puhakainen and Siponen, 2010), and cultural factors (Hovav and D'Arcy, 2012; Vroom and von Solms, 2004).

Although in the past few years Behavioural InfoSec research has seen some expansion, providing insights into insider violations and offering practical solutions to prevent devious behaviour of employees, it is still in a developing phase. For instance, while prior research shows a link between organisational culture (OC) and behaviour (Baker, 1980), we found only two conceptual papers within the established literature that argued that OC culture is a strong predictor of employee security behaviour (von Solms and von Solms, 2004; Vroom and von Solms, 2004), while calls to conduct more studies in this area are present (Hu et al., 2012). In particular, Hu et al. (2012, p.617) argued that the effect of OC, "one of the key constructs in organisational and individual behaviour literature", on information security has not been rigorously examined. Therefore, the objective of our study is to contribute to a better understanding of the answer to the following research question:

- How do organisational culture values affect employee security behaviour in organisational settings?

2. Theoretical Context

The subject of this research project is *employee security behaviour*, which is defined as "the behaviour of employees in using organisational information systems (including hardware, software, and network systems etc.), and such behaviour may have security implications" (Guo, 2013, p. 243). Examples of employee security behaviour include how members of staff handle their passwords, how they deal with organisational data, and how they use network resources (Guo, 2013). This behaviour may either pose or moderate organisational IS security threats.

The two types of employee security behaviour examined in this research project are *compliant behaviour* (i.e. adhering to the policies, procedures, and norms of an organisation in relation to information security) and *non-compliant behaviour* (i.e. intentional but non-malicious behaviours of employees that may put organisational information systems at risk and entail non-compliance to the policies, procedures, and norms of an organisation in relation to information security).

The study of culture is rooted in sociology, social psychology, and anthropology (Ali and Brooks, 2009). Culture has been studied for over a hundred years in various disciplines and, as Straub et al. (2002) put it, "culture has always been a thorny concept and an even thornier research construct". OC is defined in this research project as "culture shared between people working in an organisation" (Ali and Brooks, 2009, p. 550). Prior research shows that OC has an impact on individuals' behaviour (Baker, 1980).

OC has been conceptualised in terms of values that distinguish one organisation from another. OC research has experienced a wide range of values (Leidner and Kayworth, 2006). This research project focuses on a smaller set of OC values, including *people-orientation*, *solidarity*, *sociability*, *task-orientation,* and *flat structure*, and their impact on individuals' behaviour. Organisational value of *people-orientation* refers to organisations that are "concerned with people issues" (Cooke and Lafferty, 1987, p. 52). Goffee and Jones (1996, p.134) define *solidarity* as "a measure of community's ability to pursue shared objectives quickly and effectively regardless of personal ties" and *sociability* as "the measure of sincere friendliness among members of a community". *Task-orientation* is defined as "concern for efficiency" (Cooke and Lafferty, 1987, p.54). Finally, *flat structure* is an organisational structure that aims to reduce "the number of layers of management hierarchy" (Kettley, 1995, p.1).

3. Research Approach

The methodology adapted for this study draws on the *analytical grounded theory* (AGT) approach (Matavire and Brown, 2013) employing a *constant comparative method* by Maykut and Morehouse (1994). The method used in this study is characterised by a mix of description and interpretation of data, the outcome of which is an interpretive-explanatory framework supported by participants' quotes.

In total, 19 individuals were selected for interview, drawn from organisations across a range of industry sectors. Nine interviews were conducted in the United States of America (US) and ten in Ireland. The choice of interviewees was more opportunistic than deliberate, arising as it did out of a research exchange programme which necessitated the lead author spending extended periods of time in both countries. Details about the interviewees and their organisations are given in Table 1.

Data collection was carried out using semi-structured *in-person* interviews. The interview guide was constructed following a thorough analysis of the literature. In addition to questions about OC values, we also looked at a number of factors that are outside the scope of this paper. As regards the questions about OC, there is a wide range of OC models employed within IS research. A list of the most prominent OC frameworks was borrowed from Leidner and Kayworth's (2006) work, producing over 20 organisational values. These values were then grouped into broader categories due to their evident similarities, including *people-orientation*, *solidarity*, *sociability*, *hierarchy*, *task-orientation*, and *rule-orientation*, and interview questions were constructed around these themes. However, as the study developed, it soon became evident that we would not be able to make conclusions about the influence of *hierarchy* and *rule-orientation* on employee security behaviour due to insufficient data. Interview guide topics including corresponding references and questions are illustrated in Table 2.

