



Deposited via The University of Leeds.

White Rose Research Online URL for this paper:

<https://eprints.whiterose.ac.uk/id/eprint/114696/>

Version: Accepted Version

---

**Article:**

Yuryna Connolly, A, Lang, M, Gathegi, J et al. (2017) Organisational Culture, Procedural Countermeasures, and Employee Security Behaviour: A Qualitative Study. *Information and Computer Security*, 25 (2). pp. 118-136. ISSN: 2056-4961

<https://doi.org/10.1108/ICS-03-2017-0013>

---

(c) 2017, Emerald. This is an author produced version of a paper published in *Information and Computer Security*. Uploaded in accordance with the publisher's self-archiving policy.

**Reuse**

Items deposited in White Rose Research Online are protected by copyright, with all rights reserved unless indicated otherwise. They may be downloaded and/or printed for private study, or other acts as permitted by national copyright laws. The publisher or other rights holders may allow further reproduction and re-use of the full text version. This is indicated by the licence information on the White Rose Research Online record for the item.

**Takedown**

If you consider content in White Rose Research Online to be in breach of UK law, please notify us by emailing [eprints@whiterose.ac.uk](mailto:eprints@whiterose.ac.uk) including the URL of the record and the reason for the withdrawal request.



**Organisational Culture, Procedural Countermeasures, and Employee Security Behaviour: A Qualitative Study**

Journal:	<i>Information and Computer Security</i>
Manuscript ID	ICS-03-2017-0013
Manuscript Type:	Original Article
Keywords:	Employee Security Behaviour, Organisational Culture, Information Security Policy, Security Education, Information Security Awareness

SCHOLARONE™  
Manuscripts

Information and Computer Security

# Organisational Culture, Procedural Countermeasures, and Employee Security Behaviour: A Qualitative Study

Research Paper<sup>1</sup>

## 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

---

<sup>1</sup> This research is based upon work done at the National University of Ireland, Galway and the University of California, Berkeley

1 started to include social means in their malicious efforts, e.g. social engineering, the  
2 need for a holistic approach in addressing information security issues has emerged.  
3 The domain of behavioural information security (InfoSec) research highlights the  
4 importance of taking into consideration the “human” element when ensuring  
5 information security throughout the organisation. Research and practice have shown  
6 that technical tools are powerless when it comes to the enforcement of behavioural  
7 rules such as password sharing, reporting of security incidents, adherence to a clear  
8 desk policy, and the secure disposal of confidential documents. Rather, compliance  
9 with these rules entirely depends on employees’ motivation to conform. Therefore, it  
10 is essential to understand factors that lead to compliant behaviour or that prompt  
11 employees to break organisational information security rules. This study provides new  
12 insights about security behaviour in selected U.S. and Irish organisations by  
13 investigating how organisational culture and procedural security countermeasures  
14 influence security actions. Crossler *et al.* (2013, p.90) note that “although a  
15 predominant weakness in properly securing information assets is the individual user  
16 within an organization, much of the focus of extant security research is on technical  
17 issues”. In response, our work takes its place amongst the small number studies to date  
18 that focus on behavioural as opposed to technical issues.

19  
20 Generally, Behavioural InfoSec research falls into two broad categories: (1) those that  
21 focus on the effects of cognitive processes on employee security behaviour (Bulgurcu  
22 *et al.*, 2010), and (2) the effect of social controls (Cheng *et al.*, 2013). This study  
23 concentrates on the latter. The two basic forms of social controls are formal and  
24 informal (Ross, 1896). Formal social controls refer to rules and regulations against  
25 deviant behaviour (Cheng *et al.*, 2013). Organisational sanctions, rewards, security  
26 education and training, and information security policies are all forms of formal  
27 organisational controls. There is an abundance of research within the field of  
28 Information Systems (IS) on how formal organisational controls influence security  
29 behaviour. Bulgurcu *et al.* (2010) and Hu *et al.* (2011) emphasise the vital role of  
30 sanctions and rewards in managing security behaviour in organisational settings. Chen  
31 *et al.* (2012) and Siponen *et al.* (2009) assert the importance of security policies and  
32 education as factors that deter malicious actions of employees. Our research focuses  
33 on the effect of information security policies and security education on employee  
34 security education. Following Hovav and D’Arcy (2012), these security controls are  
35 collectively referred to as “procedural security countermeasures”.

36 Although Behavioural InfoSec research has seen some expansion in the past few years,  
37 it is still in a developing phase. Some prior literature provides evidence that procedural  
38 security countermeasures reduce IS misuse (Straub 1990; Siponen *et al.*, 2009), while  
39 other studies contradict these findings (Lee *et al.*, 2004). Straub (1990) and Chan *et al.*  
40 (2005) found that security policies were associated with lower levels of computer  
41 abuse. Similarly, Siponen *et al.* (2009) and Barlow *et al.* (2013) reported that security  
42 education is an important predictor of security-compliant behaviour. On the contrary,  
43 Lee *et al.* (2004) concluded that security policies and security awareness programs do  
44 not reduce IS misuse.

