The Impact of Procedural Security Countermeasures on Employee Security Behaviour: A Qualitative Study

Alena Yuryna Connolly *lena.connolly@gmail.com*
National University of Ireland Galway
Galway, Ireland

Michael Lang *michael.lang@nuigalway.ie*
National University of Ireland Galway
Galway, Ireland

Doug J. Tygar *doug.tygar@gmail.com*
University of California Berkeley
Berkeley, United States

Abstract

The growing number of information security breaches in organisations presents a serious risk to the confidentiality of personal and commercially sensitive data. Current research studies indicate that humans are the weakest link in the information security chain and the root cause of numerous security incidents in organisations. Based on literature gaps, this study investigates how procedural security countermeasures tend to affect employee security behaviour. Data for this study was collected in organisations located in the United States and Ireland. Results suggest that procedural security countermeasures are inclined to promote security-cautious behaviour in organisations, while their absence tends to lead to non-compliant behaviour.
Keywords: Employee Security Behaviour, Information Security Policy, Security Education, Information Security Awareness.

1. Introduction

Traditionally, organisations have prioritised a technological approach in order to protect their information assets from potential security attacks. While technical tools are essential, research and practice show that technology is unable to provide an adequate solution when it comes to certain illicit human actions such as sharing passwords with colleagues, violation of a clear desk policy, or inappropriate disposal of confidential documents [5]. Compliance with such rules entirely depends on employees' motivation to conform, while various sources refer to humans as the weakest link in the security chain [9]. IBM's 2015 Cyber Security Intelligence Index reports that 95% of cyber security breaches are due to human error [20, p.7].

Research and Crossler et al. [9, p. 90] have drawn attention to a notable gap in the literature which has arisen because much of the focus of extant security research is on technical issues, "although a predominant weakness in properly securing information assets is the individual user within an organisation". Behavioural Information Security (InfoSec) research focuses on the mitigation of threats to information assets by identifying factors that promote security cautious behaviour or trigger illicit acts of individuals. These studies enhance our understanding of employee security behaviour by drawing on perspectives such as criminology [10], psychology [23], and organisational control [4]. Additionally, IS researchers have suggested various security countermeasures that can be employed to combat non-compliant behaviour of employees [11], [21]. Based on the predictions of the general deterrence theory (GDT), security countermeasures can serve as deterrent mechanisms to prevent information systems IS misuse [11], [29].

This paper introduces an extended GDT model, indicating that in addition to their negative deterrent effect, security countermeasures also have a positive impact upon employee security behaviour. The results advance our understanding of the underlying process through which security countermeasures affect employee security actions and highlight the important role of employee information security awareness in this process. Our findings also have important implications for the practice of IS security management.

2. Literature Review

Organisational strategies for reducing IS misuse generally fall into four stages – *deterrence*, *prevention*, *detection*, and *recovery*. These four stages are collectively referred as the Security Action Cycle [30]. 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. Built on Straub and Welke's [30] framework, Willison and Warkentin [31] offered Extended Security Action Cycle that adds the *insider abuse intention formation* to the original work – the phase that occurs before deterrence. The focus of this paper is on the stage of *deterrence*. This phase refers to the use of deterrent security countermeasures such as information security policies and security education with the aim to reduce IS misuse. Following Hovav and D'Arcy [19], we use the term "procedural security countermeasures" to collectively describe these controls.

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 [11]. Security education has a similar deterrent effect through an ongoing security training. The ultimate purpose of education is to enable users to make good decisions by reminding them the guidelines regarding an acceptable usage of information systems and the potential outcomes in the event users circumvent the outlined rules. In the extant literature, security education is considered to be part of Security Education, Training, and Awareness (SETA) programmes. While there are many forms of SETA programmes, including security awareness e-mails and newsletters, and briefings on the consequences of IS misuse, this research concentrates on security education as it is the most commonly used form of SETA programmes in organisations [11].

Several IS researchers have empirically assessed the effectiveness of procedural security countermeasures. The majority of these studies have employed GDT (or some variation of GDT) as a theoretical foundation, assuming that procedural security countermeasures operate as deterrent mechanisms by increasing perceptions of some form of penalty for unacceptable behaviour and hence, reducing IS misuse. Despite the solid theoretical basis, a comprehensive literature review conducted in the course of this study has demonstrated that the findings of deterrent-based research are inconclusive. Although some studies provide evidence that information security policies reduce IS misuse [8], [28], [29], others contradict these inferences [22]. Similarly, Barlow et al. [2] reported that security education is an important predictor of security-compliant behaviour, but Lee et al. [22] concluded that security awareness programmes do not reduce IS misuse. Furthermore, under the presumption that a simple presence of security policies in organisations has no impact on employee actions, additional studies reported that user awareness about information security policy [11] and policy visibility [28] encourage compliance with security policies.