Name (aliases)	Industry type? When founded, size?	Number of people interviewed and their roles
CloudSerUS	IT; 1998; large	One person – Software Developer
RetCoUS	Finance; 1932; large	One person – Security Executive
CivEngCoUS	Civil Engineering; 1945; SME	One person – Civil Engineer
TechCorpUS	IT; 1968; large	Two people – both Security Researchers
EducInstUS	Education; 1868; large	Two people – Administrator and Professor with expertise in IS security
FinCoUS	Finance; 1982; large	One person – Security Consultant
PublCoUS	Publishing; 2005; SME	One person – Business Owner
TechCorpIrl	IT; 1968; large	Two people – Product Manager and IT Executive
CharOrgIrl	Charity; 1883; large	One person – Data Protection Officer
BevCorpIrl	Food and Beverage Manufacturing; 1944; large	One person – IT Executive
PublOrgIrl	Publishing; 2000; SME	One person – Chief Editor
EducOrgIrl	Education; 1845; large	Two people – Administrator and Lecturer with expertise in IS security
TelCommCorpIrl	IT; 1984; large	One person – Software Developer
ResRegIrl	Energy Regulation; 1999; SME	One person – Policy Analyst
BankOrgIrl	Finance; 1982; large	One person – Security Executive

Table 1: Facts about US and Irish Interviewees' Organisations

In the opening stage of the analytical process (Phase 1), the body of data was segmented into discrete 'incidents' (Glaser and Strauss, 1967). Next, a set of first-round provisional categories was generated (Phase 2), to which the segmented data would be coded. These categories, which are broad descriptions of themes and concepts, took two forms, in particular, participant-driven and researcher-driven categories. The former were derived from familiarity with the participants' customs and language, while the latter were derived from a theoretical framework underpinning this study. Having segmented and labelled the body of data and generated a set of first-round provisional categories, one-third of incidents or units were examined and placed into one or more of these categories, and, analysis of their content gave rise to the formation of additional provisional categories. The next phase of data analysis (Phase 3 - Coding on) involved further breaking down of incidents of data identified in the first phase in order to offer more in-depth understanding of the highly qualitative aspects and offer clearer insights into the meaning embedded therein. In Phase 4, the provisional categories identified in the second phase were analysed for their characteristics and properties so as to develop a 'rule for inclusion' in the form of a propositional statement, coupled with sample data.

Topics	Reference	Examples of questions
People-orientation	Cooke and Lafferty (1987)	How satisfying is the organisation you are working for with respect to employee benefits?
Solidarity	Goffee and Jones (1996)	Do you ever voluntarily work overtime in order to complete some important task?
Sociability	Goffee and Jones (1996)	Is it common to have non-work related chats with your colleagues during work hours?
Hierarchy	Ouchi (1981)	Is it easy to approach your immediate manager?
Task-orientation	Cooke and Lafferty (1987)	Do you think management expects you to put company goals before your personal goals?
Rule-orientation	Hofstede (1991)	Is it acceptable to break rules in your organisation?

Table 2: Interview Guide Topics

As a 'rule of inclusion' was developed for each relevant category, the remaining two thirds of the data segments were analysed, compared and coded. As the constant comparative procedure progressed, data incidents that fitted with a 'rule for inclusion', validated that category and emerging theoretical insights. Furthermore, data incidents that failed to fit with existing categories generated leads to the formation of additional categories. Over the course of this analytical process, categories underwent various changes: while some of them were substantiated quickly, others were eliminated as irrelevant to the focus of inquiry; some were merged due to overlaps or needed to be re-defined, and new categories emerged. Throughout this reiterative process, propositional statements of categories underwent modifications as the theoretical insights were developed and refined into the phenomenon under study. As the process drew to a conclusion, substantiated propositional statements constituted the roughly formed outcomes of this research project. Subsequently, data reduction was performed in order to emphasise findings relevant to the objectives of this study. Finally, data validation took place where evidence in data was sought to support proposed findings.

