Organisational Culture, Procedural Countermeasures, and 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
y.connolly1@nuigalway.ie
[2]School of Information, University of South Florida, Tampa, USA
[3]Electrical Engineering and Computer Science, University of California, Berkeley, USA

Research Paper

Abstract

Purpose - This paper provides new insights about security behaviour in selected U.S. and Irish organisations by investigating how organisational culture and procedural security countermeasures tend to influence employee security actions. An increasing number of information security breaches in organisations presents a serious threat to the confidentiality of personal and commercially sensitive data. While recent research shows that humans are the weakest link in the security chain and the root cause of a great portion of security breaches, the extant security literature tends to focus on technical issues.

Design/methodology/approach – This paper builds on general deterrence theory and prior organisational culture literature. The methodology adapted for this study draws on the analytical grounded theory approach employing a constant comparative method.

Findings – This paper demonstrates that procedural security countermeasures and organisational culture tend to affect security behaviour in organisational settings.

Research implications – This paper fills the void in information security research and takes its place amongst the very few studies that focus on behavioural as opposed to technical issues.

Practical implications – This paper highlights the important role of procedural security countermeasures, information security awareness, and organisational culture in managing illicit behaviour of employees.

Originality value – This study extends general deterrence theory in a novel way by including information security awareness in the research model and by investigating both negative and positive behaviours.

Keywords

Employee Security Behaviour, Organisational Culture, Information Security Policy, Security Education, Information Security Awareness

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. Rather, compliance with these rules entirely depends on employees' motivation to conform. Therefore, it is essential to understand factors that lead to compliant behaviour or that prompt employees to break organisational information security rules. This study provides new insights about security behaviour in selected U.S. and Irish organisations by investigating how organisational culture and procedural security countermeasures influence security actions. Crossler et al. (2013, p.90) note that "although a predominant weakness in properly securing information assets is the individual user within an organization, much of the focus of extant security research is on technical issues". In response, our work takes its place amongst the small number studies to date that focus on behavioural as opposed to technical issues.

Generally, Behavioural InfoSec research falls into two broad categories: (1) those that focus on the effects of cognitive processes on employee security behaviour (Bulgurcu et al., 2010), and (2) the effect of social controls (Chen et al., 2013) and this study concentrates on the latter. The two basic forms of social controls are formal and informal (Ross, 1896). Formal social controls refer to rules and regulations against deviant behaviour (Cheng et al., 2013). Organisational sanctions, rewards, security education and training, and information security policies are all forms of formal organisational controls. There is an abundance of research with the field of Information Systems (IS) on how formal organisational controls influence security behaviour. Bulgurcu et al. (2010) and Hu et al. (2011) emphasise the vital role of sanctions and rewards in managing security behaviour in organisational settings. Chan et al. (2005) and Siponen et al. (2009) assert the importance of security policies and education as factors that deter malicious actions of employees. Our research focuses on the effect of information security policies and security education on employee security education. Following Hovav and D'Arcy (2012), these security controls are collectively referred as "procedural security countermeasures".

Although Behavioural InfoSec research has seen some expansion in the past few years, it is still in a developing phase. Some prior literature provides evidence that procedural security countermeasures reduce IS misuse (Straub 1990; Siponen et al., 2009), while other studies contradict these findings (Lee et al., 2004). Straub (1990) and Chan et al. (2005) found that security policies were associated with lower levels

of computer abuse. Similarly, Siponen et al. (2009) and Barlow et al. (2013) reported that security education is an important predictor of security-compliant behaviour. On the contrary, Lee et al. (2004) concluded that security policies and security awareness programs do not reduce IS misuse.

Undeniably, these previous studies are highly informative. However, they investigated the direct effect of procedural security countermeasures on employee security behaviour, neglecting the important role of user information security awareness. The purpose of an information security policy in conjunction with appropriate security education is to increase information security awareness, which, in turn, will promote security-cautious behaviour (Barlow et al., 2013). However, within the established literature territory, we have not found any empirical studies confirming that security policies and security education affect security actions in organisations indirectly through information security awareness. Additionally, various IS studies emphasised that information security awareness plays an important role in encouraging security-cautious behaviour (Bulgurcu et al., 2010), while empirical findings appeared to be contradictory. For example, although Bulgurcu et al. (2010) reported that users' general awareness about information security has a positive effect on their behaviour, Lee et al. (2004) asserted that a degree of awareness has no impact on employees' security actions. Moreover, there are calls in the literature to "identify factors that lead to information security awareness as it would be an important contribution to academics, since there is a gap in the literature in this direction" (Bulgurcu et al., 2010, p.543).