45  
46 Undeniably, these previous studies are highly informative. However, they investigated  
47 the direct effect of procedural security countermeasures on employee security  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60

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 into 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

Please insert Figure 1

### 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 has been 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

1 deterred and prevented incidents of non-compliant behaviour and minimise those that  
2 are detected and punished. Our study concentrates on stage one of the Security Action  
3 Cycle – that is, deterrent mechanisms for the effective management of employee  
4 security behaviour. In accordance with Straub and Welke's (1998) framework, this  
5 phase refers to the use of deterrent security countermeasures such as information  
6 security policies and security education in order to encourage desirable behaviour.  
7

8 An information security policy defines rules and guidelines for the proper use of  
9 organisational IS resources. In line with a deterrence perspective, security policies rely  
10 on the same fundamental mechanisms as societal laws, – that is outlining knowledge  
11 of what constitutes illicit behaviour increases the perceived threat of punishment for  
12 unacceptable actions (D'Arcy *et al.*, 2009). Security education has a similar deterrent  
13 effect through ongoing security training. The ultimate purpose of training is to remind  
14 users of the guidelines regarding the acceptable usage of information systems and the  
15 potential outcomes in the event that users circumvent the outlined rules.  
16

### 17 **2.3. Organisational Culture**

18 The study of culture is rooted in sociology, social psychology, and anthropology (Ali  
19 and Brooks, 2009). Culture has been studied for over a hundred years in various  
20 disciplines. As a result, numerous definitions, conceptualisations, and dimensions of  
21 culture were produced by researchers. For example, Kroeber and Kluckhohn (1952)  
22 identified 164 definitions of culture. Kovačić (2005) argued that since then the number  
23 of definitions has increased to approximately 400. They range from simple to complex,  
24 incorporate and extend previous definitions, and even contradict prior definitions.  
25 Furthermore, some researchers offer more than one definition of culture. Therefore,  
26 studying culture can be a delicate assignment. As Straub *et al.* (2002, p.14) put it,  
27 "culture has always been a thorny concept and an even thornier research construct".  
28

29 OC is defined in this research project as "culture shared between people working in an  
30 organisation" (Ali and Brooks, 2009, p. 550). Prior research shows that OC has an  
31 impact on individuals' behaviour. For example, Kilmann (1985) describes OC as a  
32 separate and hidden force that controls behaviours and attitudes in organisations. A  
33 study conducted by Porter and McLaughlin (2006) further demonstrated the significant  
34 role that organisational climate plays in shaping employee behaviour. Philips (1984)  
35 portrays culture as a set of tacit assumptions that guide acceptable perceptions,  
36 thoughts, feelings, and behaviour among members of the group. Baker (1980)  
37 emphasised the importance of OC as power that can lead a company to success or  
38 weaken its vitality, because organisational culture directly affects employee behaviour  
39 in an organisation.  
40

### 41 **2.4. Organisational Culture Values**

42 OC has been conceptualised in terms of values that distinguish one organisation from  
43 another. The literature on OC has identified quite a variety of organisational values  
44 that may present themselves (Leidner and Kayworth, 2006). For the purposes of our  
45 study (as explained in section 3), we focussed on a confined set of OC values, namely  
46 *people-orientation*, *solidarity*, *sociability*, *task-orientation*, and *flat structure*, and  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60

1 investigated the impact of these values on individuals' behaviour. The organisational  
2 value of *people-orientation* refers to organisations that are "concerned with people  
3 issues" (Cooke and Lafferty, 1987, p. 52). Goffee and Jones (1996, p.134) define  
4 *solidarity* as "a measure of community's ability to pursue shared objectives quickly  
5 and effectively regardless of personal ties" and *sociability* as "the measure of sincere  
6 friendliness among members of a community". *Task-orientation* is defined as  
7 "concern for efficiency" (Cooke and Lafferty, 1987, p.54). Finally, *flat structure* is an  
8 organisational structure that aims to reduce "the number of layers of management  
9 hierarchy" (Kettley, 1995, p.1).

### 10 11 **2.5. Employee Security Behaviour**

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

19 The two types of employee security behaviour that we examined were *compliant*  
20 *behaviour* (i.e. adhering to the policies, procedures, and norms of an organisation in  
21 relation to information security) and *non-compliant behaviour* (i.e. intentional but non-  
22 malicious behaviours of employees that may put organisational information systems  
23 at risk and entail non-compliance to the policies, procedures, and norms of an  
24 organisation in relation to information security).

### 25 26 27 28 **2.6. The Role of Information Security Awareness**

29 Bulgurcu *et al.* (2010, p. 532) define *information security awareness* as "an  
30 employee's overall knowledge and understanding of potential information security-  
31 related issues and their ramifications, and what needs to be done in order to deal with  
32 security-related issues". Security-aware employees are familiar with the security  
33 practices and rules of an organisation as well as their responsibilities regarding  
34 organisational information resources and the consequences of abusing them, including  
35 loss of reputation, substantial financial losses, and even complete disruption of  
36 business. When employees understand the purpose of organisational security  
37 requirements, they tend to conform with organisational security rules (Bulgurcu *et al.*,  
38 2010).

39 Prior research confirms that public awareness can reduce certain illicit acts like drunk  
40 driving (Ferguson *et al.*, 1999), shoplifting (Sacco, 1985), and workplace drug use  
41 (Quazi, 1993). Furthermore, Bulgurcu *et al.* (2010) and D'Arcy *et al.* (2009)  
42 emphasised the important role of user security awareness in encouraging compliant  
43 behaviour. Procedural security countermeasures are important organisational artifacts  
44 that raise employee awareness regarding potential security threats and consequences  
45 of devious behaviour (D'Arcy *et al.*, 2009). In turn, the increased awareness has a  
46 positive impact upon security-related behaviours because employees tend to  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60

1 understand the importance of following organisational information security rules  
2 (Bulgurcu *et al.*, 2010).

### 3. Research Approach

3 Our intention was to explore employee security behaviour from the perspective of  
4 study participants and to obtain rich qualitative findings that will help us to better  
5 understand it. The methodology adapted for this study draws on the *analytical*  
6 *grounded theory* approach (Matavire and Brown, 2013) employing the *constant*  
7 *comparative method* as elucidated by Maykut and Morehouse (1994). The method  
8 used in this study is characterised by a mix of description and interpretation of data,  
9 the outcome of which is an interpretive-explanatory framework supported by  
10 participants' quotes.