4. Research Findings and Discussion

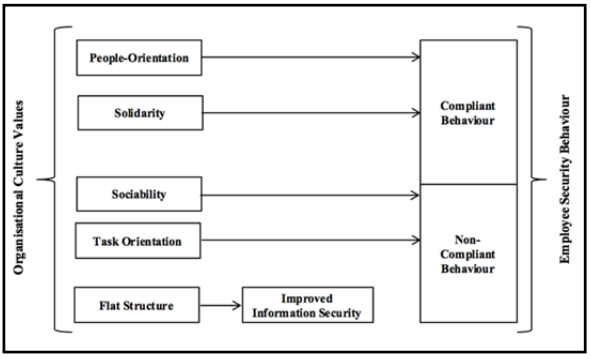

Figure 1: Conceptual Framework

This study's findings indicate that OC values affect employee security behaviour in organisational settings (Fig. 1). In particular, values of *solidarity* and *people-*

orientation are positively associated with security behaviours, while *sociability*, and *task-orientation* have a negative effect on security-related actions. Additionally, a *flat structure* encourages employees to address issues related to information security and therefore, *improves the overall level of information security* in organisations.

4.1. People-Orientation

In both countries, study informants from TechCorpIrl, BankOrgIrl, CharOrgIrl, BevCorpIrl, CloudSerUS, RetCoUS, TechCorpUS, and FinCoUS believe that *high people-orienation* encourages *information security compliance*, while *low people-orientation* has a negative effect on *employee security behaviour* as expressed by interviewees from BevCorpIrl, EducOrgIrl, and CivEngCoUS. For example, RetCoUS puts high value on employee satisfaction and ensures their members' happiness and health in order to promote *information security compliance*. A Security Executive from RetCoUS shares:

> "I think satisfaction could affect employee security behaviour in a sense that if people are happy and healthy, they are more likely to follow rules and be more willing to go that extra mile when they are doing their job".

Data results lead to a conclusion that an organisational value of *people-orientation* has a positive impact on *security-related behaviour*. When an organisation takes care of its employees, they feel satisfied in their jobs. The satisfaction refers to the employees' state of contentment with their organisation. Sources of satisfaction could be good working conditions (e.g. bright office, fast computer), an excellent reward/benefit system, opportunities to grow and realise potential (e.g. promotions), or job security. These results are in line with prior studies. In particular, Danish and Usman (2010) concluded that rewards and recognition are important predictors of employee work motivation. Xue et al. (2011) reported that employee satisfaction has a positive impact on their compliance with organisational information security requirements. Furthermore, Probst and Brubaker (2001) found out that employee who report high perceptions of job insecurity exhibit decreased safety motivation and compliance. Hence, organisations should strive to cultivate a value on people-orientation in order to encourage compliance with information security rules.

4.2. Solidarity

In both countries, four study participants from CloudSerUS, TechCorpUS, and EducOrgIrl believe that a high level of *solidarity* has a positive impact on *employee security behaviour*. For example, CloudSerUS is an organisation that highly values the security of their assets and therefore, has in place various security measures and controls to protect valuable information. Employees realise a company's goal as regards to information security and demonstrate their solidarity by following information security rules. A Software Developer from CloudSerUS shares:

> "There is a renewed focus...everybody understands that security is a big concern from a lot of aspects…people do tend to adhere to a policy just because it is there... nobody has tried to violate information security rules".

Our findings lead us to conclude that when employees realise and share organisational goals, and the goal is to protect sensitive information, they are more likely to comply with organisational security requirements. Furthermore, if employees understand that, generally, exercising good security practices is important for their organisation, they follow safe practices even if the organisation itself does not enforce them. Hence, solidarity encourages behaviour that supports an organisation. These results are in accordance with contemporary literature. In particular, Long (1978) demonstrated a link between employee ownership and behaviour that supports the organisation. Guo and Yuan (2012) reported that employees prefer to conduct within social norms of their particular workgroup. Cheng et al. (2013) concluded that attachment to one's organisation and commitment discourage security violations in organisations. Therefore, it is important to promote *solidarity* among employees, which can be done via a good benefit system, favourable working conditions, and opportunities to realise potential.