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). While it has long been the established wisdom that there is a link between organisational culture (OC) and behaviour (Baker, 1980), our literature search found only two conceptual papers within mainstream outlets that argued that OC culture is a strong predictor of employee security behaviour (von Solms and von Solms, 2004; Vroom and von Solms, 2004). In calling for more studies to be conducted in this area, Hu et al. (2012, p.617) argue that the effect of OC, which is "one of the key constructs in organisational and individual behaviour literature", on information security has not been rigorously examined.

Therefore, taking in consideration the aforementioned research gaps, the objective of our study is to answer the following research questions:

- How do procedural security countermeasures affect employee security behaviour?

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

By answering these questions, this research helps to fill a void in the literature as it focuses on behavioural aspects as opposed to technical issues. Additionally, practical implications are revealed as it is significant for IT managers to understand factors that affect employee security behaviour.

2. Theoretical Context

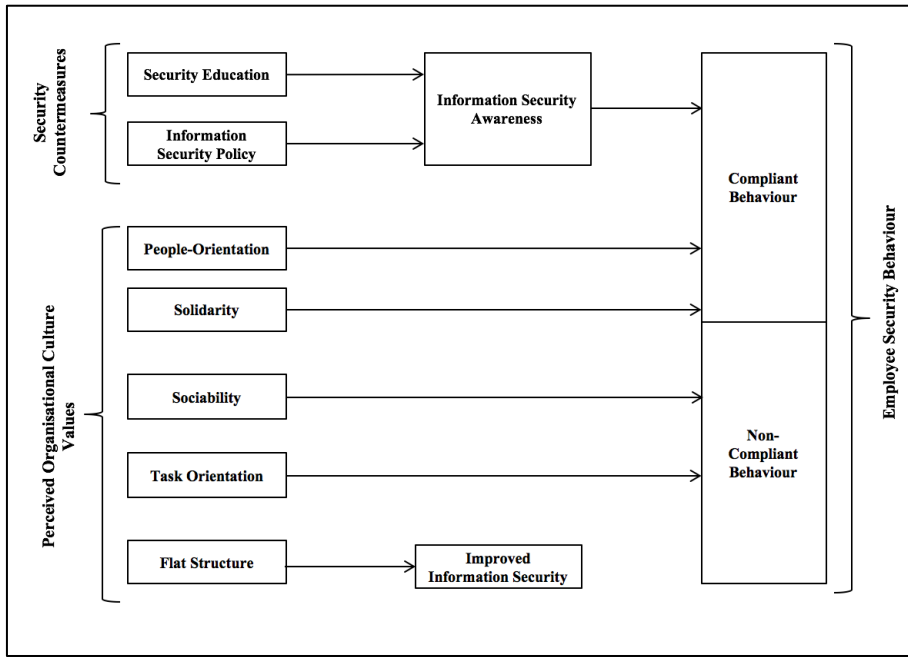

Figure 1: Conceptual Framework

Our proposed theoretical model, shown in Figure 1, integrates organisational culture values, procedural security countermeasures, information security awareness, and employee security behaviour. General Deterrence Theory (GDT) and prior organisational culture literature underpin this model. This framework expands GDT by including procedural security countermeasures as factors that tend to increase employee information security awareness. In turn, employee awareness about organisational information security requirements, security threats and consequences of illicit actions is inclined to lead to compliant behaviour. That is, procedural security countermeasures influence employee security behaviour indirectly through employee security awareness. Commonly, GDT is employed to study negative behaviours, while we include both negative and positive, further extending this theory.

2.1. General Deterrence Theory

The theory of deterrence relies on three individual components: severity, certainty, and celerity of sanctions. Based on the rational choice view of human behaviour, GDT is based upon the central proposition that illicit behaviour can be controlled by the threat of sanctions. Therefore, GDT focuses on disincentives against committing a criminal act and the effect of these disincentives on deterring others from committing deviant acts (Blumstein et al., 1978). The original theory assumes that if a punishment is severe, certain and swift, a rationally calculating human being will measure the gains and losses before engaging in crime and will desist from a criminal act if the loss is greater than the gain. Therefore, GDT posits that "people respond to policing and the punishment that is associated with the effective policing" (Straub, 1990, p. 258).