11 Data collection was carried out using semi-structured in-person interviews. The  
12 interview guide was constructed following a thorough analysis of the literature.  
13 Questions were asked about OC values, procedural security countermeasures,  
14 information security awareness and the impact of these factors on employee security  
15 behaviour. As regards the questions about OC, there is a wide range of OC models  
16 employed within IS research. A list of the most prominent OC frameworks was  
17 borrowed from Leidner and Kayworth's (2006) work, producing over 20  
18 organisational values. These values were then grouped into broader categories due to  
19 their evident similarities, including *people-orientation*, *solidarity*, *sociability*,  
20 *hierarchy*, *task-orientation*, and *rule-orientation*, and interview questions were  
21 constructed around these themes. Interview guide topics including corresponding  
22 references and questions are illustrated in Table 1.

23 *Please insert Table 1*

24 In total, 19 individuals were selected for interviews, drawn from organisations across  
25 a range of industry sectors. Nine interviews were conducted in the United States and  
26 ten in Ireland. Details about the interviewees and their organisations are given in Table  
27 2. As the interviews progressed, it became evident that we would not be able to make  
28 conclusions about the influence of *hierarchy* and *rule-orientation* on employee  
29 security behaviour due to insufficient data under these two categories.

30 *Please insert Table 2*

31 Organisations and participants were purposefully selected. We felt that it was  
32 important to interview organisations from a range of industries in order to capture data  
33 from organisations with various levels of security, our aim being to develop a holistic  
34 view of the research problem. The initial intent was to interview one person in a  
35 managerial position and one regular employee in each organisation in order to  
36 understand the views of both an experienced user and someone with little (if any)  
37 experience in the area of information security. Although this proved to be difficult due  
38 to the access issues, out of 19 interviewees that did participate, eight had expert  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60

1 knowledge on the topic of information security, six had very good knowledge, and the  
2 remaining five had basic knowledge regarding information security.

3  
4 The principle of theoretical sampling was employed in order to guide data collection.  
5 Data collection was divided into four stages. In the opening stage (Stage 1), four US  
6 organisations of various sizes and with different levels of security were selected,  
7 particularly RetCoUS, FinCoUS, PublCoUS, and CivEngCoUS. Four interviews, -  
8 one in each organisation, - were conducted. This data was analysed (Phases 1 and 2 of  
9 data analysis) in order to guide further data collection. Phase 1 of data analysis  
10 involved the segmentation of the body of data into discrete 'incidents' (Glaser and  
11 Strauss, 1967). In Phase 2, a set of first-round provisional categories was generated, to  
12 which the segmented data would be coded. These categories took two forms:  
13 participant-driven and researcher-driven. Having segmented and labelled the body of  
14 data and generated a set of first-round provisional categories, one-third of incidents or  
15 units were examined and placed into one or more of these categories and analysis of  
16 their content gave rise to the formation of additional provisional categories. As the  
17 process unfolded, connections between emerged categories started to arise, including  
18 both positive and negative cases (see Table 3).

19  
20 *Please insert Table 3*

21  
22 Following the emerged associations between the aforementioned concepts, the next  
23 step of data collection (Stage 2) was to interview organisations where procedural  
24 security countermeasures were either present or absent in order to find out how these  
25 controls tend to influence security behaviour. Furthermore, we aimed to select  
26 organisations where the abovementioned organisational culture values would prevail.  
27 It was also important to choose interviewees with different levels of knowledge in the  
28 area of information security in order to discover the role of information security  
29 awareness. To meet this criteria, a short questionnaire was conducted over the phone  
30 with potential participants. Subsequently, a further five interviews were conducted in  
31 organisations CloudSerUS, TechCorpUS, and EducInstUS. The body of data was  
32 analysed again (Phases 1 and 2 of data analysis, see Figure 1) and provisional results  
33 have confirmed the associations emerged in Stage 1.

34  
35 Next, the same process was repeated in Ireland. In particular, Stage 3 involved  
36 selecting comparable organisations in terms of the size and level of security, including  
37 BankOrgIrl, CharOrgIrl, ResRegIrl, BevCorpIrl, and PublOrgIrl. Five interviews were  
38 conducted in these organisations (one in each organisation) and subsequently analysed  
39 (Phases 1 and 2 of data analysis). Concepts and associations between these concepts  
40 started to emerge and were identical to the provisional findings discovered in the US  
41 organisations interviewed in Stage 1 of data collection (please refer to Table 3).  
42 Therefore, the selection criteria for Stage 4 was identical to the criteria used to choose  
43 organisations in the United States for Stage 2. Three organisations located in Ireland  
44 (TechCorpIrl, TelCommCorpIrl, and EducOrgIrl), which were comparable with the  
45 US organisations selected in Stage 2 in terms of the size and level of security, were  
46 chosen for further interviewing. Five more interviews were conducted in these  
47 organisations. The interviews were transcribed and analysed (Phases 1 and 2 of data  
48 analysis) and the results confirmed the associations that had emerged in Stages 1 and  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60

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 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 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:

1                    “[when a security policy is present], people are very conscious of what is  
2                    appropriate and what is not appropriate because the policy dictates what they  
3                    can do and what they cannot do...”