4.3. Sociability

In both countries, study participants from EducInstUS, CharOrgIrl, EducOrgIrl, TelCommCorpIrl, and ResRegIrl suggest that *high sociability* can encourage *non-compliant behaviour*. For example, a Software Developer from TelCommCorpIrl shares:

> "People are probably more lax in terms of information security because of a friendly atmosphere...If the PC police were beside our cubicle, we would be all fired a long time ago...especially a guy beside me...we always slag him that the HR are coming for him."

Although *high sociability* forms a special bond between employees, where employees begin to trust each other and work as a team, it may also create an informal atmosphere and therefore, drive wrong behaviours. Organisational members may not take any form of formality or authority seriously like managers instructions or organisational rules. High sociability is therefore detrimental unless management can preserve a required level of professionalism. Subsequently, employees will realise that although management is friendly, they still represent organisational authority and therefore, their orders and instructions are a requirement as the obligation to follow information security rules. Although friendliness has a lot of advantages (e.g. openness to new ideas, teamwork), there are also drawbacks. For example, the prevalence of friendships may allow poor performance to be accepted as no one wants to rebuke or fire a friend (Goffee and Jones, 1996). As a result, when rules get broken, it can be deliberately overlooked. Rashid et al. (2004) added that a friendly environment can breed mediocrity among employees. Normally, friends are reluctant to disagree with or challenge one another, which can lead to an exaggerated concern for consensus and subsequently, to a loss of focus on a company's mission and goals.

4.4. Task-Orientation

Study participants from both countries from BevCorpIrl, ResRegIrl, FinCoUS, and EducInstUS believe that work pressure pushes them to break rules with regards to information security. For example, an IT Executive from BevCorpIrl notes:

> "Sometimes IT security policies and procedures are a barrier to getting things done as quickly and as correctly as possible. And if you are being rewarded for getting stuff done quicker…it is going to happen [that information security rules will be broken]. I definitely think that."

Task completion implies finishing a particular job within a certain time frame. Often, the time frames are unrealistic as they are driven by a desire to satisfy customers by all means necessary. Study participants report that unrealistic deadlines or tasks push people to take shortcuts and break rules. If there is an imbalance between workload and the time allocated to complete tasks or meet deadlines, *high task-orientation* has a negative impact on *employee security behaviour*.

This inference is confirmed in the extant literature (Albrechtsen, 2007; Bulgurcu et al., 2010). For example, Bulgurcu et al. (2010) argued that commonly employees perceive information security rules as inconvenience and obstruction to meet daily work requirements. Albrechtsen (2007) concluded that employees circumvent information security rules if the rules are a barrier to productivity. In organisations that put high emphasis on results, employees may feel oppressed due to continuous stress and pressure, which may result in negative feelings about an organisation. In turn, ill feelings can have a negative effect on employee compliance with information security rules (Cavallari, 2012).

Therefore, it is up to organisational leaders to find a balance between employees' daily commitments and information security requirements. Our results indicate that security staff should take feedback from employees and adjust security requirements accordingly. It is meaningless to have rules in place that are impossible or hard to implement in practice. Top management and security staff should work as one unit in order to find the balance between employee workload and their obligations related to information security.

4.5. Flat Structure

The organisational value of *flat structure* has emerged as the opposite value to *hierarchy*. Study participants from PublCoUS, RetCoUS, TechCorpUS, FinCoUS, TechCorpIrl, TelCommCorpIrl, CloudSerUS, and CharOrgIrl believe that *flat structure* has a positive impact on the overall level of security in organisations; in particular, it improves *information security*. When management are open to suggestions, employees freely express their concerns and problems, which, in turn, may improve the level of information security in organisations. For example, an IT Executive from TechCorpIrl shares that management tends to encourage employees to speak their mind in order to improve their processes:

> "I am approachable...I guess this would just reinforce the strength of information security because I believe if people were to feel there was some type of a problem or issue, they would not hesitate to talk to me about it".