Classic GDT has been widely employed in the IS security context under the presumption that employees choose to engage in inappropriate behaviour and therefore, organisational sanctions will prevent deviant actions of employees and deter computer abuse (D'Arcy et al., 2014). GDT was further extended and policing is being associated with security countermeasures, including information security policies (Lee et al., 2004), security education (Barlow et al., 2013), and technical controls (D'Arcy and Hovav, 2007), assuming that these controls also deter illicit actions of individuals. Therefore, in keeping with the rationale of GDT, security researchers and practitioners generally believe that organisations can reduce IS misuse by implementing anti-virus software, using password protection systems, enforcing information security policies, and fostering employee information security awareness through effective security education programs.

2.2. Procedural Security Countermeasures

Organisational strategies for reducing IS misuse generally fall into four stages – deterrence, prevention, detection, and recovery. These four stages are collectively referred to as the *Security Action Cycle* (Straub and Welke, 1998). Based on this model, effective IS security management should aim to maximise the number of deterred and prevented incidents of non-compliant behaviour and minimise those that are detected and punished. Our study concentrates on stage one of the Security Action Cycle – that is, deterrent mechanisms for the effective management of employee security behaviour. In accordance with Straub and Welke's (1998) framework, this phase refers to the use of deterrent security countermeasures such as information security policies and security education in order to encourage desirable behaviour.

An information security policy defines rules and guidelines for the proper use of organisational IS resources. In line with a deterrence perspective, security policies rely on the same fundamental mechanisms as societal laws, – that is outlining knowledge of what constitutes illicit behaviour increases the perceived threat of punishment for unacceptable actions (D'Arcy et al., 2009). Security education has a similar deterrent effect through ongoing security training. The ultimate purpose of training is to remind users of the guidelines regarding the acceptable usage of

information systems and the potential outcomes in the event that users circumvent the outlined rules.

2.3. Organisational Culture

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. As a result, numerous definitions, conceptualisations, and dimensions of culture were produced by researchers. For example, Kroeber and Kluckhohn (1952) identified 164 definitions of culture. Kovačić (2005) argued that since then the number of definitions has increased to approximately 400. They range from simple to complex, incorporate and extend previous definitions, and even contradict prior definitions. Furthermore, some researchers offer more than one definition of culture. Therefore, studying culture can be foreseen as a delicate assignment. As Straub et al. (2002, p.14) put it, "culture has always been a thorny concept and an even thornier research construct".

Organisational culture (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. For example, Kilmann (1985) describes OC as a separate and hidden force that controls behaviours and attitudes in organisations. A study conducted by Porter and McLaughlin (2006) further demonstrated the significant role that organisational climate plays in shaping employee behaviour. Philips (1984) portrays culture as a set of tacit assumptions that guide acceptable perceptions, thoughts, feelings, and behaviour among members of the group. Baker (1980) emphasised the importance of OC as power that can lead a company to success or weaken its vitality because organisational culture directly affects employee behaviour in an organisation.

2.4. Organisational Culture Values

OC has been conceptualised in terms of values that distinguish one organisation from another. The literature on OC has identified quite a variety of organisational values that may present themselves (Leidner and Kayworth, 2006). For the purposes of our study (as explained in section 3), we focussed on a confined set of OC values, namely *people-orientation*, *solidarity*, *sociability*, *task-orientation*, and *flat structure*, and investigated the impact of these values on individuals' behaviour. The 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).

2.5. Employee Security Behaviour

The subject of our interest in this study 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 that we examined were *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).

2.6. The Role of Information Security Awareness

Bulgurcu et al. (2010, p. 532) define *information security awareness* as "an employee's overall knowledge and understanding of potential information security-related issues and their ramifications, and what needs to be done in order to deal with security-related issues". Security-aware employees are familiar with the security practices and rules of an organisation as well as their responsibilities regarding organisational information resources and the consequences of abusing them, including loss of reputation, substantial financial losses, and even complete disruption of business. When employees understand the purpose of organisational security requirements, they tend to conform with organisational security rules (Bulgurcu et al., 2010).