4  
5                    As another example, a Software Developer from ClousSerUS believes that the  
6                    information security policy tends to increase information security awareness and  
7                    hence, leads to compliant behaviour. He stresses that when the information security  
8                    policy is present, employees understand what “good” and what “bad” behaviour is and  
9                    act accordingly:

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

16  
17                    Our findings demonstrate that a security policy tends to enhance awareness about  
18                    information security. Typically, a security policy aims to outline organisational  
19                    information security requirements and the rules that derive from these requirements.  
20                    Furthermore, security policies provide information on sanctions in the event of non-  
21                    compliant behaviour, and rewards to encourage compliant behaviour. Our findings are  
22                    consistent with Straub (1990) and Chan *et al.* (2005), confirming that the establishment  
23                    of information security policies in organisations is vital to encourage security  
24                    compliant behaviour. However, in contrast with Straub (1990) and Chan *et al.* (2005),  
25                    we found that security policies affect employee actions indirectly through information  
26                    security awareness. The notion of information security awareness, as distinct from  
27                    security policy, has been largely overlooked in prior research. The surprising finding  
28                    of Lee *et al.* (2004) that an information security policy has no impact on IS misuse  
29                    behaviour, which is at odds with our findings, could be explained by the employees’  
30                    lack of awareness in the first instance of the security policy. It is not merely enough to  
31                    formulate security policy; awareness of policy must be promulgated through  
32                    appropriate education and training of staff.

#### 33                    **4.2. Security Education**

34  
35                    Study participants from CloudSerUS, TechCorpUS, TechCorpIrl, and CharOrgIrl  
36                    reveal that security education tends to increase employee information security  
37                    awareness. An IT Executive from TechCorpIrl comments:

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

41  
42                    Conversely, study participants from organisations such as BankOrgIrl, EducOrgIrl,  
43                    TelCommCorpIrl, and CivEngCoUS, share that the lack of security education tends to  
44                    lead to the lack of information security awareness. For example, a Security Executive  
45                    of TechCorpIrl notes:  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60

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

4 Overall, our results demonstrate that security education tends to enhance awareness  
5 about information security. The purpose of security training is to educate employees  
6 on how to protect vital organisational assets and why a certain set of rules must be  
7 implemented. The ‘why’ is particularly important because if employees underestimate  
8 the significance of a certain rule, they may not be able to justify the extra effort they  
9 need to make in order to follow the rule, and, consequently, violate information  
10 security requirements. Additionally, when employees fail to understand the reason  
11 behind security rules, they may give inaccurate interpretation of their presence and,  
12 consequently, misjudge the importance of security requirements.

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

#### 30 31 **4.3. Information Security Awareness**

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

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

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

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

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60

1 The above statements confirm that employee information security awareness is an  
2 important factor that tends to promote compliant behaviour. In particular, study  
3 participants reveal that when employees understand that there is a good reason behind  
4 a certain rule, they exercise safe practices. Knowledge about consequences of non-  
5 compliant behaviour is vital. On the other hand, when employees do not understand  
6 why a certain rule is in place, they try to bypass it as they perceive it as a barrier to  
7 perform their main duties. Bulgurcu *et al.* (2010) and D'Arcy *et al.* (2009) confirmed  
8 the important role of information security awareness, suggesting that when users are  
9 aware that security policies exist, they are less likely to engage in IS policies misuse.  
10 Our findings are in accord with these studies. Although Lee *et al.* (2004) reported that  
11 degree of security awareness has no impact on employees' actions, our results show  
12 the opposite.

#### 13 **4.4. People-Orientation**

14 In both Ireland and US, several informants from TechCorpIrl, BankOrgIrl, CharOrgIrl,  
15 BevCorpIrl, CloudSerUS, RetCoUS, TechCorpUS, FinCoUS believe that high people-  
16 orientation encourages information security compliance, while low people-orientation  
17 tends to have a negative effect on employee security behaviour as expressed by  
18 interviewees from BevCorpIrl, EducOrgIrl, and CivEngCoUS. For example, RetCoUS  
19 puts a high value on employee satisfaction and ensures their members' happiness and  
20 health in order to promote information security compliance. A Security Executive  
21 from RetCoUS shares:

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

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

#### 39 **4.5. Solidarity**

40 In both countries, four study participants from CloudSerUS, TechCorpUS, and  
41 EducOrgIrl believe that a high level of solidarity is inclined to promote compliant  
42 behaviour. For example, CloudSerUS is an organisation that highly values the security  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60

1 of their assets and therefore, has in place various security measures and controls to  
2 protect valuable information. Employees realise a company's goal as regards to  
3 information security and demonstrate their solidarity by following information  
4 security rules. A Software Developer from CloudSerUS shared his view:

5  
6 "Everybody understands that security is a big concern from a lot of  
7 aspects...people do tend to adhere to a policy just because it is there... nobody  
8 has tried to violate information security rules".

9  
10 We found that when employees realise and share organisational goals, and the goal is  
11 to protect sensitive information, they are more likely to comply with organisational  
12 security requirements. Furthermore, if employees understand that, generally,  
13 exercising good security practices is important for their organisation, they follow safe  
14 practices even if the organisation itself does not enforce them. Hence, solidarity  
15 encourages behaviour that supports an organisation. These results are in accordance  
16 with contemporary literature. In particular, Long (1978) demonstrated a link between  
17 employee ownership and behaviour that supports the organisation. Guo and Yuan  
18 (2012) reported that employees prefer to conduct within social norms of their  
19 particular workgroup. Cheng *et al.* (2013) concluded that attachment to one's  
20 organisation and commitment discourage security violations in organisations.  
21 Therefore, it is important to promote *solidarity* among employees, which can be done  
22 via a good benefit system, favourable working conditions, and opportunities to realise  
23 potential.