Flat structure has a positive impact on information security. In particular, accessibility and approachability of management improves visibility for information security throughout the organisation. Furthermore, if employees become aware of any problem, they are more likely to express their concerns to a manager and possibly improve current processes or rules, which will benefit an organisation in a long-run. Acquiring user perspective on some issues is especially important because managers or policy makers may not be familiar with all aspects of working environments.

This finding is in line with results reported in the extant literature. In particular, Chipperfield and Furnell (2010) stressed that in flatter organisations, management is easy to approach and therefore employees freely address concerns. Pearson (1987) asserted that a flat structure empowers employees to protect organisational interests because employees and leaders share a common set of values and feel personal ownership for the success of their organisation. As a result, employees will not hesitate to speak up if any issues arise. Furthermore, Lim et al. (2009) asserted that in organisations where management is opened to discussions and all members are involved in security affairs, employees tend to feel responsible to adhere to organisational security procedures and guides.

5. Conclusion

The findings of this study indicate that OC values have an effect on employee security behaviour in organisational settings. Study participants reveal that *high people-oriented* organisations benefit from a satisfied workforce, which in turn motivates employees to comply with information security rules, while *low-people-orientation* has a negative effect on *employee security behaviour*. Moreover, *high solidarity* has a positive effect on employee security behaviour because employees realise and pursue organisational goals, while *low solidarity* encourages non-compliance. Next, *high sociability* and *high task-orientation* have a negative impact upon employee security behaviour, while *flat structure* improves the overall level of information security in an organisation.

In terms of study limitations, US data was collected in organisations located in the Bay Area, California. The US is a vast country and different parts have distinctive characteristics. For example, the Californian Bay Area is home to Silicon Valley, and therefore is home to a great number of achievers. This culture may have a certain influence on employee security behaviour as opposed to the less competitive culture that prevails in some other parts of the US.

Furthermore, one of the main concerns with qualitative studies is the generalisability of research findings. As this study is exploratory in nature, it is not attempting to generalise the findings but rather to present uniqueness within its context. Therefore, study results cannot be generalised at a country level because as with most of

qualitative studies, the sample is too small. Future research would benefit from conducting a quantitative study that would confirm generalisability of the aforementioned findings.

Nevertheless, this research project makes a contribution by taking its place amongst the very few studies in Behavioural InfoSec research that investigate effects of OC on employee security behaviour. It provides an insight for managers on which OC values should be fostered in order to encourage information security compliance and which should be promoted with caution. For example, while task-orientation is inevitable in some organisations, practitioners should find a balance between requirements for results and information security requirements.

6. References

Albrechtsen, E. (2007), "A qualitative study of users' view on information security", *Computers & Security*, Vol. 26, No. 4, pp 276-289.

Ali, M. and Brooks, L. (2009), Culture and IS: National Cultural Dimensions within IS Discipline. In: *Proceedings of the 13th Annual Conference of the UK Academy for Information Systems*, pp 1-14.

Baker, E.L. (1980) "Managing organizational culture", *Management Review*, Vol. 69, pp 8-13.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010), "Information security policy compliance: An empirical study of rationally-based beliefs and information security awareness", *MIS Quarterly*, Vol. 34 No. 3, pp 523-548.

Cavallari, M. (2012) "A Conceptual Analysis about the Organizational Impact of Compliance on Information Security Policy". In – 3rd International Conference Exploring Services Science, IESS 2012. Geneva, Switzerland, 15th to 17th February 2012. Berlin: Springer. pp. 101-114.

Chen, Y.K. Ramamurthy, K. and Kuang-Wei, W. (2012) "Organizations' information security policy compliance: Stick or carrot approach?", *Journal of Management Information Systems*, Vol. 29, No. 3, pp 157-188.

Cheng, L., Ying, L., Wenli, L., Holm, E. and Zhai, Q. (2013) "Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory", *Computers & Security*, Vol. 39, pp 447-459.