Prior research confirms that public awareness can reduce certain illicit acts like drunk driving (Ferguson et al., 1999), shoplifting (Sacco, 1985), and workplace drug use (Quazi, 1993). Furthermore, Bulgurcu et al. (2010) and D'Arcy et al. (2009) emphasised the important role of user security awareness in encouraging compliant behaviour. Procedural security countermeasures are important organisational artifacts that raise employee awareness regarding potential security threats and consequences of devious behaviour (D'Arcy et al., 2009). In turn, the increased awareness has a positive impact upon security-related behaviours because employees tend to understand the importance of following organisational information security rules (Bulgurcu et al., 2010).

3. Research Approach

Our intention was to explore employee security behaviour from the perspective of study participants and to obtain rich qualitative findings that will help us to better understand it. The methodology adapted for this study draws on the *analytical grounded theory* (AGT) approach (Matavire and Brown, 2013) employing the

constant comparative method as elucidated 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.

Data collection was carried out using semi-structured in-person interviews. The interview guide was constructed following a thorough analysis of the literature. Questions were asked about OC values, procedural security countermeasures, information security awareness and the impact of these factors on employee security behaviour. 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. Interview guide topics including corresponding references and questions are illustrated in Table 1.

Elements of Conceptual Framework	Reference	Examples of questions
Information Security Policy	Cheng et al. (2013)	Is there an information security policy in your organisation?
Security Education	D'Arcy et al. (2009)	Do you ever attend information security training courses in your organisation?
Information Security Awareness	Bulgurcu et al. (2010)	What information security rules and practices are used in your organisation?
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?
Security Behaviour	Albrechtsen (2007)	Did your organisation ever experience an information security breach? If yes, did this incident affect your behaviour with regards to information security? If yes, then how?

Table 1: Interview Guide Topics

In total, 19 individuals were selected for interviews, drawn from organisations across a range of industry sectors. Nine interviews were conducted in the United States and ten in Ireland. Details about the interviewees and their organisations are given in Table 2. As the interviews progressed, it 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 under these two categories.

Organisation Name (aliases)	Industry type; Year 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 2: Profile of US and Irish Interviewees' Organisations

Organisations and participants were purposefully selected. We felt that it was important to interview organisations from a range of industries in order to capture data from organisations with various levels of security, our aim being to develop a holistic view of the research problem. The initial intent was to interview one person in a managerial position and one regular employee in each organisation in order to understand the views of both an experienced user and someone with little (if any) experience in the area of information security. Although this proved to be difficult due to the access issues, out of 19 interviewees that did participate, eight had expert knowledge on the topic of information security, six had very good knowledge, and the remaining five had basic knowledge regarding information security.

The principle of theoretical sampling was employed in order to guide data collection. Data collection was divided into four stages. In the opening stage (Stage 1), four US organisations of various sizes and with different levels of security were selected, particularly RetCoUS, FinCoUS, PublCoUS, and CivEngCoUS. Four interviews, - one in each organisation, - were conducted. This data was analysed (Phases 1 and 2 of data analysis) in order to guide further data collection. Phase 1 of data analysis involved the segmentation of the body of data into discrete 'incidents' (Glaser and Strauss, 1967). In Phase 2, a set of first-round provisional categories was generated, to which the segmented data would be coded. These categories took two forms: participant-driven and researcher-driven. 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. As the process unfolded, connections between emerged categories started to arise, including both positive and negative cases (see Table 3).

Emerged Associations
Information Security Policy and Increased Information Security Awareness Lack of Information Security Policy and Lack of Information Security Awareness
Security Education and Increased Information Security Awareness Lack of Security Education and Lack of Information Security Awareness
Increased Information Security Awareness and Compliant Behaviour Lack of Information Security Awareness and Non-Compliant Behaviour
High People-Orientation and Compliant Behaviour Low People-Orientation and Non-Compliant Behaviour
High Solidarity and Compliant Behaviour Low Solidarity and Non-Compliant Behaviour
High Sociability and Non-Compliant Behaviour
High Task-Orientation and Non-Compliant Behaviour
Flat Structure and Improved Information Security

Table 3: Results of Phases 1 and 2 (US interviews)

Following the emerged associations between the aforementioned concepts, the next step of data collection (Stage 2) was to interview organisations where procedural security countermeasures were either present or absent in order to find out how these controls tend to influence security behaviour. Furthermore, we aimed to select organisations where the abovementioned organisational culture values would prevail. It was also important to choose interviewees with different levels of knowledge in the area of information security in order to discover the role of information security awareness. To meet this criteria, a short questionnaire was conducted over the phone with potential participants. Subsequently, a further five interviews were conducted in organisations CloudSerUS, TechCorpUS, and EducInstUS. The body of data was analysed again (Phases 1 and 2 of data analysis, see Figure 1) and provisional results have confirmed the associations emerged in Stage 1.