#### 24 **4.6. Sociability**

25  
26 In both countries, study participants from EducInstUS, CharOrgIrl, EducOrgIrl,  
27 TelCommCorpIrl, and ResRegIrl suggest that high sociability tends to encourage non-  
28 compliant behaviour. For example, a Software Developer from TelCommCorpIrl  
29 shares:

30  
31 "People are probably more lax in terms of information security because of a  
32 friendly atmosphere...If the PC police were beside our cubicle, we would be all  
33 fired a long time ago...especially a guy beside me...we always slag him that the  
34 HR are coming for him."

35  
36 Although high sociability forms a special bond between employees, where employees  
37 begin to trust each other and work as a team, it may also create an informal atmosphere  
38 and therefore, drive wrong behaviours. Organisational members may not take any  
39 form of formality or authority seriously like managers instructions or organisational  
40 rules. High sociability is therefore detrimental unless management can preserve a  
41 required level of professionalism. Subsequently, employees will realise that although  
42 management is friendly, they still represent organisational authority and therefore,  
43 their orders and instructions are a requirement as the obligation to follow information  
44 security rules. Although friendliness has a lot of advantages (e.g. openness to new  
45 ideas, teamwork), there are also drawbacks. For example, the prevalence of friendships  
46 may allow poor performance to be accepted as no one wants to rebuke or fire a friend  
47 (Goffee and Jones, 1996). As a result, when rules get broken, it can be deliberately  
48 overlooked. Rashid *et al.* (2004) added that a friendly environment can breed  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60

1 mediocrity among employees. Normally, friends are reluctant to disagree with or  
2 challenge one another, which can lead to an exaggerated concern for consensus and  
3 subsequently, to a loss of focus on a company's mission and goals.

#### 4 **4.7. Task-Orientation**

5  
6 Study participants from both countries from BevCorpIrl, ResRegIrl, FinCoUS, and  
7 EducInstUS believe that work pressure pushes them to break rules with regards to  
8 information security. For example, an IT Executive from BevCorpIrl notes:

9  
10  
11 “Sometimes IT security policies and procedures are a barrier to getting things  
12 done as quickly and as correctly as possible. And if you are being rewarded  
13 for getting stuff done quicker...it is going to happen [that information security  
14 rules will be broken]. I definitely think that.”

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

21  
22 This inference is confirmed in the extant literature (Albrechtsen, 2007; Bulgurcu *et al.*,  
23 2010). For example, Bulgurcu *et al.* (2010) argued that commonly employees perceive  
24 information security rules as inconvenience and obstruction to meet daily work  
25 requirements. Albrechtsen (2007) concluded that employees circumvent information  
26 security rules if the rules are a barrier to productivity. In organisations that put high  
27 emphasis on results, employees may feel oppressed due to continuous stress and  
28 pressure, which may result in negative feelings about an organisation. In turn, ill  
29 feelings can have a negative effect on employee compliance with information security  
30 rules (Cavallari, 2012).

31  
32 Therefore, it is up to organisational leaders to find a balance between employees' daily  
33 commitments and information security requirements. Our results indicate that security  
34 staff should take feedback from employees and adjust security requirements  
35 accordingly. It is meaningless to have rules in place that are impossible or hard to  
36 implement in practice. Top management and security staff should work as one unit in  
37 order to find the balance between employee workload and their obligations related to  
38 information security.

#### 39 **4.8. Flat Structure**

40  
41 The organisational value of flat structure has emerged as the opposite value to  
42 hierarchy. Study participants from PublCoUS, RetCoUS, TechCorpUS, FinCoUS,  
43 TechCorpIrl, TelCommCorpIrl, CloudSerUS, and CharOrgIrl believe that flat  
44 structure tends to improve the overall level of security in organisations. When  
45 management is open to suggestions, employees freely express their concerns and  
46 problems, which, in turn, may improve the level of information security in  
47 organisations. For example, an IT Executive from TechCorpIrl shares that  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60

1 management tends to encourage employees to speak their mind in order to improve  
2 their processes:

3  
4 “I am approachable...I guess this would just reinforce the strength of  
5 information security because I believe if people were to feel there was some  
6 type of a problem or issue, they would not hesitate to talk to me about it”.

7  
8 Our results suggest that flat structure tends to improve information security. In  
9 particular, accessibility and approachability of management increases visibility for  
10 information security throughout the organisation. Furthermore, if employees become  
11 aware of any problem, they are more likely to express their concerns to a manager and  
12 possibly improve current processes or rules, which will benefit an organisation in the  
13 long-run. Acquiring user perspective on some issues is especially important because  
14 managers or policy makers may not be familiar with all aspects of working  
15 environments.

16  
17 This finding is in line with results reported in the extant literature. In particular,  
18 Chipperfield and Furnell (2010) stressed that in flatter organisations, management is  
19 easy to approach and therefore employees freely address concerns. Pearson (1987)  
20 asserted that a flat structure empowers employees to protect organisational interests  
21 because employees and leaders share a common set of values and feel personal  
22 ownership for the success of their organisation. As a result, employees will not hesitate  
23 to speak up if any issues arise. Furthermore, Lim *et al.* (2009) asserted that in  
24 organisations where management is opened to discussions and all members are  
25 involved in security affairs, employees tend to feel responsible to adhere to  
26 organisational security procedures and guides.

## 27 **5. Conclusion**

28  
29 Our results show that information security policies and security education tend to  
30 increase employee information security awareness. In turn, the awareness is inclined  
31 to lead to compliant behaviour. These insights extend general deterrence theory in a  
32 novel way. In particular, the deterrent effect of procedural security countermeasures  
33 increases information security awareness. This awareness, in turn, tends to prevent  
34 malicious actions of employees and encourage security-cautious behaviour.  
35 Furthermore, general deterrence theory is typically used to study negative behaviours,  
36 while there are calls in the literature to apply the theory across the variety of  
37 behaviours, including negative and positive (D’Arcy and Herath, 2011). The focus of  
38 this study is both negative and positive behaviours, which further extends general  
39 deterrence theory.