Chipperfield, C. and Furnell, S. (2010) "From security policy to practice: Sending the right messages", *Computer Fraud & Security*, Vol. 3, pp 13–19.

Cooke, R.A. and Lafferty, E. (1987) "Organizational Culture Inventory", Human Synergistics, Plymouth.

Danish, R.Q. and Usman, A. (2010) "Impact of Reward and Recognition on Job Satisfaction and Motivation: An Empirical study from Pakistan", *International Journal of Business and Management*, Vol. 5, No. 2, pp 159-167.

Glaser, B. G., Stauss A. L. (1967) *The Discovery of Grounded Theory*, Aldine, Chicago.

Goffee, R., and Jones, G. (1996) "What holds the modern company together?", *Harvard Business Review*, Vol. 74, No. 6, pp 133-148.

Guo, K.H. (2013) "Security-related behavior in using information systems in the workplace: A review and synthesis", *Computers & Security*, Vol. 32, pp 242-251.

Guo, K.H. and Yuan, Y. (2012) "The effect of multilevel sanctions on information security violations: A mediating model", *Information & Management*, Vol. 49, No. 6, pp 320-326.

Hofstede, G. (1991) *Cultures and organizations: Software of the mind*. London, McGraw-Hill.

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.

Hu, Q., Dinev, T., Hart, P. and Cooke D. (2012) "Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture", *Decision Sciences*, Vol. 43, No. 4, pp 615-659.

Ifinedo, P. (2014) "Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition", *Information & Management*, Vol. 51, No. 1, pp 69-79.

Kettley, P. (1995) "Is Flatter Better? Delayering the Management Hierarchy", Report 290, The Institute for Employment Studies, Publisher: Microgen UK Ltd. [Online] Available from: http://www.employment-studies.co.uk/system/files/resources/files/290.pdf [Accessed November 15th, 2015].

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.

Lim, J.S., Chang, S., Maynard, S. and Ahmad, A. (2009) "Exploring the relationships between organizational culture and information security culture". In – 7th Australian Information Security Management Conference. Australia, Perth, 1st – 3rd December 2007.

Long, R. J. (1978) "The effects of employee ownership on organizational identification, employee job attitudes, and organizational performance: A tentative framework and empirical findings", *Human Relations*, Vol. 31, No. 1, pp 29-48.

Matavire, R. and Brown, I. (2013) "Profiling grounded theory approaches in information systems research", *European Journal of Information Systems*, Vol. 22, No. 1, pp 119-129.

Maykut, P. and Morehouse, R. (1994) *Beginning Qualitative Research: A Philosophic and Practical Guide*. The Falmer Press, London.

Ouchi, W. (1981) *Theory Z: How American business can meet the Japanese challenge*. Addison-Wesley Publishing Company, Reading.

Pearson, A.E. (1987) "Muscle-build the organisation", *Harvard Business Review*, Vol. 65, No. 4, pp 49-55.

Probst, T.M. and Brubaker, T.L. (2001) "The effects of job insecurity on employee safety outcomes: cross-sectional and longitudinal explorations", *Journal of Occupational Health Psychology*, Vol. 6, No. 2, pp 139-159.

Rashid, Z.A., Samasivan, M. and Rahman, A.A. (2004) "The Influence of organizational culture on attitudes toward organizational change", *Leadership & Organization Development Journal*, Vol. 25, No. 2, pp 161-179.

Ross, E.A. (1896) "Social Control", *American Journal of Sociology*, Vol. 1, No. 5, pp 513-535

Straub, D., Loch, K., Evaristo, R., Karahanna, E., and Strite, M. (2002) "Toward a theory-based measurement of culture" *Journal of Global Information Management*, Vol. 10, pp 13-23

Von Solms, R. and von Solms, B. (2004) "From policies to culture", *Computers & Security*, Vol. 23, pp 275-279.

Vroom, C. and von Solms, R. (2004) "Towards information security behavioural compliance", *Computers & Security*, Vol. 23, pp 191-198.

Xue, Y., Liang, H. and Wu, L. (2011) "Punishment, Justice, and Compliance in Mandatory IT Settings", *Information Security Research*, Vol. 22, No. 2, pp 400-414.