Next, the same process was repeated in Ireland. In particular, Stage 3 involved selecting comparable organisations in terms of the size and level of security, including BankOrgIrl, CharOrgIrl, ResRegIrl, BevCorpIrl, and PublOrgIrl. Five interviews were conducted in these organisations (one in each organisation) and subsequently analysed (Phases 1 and 2 of data analysis). Concepts and associations between these concepts started to emerge and were identical to the provisional findings discovered in the US organisations interviewed in Stage 1 of data collection (please refer to Table 3). Therefore, the selection criteria for Stage 4 was identical to the criteria used to choose organisations in the United States for Stage 2. Three organisations located in Ireland (TechCorpIrl, TelCommCorpIrl, and EducOrgIrl), which were comparable with the US organisations selected in Stage 2 in terms of the size and level of security, were chosen for further interviewing. Five more interviews were conducted in these organisations. The interviews were transcribed and analysed (Phases 1 and 2 of data analysis) and the results confirmed the associations that had emerged in Stages 1 and 3 (Table 3). It is important to note that our study's findings are based on the data combined from both data sets – US and Ireland).

The following phase of data analysis (Phase 3 - Coding on) involved merging both data sets and further breaking down incidents of data identified in the first phase in order to offer a 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. As a 'rule of inclusion' was developed for each 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 redefined, and new categories emerged. Subsequently, data reduction (Phase 5) was performed in order to emphasise findings relevant to the objectives of this study. Finally, Phase 6 involved writing analytical memos and validating the proposed findings by seeking evidence in data. Eisenhardt (1989) argued that theoretical saturation is reached when a researcher is observing phenomena that have been seen before and therefore, incremental learning becomes minimal. We felt that we had reached the point of theoretical saturation after 19 interviews in total had been conducted.

4. Research Findings and Discussion

Our findings indicate that procedural security countermeasures and OC values tend to affect employee security behaviour in organisational settings (Fig. 1). In particular, information security policy and security education tend to increase information security awareness. This awareness, in turn, is inclined to lead to compliant behaviour. Furthermore, OC values of *solidarity* and *people-orientation* are positively associated with security behaviours, while *sociability*, and *task-orientation* tend to have a negative effect on security-related actions. Additionally, a *flat structure* is inclined to encourage employees to address issues related to information security and therefore, *improves the overall level of information security* in organisations.

4.1. Information Security Policy

Study informants from ClousSerUS, TechCorpIrl, TechCorpUS, and RetCoUS suggest that a policy tends to increase employee security awareness. At TechCorpIrl, information security is a top priority so there is a detailed information security policy in place that outlines organisational information security requirements and instructs employees in terms of appropriate and inappropriate actions. Their Product Manager expressed his view that:

> "[when a security policy is present], people are very conscious of what is appropriate and what is not appropriate because the policy dictates what they can do and what they cannot do..."

As another example, a Software Developer from ClousSerUS believes that the information security policy tends to increase information security awareness and hence, leads to compliant behaviour. He stresses that when the information security

policy is present, employees understand what "good" and what "bad" behaviour is and act accordingly:

> "When there are no security policies, employees generally do not know what is right and what is wrong... therefore, employees are probably more susceptible to doing something that one may not think is wrong. [When policy is present], people are very conscious of what is appropriate and what is not appropriate because the policy dictates what they can do and what they cannot do…"

Our findings demonstrate that a security policy tends to enhance awareness about information security. Typically, a security policy aims to outline organisational information security requirements and the rules that derive from these requirements. Furthermore, security policies provide information on sanctions in the event of non-compliant behaviour, and rewards to encourage compliant behaviour. Our findings are consistent with Straub (1990) and Chan et al. (2005), confirming that the establishment of information security policies in organisations is vital to encourage security compliant behaviour. However, in contrast with Straub (1990) and Chan et al. (2005), we found that security policies affect employee actions indirectly through information security awareness. The notion of information security awareness, as distinct from security policy, has been largely overlooked in prior research. The surprising finding of Lee et al. (2004) that an information security policy has no impact on IS misuse behaviour, which is at odds with our findings, could be explained by the employees' lack of awareness in the first instance of the security policy. It is not merely enough to formulate security policy; awareness of policy must be promulgated through appropriate education and training of staff.