40  
41 Furthermore, OC values are inclined to have an effect on employee security behaviour  
42 in organisational settings. Study participants reveal that *high people-oriented*  
43 organisations benefit from a satisfied workforce, which in turn motivates employees  
44 to comply with information security rules. Moreover, *high solidarity* tends to lead to  
45 compliant behaviour because employees realise and pursue organisational goals. Next,  
46 *high sociability* and *high task-orientation* tend to encourage non-compliant behaviour.  
47 Finally, *flat structure* is inclined to improve the overall level of information security  
48 in an organisation.  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60

1 This study makes an important research contribution. The extant security research  
2 tends to focus on technical issues as opposed to the behaviour of individual users. On  
3 the contrary, our study builds on general deterrence theory and prior organisational  
4 culture literature to make an empirical contribution, which takes its place amongst the  
5 very few studies in Behavioural InfoSec research that investigate how procedural  
6 security countermeasures and organisational culture affect employee security  
7 behaviour. Further, prior studies that investigate the impact of procedural security  
8 countermeasures on employee security behaviour report contradictory and therefore,  
9 inconclusive results. This research provides empirical evidence that procedural  
10 security countermeasures, including information security policies and security  
11 education, tend to lead to compliant behaviour. Moreover, prior research that focuses  
12 on procedural security countermeasures, tend to investigate the direct effect of these  
13 measures on employee security behaviour. Therefore, the role of information security  
14 awareness has been neglected in the extant literature. Our research emphasises the  
15 important role of information security awareness.

16  
17 Our results also have important practical implications. First, this study highlights the  
18 important role of procedural security countermeasures in managing illicit actions in  
19 organisations. Security practitioners must realise that focusing on technical measures  
20 alone puts organisations at higher risk of security breaches occurring due to “human  
21 error”. Second, since information security awareness is the key factor in encouraging  
22 compliant behaviour, IS security managers must design security education and policies  
23 with the aim increasing awareness about security threats and consequences of  
24 information security breaches. In particular, real life incidents should be part of  
25 security education. Employee awareness that a security breach may lead to  
26 organisation’s bankruptcy and complete shutdown and consequently, their job loss,  
27 would be a strong drive to comply with organisational information security  
28 requirements. Third, security practitioners must take into consideration the effect of  
29 OC values on employee security behaviour. Organisational culture can be assessed  
30 and changed if required.

31  
32 An additional and important contribution of this study is in its methodology. While  
33 studies in the Behavioural InfoSec field make a valuable contribution to the pool of  
34 Behavioural InfoSec research, quantitative methodologies prevail in this research  
35 stream. Crossler *et al.* (2013), however, brought attention to the methodological  
36 challenges of quantitative methods and called for more studies that employ alternative  
37 methods, including qualitative. Moreover, Straub (1990) pointed out that “qualitative  
38 studies would enhance our [quantitative] perspective.” In particular, in our study we  
39 had a personal contact with interviewees, which allowed to probe and hence, grasp a  
40 deeper understanding of the central phenomenon of this study, that is security  
41 behaviour in organisations, as well as factors that tend to affect employee actions.

42  
43 In terms of study limitations, US data was collected in organisations located in the Bay  
44 Area, California. The US is a vast country and different parts have distinctive  
45 characteristics. For example, the Californian Bay Area is home to Silicon Valley, and  
46 therefore is home to a great number of achievers. This culture may have a certain  
47 influence on employee security behaviour as opposed to the less competitive culture  
48 that prevails in some other parts of the US.

49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60

1 Furthermore, one of the main concerns with qualitative studies is the generalisability  
2 of research findings. As this study is exploratory in nature, it is not attempting to  
3 generalise the findings but rather to present uniqueness within its context. Therefore,  
4 study results cannot be generalised at a country level because as with most of  
5 qualitative studies, the sample is too small. Future research would benefit from  
6 conducting a quantitative study that would confirm generalisability of the  
7 aforementioned findings. Nevertheless, this research builds on existing theories to  
8 make an empirical contribution, which takes its place amongst the very few studies in  
9 Behavioural InfoSec research that investigate how procedural security  
10 countermeasures and organisational culture affect employee security behaviour.

## 11 6. References

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

14 Ali, M. and Brooks, L. (2009), "A situated cultural approach for cross-cultural studies in IS",  
15 *Journal of Enterprise Information Management*, Vol. 22 No. 5, pp. 548-563.

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

17 Barlow, J.B., Warkentin, M., Ormond, D. and Dennis, A.R. (2013), "Don't make excuses!  
18 Discouraging neutralization to reduce IT policy violation", *Computers & Security*, Vol. 39  
19 Part B, pp. 145-159.

20 Blumstein, A., Cohen, J. and Nagin, D. (1978), "Deterrence and incapacitation: Estimating the  
21 effects of criminal sanctions on crime rates", in Bridges, G., Crutchfield, R., and Weis, R.  
22 (Eds.), *Crime and Society: Reading in Criminal Justice*, Vol. 3. Thousand Oaks: Pine Forge  
23 Press, 1996, pp. 96-100.

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

27 Cavallari, M. (2012), "A Conceptual Analysis about the Organizational Impact of Compliance  
28 on Information Security Policy", in Proceedings of 3rd International Conference Exploring  
29 Services Science, IESS in Geneva, Switzerland, 2012, pp. 101-114.