4.2. Security Education

Study participants from CloudSerUS, TechCorpUS, TechCorpIrl, and CharOrgIrl reveal that security education tends to increase employee information security awareness. An IT Executive from TechCorpIrl comments:

> "When a new member of staff starts, they have to do a generic training to increase their understanding [about security], so that they do not compromise the company..."

Conversely, study participants from organisations such as BankOrgIrl, EducOrgIrl, TelCommCorpIrl, and CivEngCoUS, share that the lack of security education tends to lead to the lack of information security awareness. For example, a Security Executive of TechCorpIrl notes:

> "A lot of security issues are associated with human ignorance. I think there is an aspect of what people do not know. If they do not know, it then causes the gaps and exposures."

Overall, our results demonstrate that security education tends to enhance awareness about information security. The purpose of security training is to educate employees on how to protect vital organisational assets and why a certain set of rules must be

implemented. The 'why' is particularly important because if employees underestimate the significance of a certain rule, they may not be able to justify the extra effort they need to make in order to follow the rule, and, consequently, violate information security requirements. Additionally, when employees fail to understand the reason behind security rules, they may give inaccurate interpretation of their presence and, consequently, misjudge the importance of security requirements.

Security education appeals to employees' conscience by providing details of dreadful consequences that an organisation may experience in the event of a security breach. Fear appeals are induced when consequences for the offender are outlined during security education sessions. Once all these aspects are covered through security education (e.g. how to protect sensitive information, why there is a need to follow rules, consequences of non-conformity for both the organisation and the offender), employees become security-conscious and therefore, are inclined to follow rules. In contrast with the previous finding of Lee et al. (2004) that awareness programs have no significant impact on behaviour, we found that security education tends to lead to compliant behaviour. Furnell et al. (2002) argued that user information security knowledge is critical to ensure compliance and can be delivered to end-users through education and training. While studies by Straub (1990), Siponen et al. (2009), and Barlow et al. (2013) indicated that security education has a direct effect on employee security actions, it must be noted that information security awareness is an outcome of security education and therefore, security education tends to lead to compliant behaviour indirectly, through security awareness.

4.3. Information Security Awareness

Study participants from CloudSerUS, CharOrgIrl, TechCorpUS, and EducInstUS share that employee security awareness tends to lead to compliant behaviour. In particular, a Software Developer from CloudSerUS reports the following:

> "When [employees] generally know that there is a good reason for not doing something, they tend to adhere to the information security policy… But if [employees] do not know, then it is bad..."

On the other hand, study informants from BevCorpIrl, EducOrgIrl, and EducInstUS report that the lack of information security awareness prompts employees to circumvent information security rules or exercise poor practices. An IT Executive from BevCorpIrl shares:

> "Information security rules are useful... But I can see why people circumvent them. Employees are not seeing the implications of why the rule is in place. So they just see it as a challenge to bypass a system…"

The above statements confirm that employee information security awareness is an important factor that tends promote compliant behaviour. In particular, study participants reveal that when employees understand that there is a good reason behind a certain rule, they exercise safe practices. Knowledge about consequences of non-compliant behaviour is vital. On the other hand, when employees do not understand why a certain rule is in place, they try to bypass it as they perceive it as a

barrier to perform their main duties. Bulgurcu et al. (2010) and D'Arcy et al. (2009) confirmed the important role of information security awareness, suggesting that when users are aware that security policies exist, they are less likely to engage in IS policies misuse. Our findings are in accord with these studies. Although Lee et al. (2004) reported that degree of security awareness has no impact on employees' actions, our findings show the opposite.