30 Chan, M., Woon, I. and Kankanhalli, A. (2005), "Perceptions of information security at the  
31 workplace: Linking information security climate to compliant behaviour", *Journal of*  
32 *Information Privacy and Security*, Vol. 1 No. 3, pp. 18-41.

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

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

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

40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60

- 1 Crossler, R.E., Johnson, A.C., Lowry, P.B., Hu, Q., Warkentin, M. and Baskerville, R. (2013),  
2 "Future directions for behavioral information security research", *Computers & Security*, Vol.  
3 32, pp. 90-101.
- 4 Danish, R.Q. and Usman, A. (2010), "Impact of Reward and Recognition on Job Satisfaction  
5 and Motivation: An Empirical study from Pakistan", *International Journal of Business and  
6 Management*, Vol. 5 No. 2, pp. 159-167.
- 7 D'Arcy, J. & Herath, T. (2011), "A review and analysis of deterrence theory in the IS security  
8 literature: Making sense of the disparate findings", *European Journal of Information Systems*,  
9 Vol. 20 No. 6, pp. 643-658.
- 10 D'Arcy, J. and Hovav, A. (2007), "Deterring internal information systems misuse,  
11 *Communications of the ACM*, Vol. 50 No. 10, pp. 113-117.
- 12 D'Arcy, J., Hovav, A. and Galletta, D. (2009), "User awareness of security countermeasures  
13 and its impact on information systems misuse: A deterrence approach", *Information Systems  
14 Research*, Vol. 20 No. 1, pp. 1-20.
- 15 D'Arcy, J., Herath, T. and Shoss, M.K. (2014), "Understanding employee responses to  
16 stressful information security requirements: A coping perspective", *Journal of Management  
17 Information Systems*, Vol. 31 No. 2, pp. 285-318.
- 18 Eisenhardt, K.M. (1989), "Building theories from case study research", *Academy of  
19 Management Review*, Vol. 14 No. 4, pp. 532-550.
- 20 Ferguson, M., Sheehan, M., Davey, J. and Watson, B. (1999) *Drink Driving Rehabilitation:  
21 The Present Context – A Road Safety Research Report*. Centre for Accidental Research and  
22 Road Safety, Brisbane, Australia, available at:  
23 [http://eprints.qut.edu.au/7379/1/Alc\\_Rehab\\_2.pdf](http://eprints.qut.edu.au/7379/1/Alc_Rehab_2.pdf) (accessed 10 October, 2015).
- 24 Furnell, S.M., Gennatou, M. and Dowland, P.S. (2002), "A prototype tool for IS security  
25 awareness and training, *International Journal of Logistics and Information Management*, Vol.  
26 15 No. 5, pp. 352-357.
- 27 Goffee, R., and Jones, G. (1996), "What holds the modern company together?" *Harvard  
28 Business Review*, Vol. 74 No. 6, pp. 133-148.
- 29 Guo, K.H. (2013), "Security-related behavior in using information systems in the workplace: A  
30 review and synthesis", *Computers & Security*, Vol. 32, pp. 242-251.
- 31 Guo, K.H. and Yuan, Y. (2012) "The effect of multilevel sanctions on information security  
32 violations: A mediating model", *Information & Management*, Vol. 49 No. 6, pp. 320-326.
- 33 Hovav, A. and D'Arcy, J. (2012), "Applying an extended model of deterrence across cultures:  
34 An investigation of information systems misuse in the U.S. and South Korea", *Information &  
35 Management*, Vol. 49 No. 2, pp 99-110.
- 36 Hu, Q., Xu, Z., Dinev, T. and Ling H. (2011), "Does deterrence work in reducing information  
37 security policy abuse by employees?" *Communications of the ACM*, Vol. 54 No. 6, pp. 54-  
38 60.
- 39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60

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

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

7 Kettley, P. (1995) "Is Flatter Better? Delaying the Management Hierarchy", Report 290, The  
8 Institute for Employment Studies, Publisher: Microgen UK Ltd., available at:  
9 <http://www.employment-studies.co.uk/system/files/resources/files/290.pdf> (accessed 15  
10 November, 2015).

11 Kilmann, R.H. (1985), "Managing your organization's culture", *The Nonprofit World Report*,  
12 Vol. 3 No. 2, pp. 12-15.

13 Kovačić, Z.J. (2005), "The impact of national culture on worldwide e-Government readiness",  
14 *Informing Science Journal*, Vol. 8, pp. 143-58.

15 Kroeber, A.L. and Kluckhohn, C. (1952), *Culture: A critical review of concepts and*  
16 *definitions*, Peabody Museum, Cambridge, Massachusetts.

17 Lee, S.M., Lee, S.G. and Yoo, S. (2004), "An integrative model of computer abuse based on  
18 social control and general deterrence theories", *Information & Management*, Vol. 41 No. 6,  
19 pp. 707-718.

20 Leidner, D.E. and Kayworth, T. (2006), "Review: A review of culture in information systems  
21 research: Toward a theory of information technology culture conflict", *MIS Quarterly*, Vol. 30  
22 No. 2, pp. 357-399.

23 Lim, J.S., Chang, S., Maynard, S. and Ahmad, A. (2009), "Exploring the relationships between  
24 organizational culture and information security culture", in Proceedings of 7th Australian  
25 Information Security Management Conference in Perth, Australia, 2009, pp. 88-97.

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

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

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

33 Pearson, A.E. (1987), "Muscle-build the organisation", *Harvard Business Review*, Vol. 65 No.  
34 4, pp. 49-55.

35 Phillips, M.E. (1994), "Industry mindsets: Exploring the cultures of two macro-organizational  
36 setting", *Organization Science*, Vol. 5 No. 3, pp. 363-383.

37 Porter, L.W. and McLaughlin, G.B. (2006), "Leadership and the organizational context: Like  
38 the weather?" *Leadership Quarterly*, Vol. 17 No. 6, pp. 559-576.

39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60

- 1 Probst, T.M. and Brubaker, T.L. (2001), "The effects of job insecurity on employee safety  
2 outcomes: cross-sectional and longitudinal explorations", *Journal of Occupational Health*  
3 *Psychology*, Vol. 6 No. 2, pp. 139-159.
- 4 Puhakainen, P. and Siponen, M. (2010), "Improving employees' compliance through  
5 information systems security training: An action research study", *MIS Quarterly*, Vol. 34 No.  
6 4, pp. 757-778.
- 7 Quazi, M.M. (1993), "Effective drug-free workplace plan uses worker testing as deterrent",  
8 *Occupational Health Safety*, Vol. 62 No. 6, pp. 26-31.
- 9 Rashid, Z.A., Samasivan, M. and Rahman, A.A. (2004), "The Influence of organizational  
10 culture on attitudes toward organizational change", *Leadership & Organization Development*  
11 *Journal*, Vol. 25 No. 2, pp. 161-179.
- 12 Ross, E.A. (1896), "Social Control", *American Journal of Sociology*, Vol. 1 No. 5, pp. 513-535.
- 13 Sacco, V.F. (1985), "Shoplifting prevention: The role of communication-based intervention  
14 strategies", *Canadian Journal of Criminology*, Vol. 27 No. 1, pp. 15-29.
- 15 Siponen, M., Mahmood, M. A., and Pahlila, S. (2009), "Are employees putting your company  
16 at risk by not following information security policies?" *Communications of the ACM*, Vol. 52  
17 No. 12, pp. 145-147.
- 18 Straub, D.W. (1990), "Effective IS security: An empirical study", *Information Systems*  
19 *Research*, Vol. 1 No. 3, pp. 255-276.
- 20 Straub, D.W. and Welke, R.J. (1998), "Coping with systems risk: security planning models for  
21 management decision making", *MIS Quarterly*, Vol. 22 No. 4, pp. 441-469.
- 22 Straub, D., Loch, K., Evaristo, R., Karahanna, E. and Srite, M. (2002), "Toward a theory-based  
23 measurement of culture", *Journal of Global Information Management*, Vol. 10, pp. 13-23.
- 24 Von Solms, R. and von Solms, B. (2004), "From policies to culture", *Computers & Security*,  
25 Vol. 23, pp. 275-279.
- 26 Vroom, C. and von Solms, R. (2004) "Towards information security behavioural compliance",  
27 *Computers & Security*, Vol. 23, pp. 191-198.
- 28 Xue, Y., Liang, H. and Wu, L. (2011), "Punishment, Justice, and Compliance in Mandatory IT  
29 Settings", *Information Security Research*, Vol. 22 No. 2, pp. 400-414.
- 30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60

Elements of Conceptual Framework	Reference	Examples of questions
Information Security Policy	Cheng <i>et al.</i> (2013)	Is there an information security policy in your organisation?
Security Education	D'Arcy <i>et al.</i> (2009)	Do you ever attend information security training courses in your organisation?
Information Security Awareness	Bulgurcu <i>et al.</i> (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?

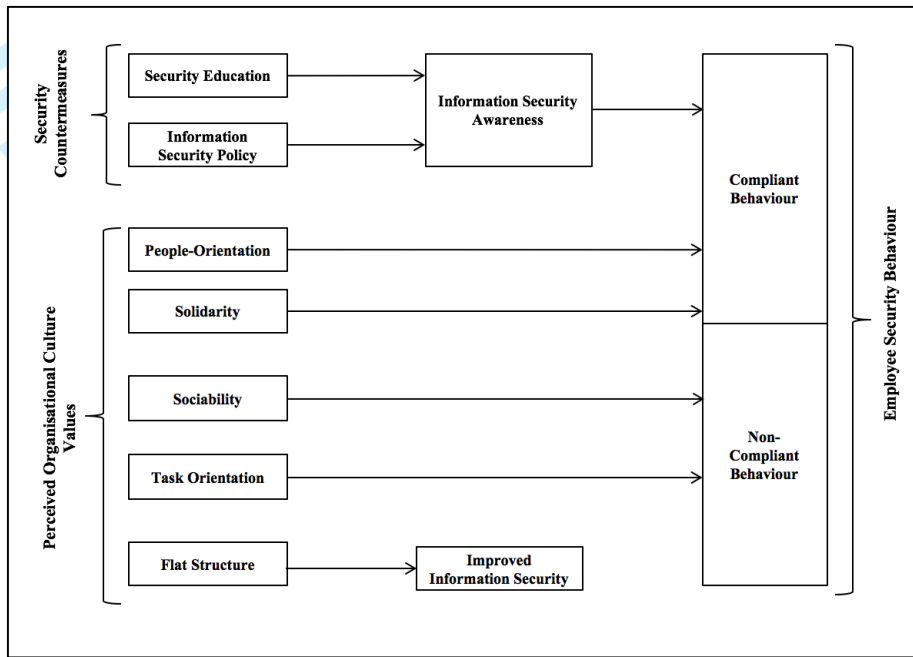
Table 1: Interview Guide Topics

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

Emerg ed 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-Oriented and Compliant Behaviour
Low People-Oriented and Non-Compliant Behaviour
High Solidarity and Compliant Behaviour
Low Solidarity and Non-Compliant Behaviour
High Sociability and Non-Compliant Behaviour
High Task-Oriented and Non-Compliant Behaviour
Flat Structure and Improved Information Security

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



and Computer Security

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60