4.4. People-Orientation

In both Ireland and US, several informants from TechCorpIrl, BankOrgIrl, CharOrgIrl, BevCorpIrl, CloudSerUS, RetCoUS, TechCorpUS, FinCoUS believe that high people-orienation encourages information security compliance, while low people-orientation tends to have a negative effect on employee security behaviour as expressed by interviewees from BevCorpIrl, EducOrgIrl, and CivEngCoUS. For example, RetCoUS puts a 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".

Our data impels us to conclude that an organisational value of people-orientation tends to lead to compliant 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 of *people-orientation* in order to encourage compliance with information security rules.

4.5. Solidarity

In both countries, four study participants from CloudSerUS, TechCorpUS, and EducOrgIrl believe that a high level of solidarity is inclined to promote compliant 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 shared his view:

> "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".

We found 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.

4.6. Sociability

In both countries, study participants from EducInstUS, CharOrgIrl, EducOrgIrl, TelCommCorpIrl, and ResRegIrl suggest that high sociability tends to 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.

4.7. 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 is inclined to have 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.

4.8. 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 tends to improve the overall level of security in organisations. When management is 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".

Our results suggest that flat structure tends to improve 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

Our results show that information security policies and security education tend to increase employee information security awareness. In turn, the awareness is inclined to lead to compliant behaviour. These insights extend general deterrence theory in a novel way. In particular, the deterrent effect of procedural security countermeasures increases information security awareness. This awareness, in turn, tends to deter malicious actions of employees and encourage security-cautious behaviour. Furthermore, general deterrence theory is typically used to study negative behaviours, while there are calls in the literature to apply the theory across the variety of behaviours, including negative and positive (D'Arcy and Herath, 2011). The focus of this study is both negative and positive behaviours, which further extends general deterrence theory.

Furthermore, OC values are inclined 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. Moreover, *high solidarity* tends to lead to compliant behaviour because employees realise and pursue organisational goals. Next, *high sociability* and *high task-orientation* tend to encourage non-compliant behaviour. Finally, *flat structure* is inclined to improve the overall level of information security in an organisation.

This study makes an important research contribution. The extant security research tends to focus on technical issues as opposed to the behaviour of individual users. On

the contrary, our study builds on general deterrence theory and prior organisational culture literature to make an empirical contribution, which takes its place amongst the very few studies in Behavioural InfoSec research that investigate how procedural security countermeasures and organisational culture affect employee security behaviour. Further, prior studies that investigate the impact of procedural security countermeasures on employee security behaviour report contradictory and therefore, inconclusive results. This research provides empirical evidence that procedural security countermeasures, including information security policies and security education, tend to lead to compliant behaviour. Moreover, prior research that focuses on procedural security countermeasures, tend to investigate the direct effect of these measures on employee security behaviour. Therefore, the role of information security awareness has been neglected in the extant literature. Our research emphasises the important role of information security awareness.

Our results also have important practical implications. First, this study highlights the important role of procedural security countermeasures in managing illicit actions in organisations. Security practitioners must realise that focusing on technical measures alone puts organisations at higher risk of security breaches occurring due to "human error". Second, since information security awareness is the key factor in encouraging compliant behaviour, IS security managers must design security education and policies with the aim to increase awareness about security threats and consequences of information security breaches. In particular, real life incidents should be part of security education. Employee awareness that a security breach may lead to organisation's bankruptcy and complete shutdown and consequently, their job loss, would be a strong drive to comply with organisational information security requirements. Third, security practitioners must take in consideration the effect of OC values on employee security behaviour. Organisational culture can be assessed and changed if required.

An additional and important contribution of this study is in its methodology. While studies in the Behavioural InfoSec field make a valuable contribution to the pool of Behavioural InfoSec research, quantitative methodologies prevail in this research stream. Crossler et al. (2013), however, brought attention to the methodological challenges of quantitative methods and called for more studies that employ alternative methods, including qualitative. Moreover, Straub (1990) pointed out that "qualitative studies would enhance our [quantitative] perspective." In particular, in our study we had a personal contact with interviewees, which allowed to probe and hence, grasp a deeper understanding of the central phenomenon of this study, that is security behaviour in organisations, as well as factors that tend to affect employee actions.

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 builds on existing theories to make an empirical contribution, which takes its place amongst the very few studies in Behavioural InfoSec research that investigate how procedural security countermeasures and organisational culture that affect employee security behaviour.

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 Srite, 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.