Although these previous studies are highly informative, they investigated the direct effect of procedural security countermeasures on employee security behaviour, neglecting the important role of user information security awareness. In particular, a simple presence of the information security policy may not have a desired effect on employee security behaviour [5]. The purpose of the information security policy, as is security education, is to increase information security awareness, which, in turn, will promote security-cautious behaviour [2]. 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 [5], while empirical findings appeared to be contradictory. For example, although Bulgurcu et al. [5] reported that user general awareness about information security has a positive effect on their behaviour, Lee et al. [22] asserted that a degree of awareness has no impact on employee 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" [5, p.543].

Hence, despite the growing body of knowledge in the area of Behavioural InfoSec in recent years, which offers practical solutions on how to encourage security-cautious behaviour and prevent non-compliant actions of employees, there are still several avenues of research that have only barely been explored. In particular, in comparison to other areas of Behavioural InfoSec research, the impact of security countermeasures on security-related behaviour has received relatively little attention. Moreover, the empirical findings are contradictory and therefore, inconclusive. Hence, taking in consideration the aforementioned literature gaps, the objective of this study is to answer the following research question:

- How do procedural security countermeasures affect security behaviour in organisational settings?

3. Theoretical Context

Our proposed theoretical model, shown in Figure 1, integrates procedural security countermeasures (e.g. security education and an information security policy), information security awareness, and employee security behaviour. The model expands on 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.

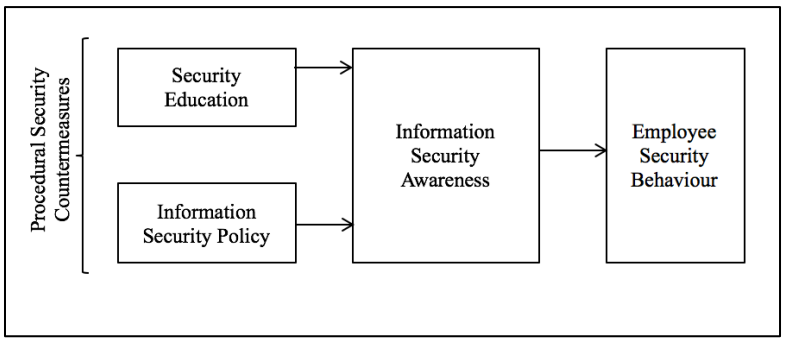

Figure 1. Conceptual framework

3.1. 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 [3]. 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" [29, p. 258]

Classic GDT has been widely employed in the IS security context under presumption that employees choose to engage in inappropriate behaviour and therefore, organisational sanctions will prevent deviant actions of employees and deter computer abuse [13]. GDT was further extended and policing is being associated with security countermeasures, including information security policies [22], security education [2], and technical controls [10], assuming that these controls also deter illicit actions of individuals. Therefore, in line with GDT, researchers assume 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 programmes.

3.2. Employee Security Behaviour

In this research, *employee security behaviour* 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" [18, 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 [18]. This behaviour may either pose or moderate organisational IS security threats.

This study does not focus on any specific type of behaviour but at the same time aims to distinguish between positive and negative behaviours because factors that influence these actions may vary. Subsequently, the behaviours of interest include 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).

3.3. The Role of Information Security Awareness

Bulgurcu et al. [5, 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 [5].

Prior research confirms that public awareness can reduce certain illicit acts like drunk driving [15], shoplifting [27], and workplace drug use [26]. Furthermore, Bulgurcu et al. [5] and D'Arcy et al. [11] 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 [11]. 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 [5].

4. Research Approach

The endeavour of our research is to understand social interactions between security countermeasures and employee behaviour from a perspective of study participants. Rich qualitative findings within a given context as opposed to broad generalisations are essential for this purpose and therefore, a qualitative approach was adapted in this study. The methodology employed in this research draws on the analytical grounded theory approach [24] and employs the constant comparative method [25].

Data collection was carried out using semi-structured in-person interviews. 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 1. The interview guide was constructed following a thorough analysis of the literature. The guide included questions about procedural security countermeasures, information security awareness and the impact of these factors on employee security behaviour.

Table 1. Facts about interviewees of US and Irish organisations

Names (aliases)	Column 1	Column 2
CloudSerUS	IT; 1998; large	1 person: Software Developer
RetCoUS	Finance; 1932; large	1 person: Security Executive
CivEngCoUS	Civil Engineering; 1945; SME	1 person: Civil Engineer
TechCorpUS	IT; 1968; large	2 people: Security Researchers
EducInstUS	Education; 1868; large	2 people: Administrator & Professor
FinCoUS	Finance; 1982; large	1 person: Security Consultant
PublCoUS	Publishing; 2005; SME	1 person: Business Owner
TechCorpIrl	IT; 1968; large	2 people: Product Manager & IT Executive
CharOrgIrl	Charity; 1883; large	1 person: Data Protection Officer
BevCorpIrl	Beverage Manufacturing; 1944; large	1 person: IT Executive
PublOrgIrl	Publishing; 2000; SME	1 person: Chief Editor
EducOrgIrl	Education; 1845; large	2 people: Administrator & Lecturer
TelCommCorpIrl	IT; 1984; large	1 person: Software Developer
ResRegIrl	Energy Regulation; 1999; SME	1 person: Policy Analyst
BankOrgIrl	Finance; 1982; large	1 person: Security Executive

Organisations and participants were purposefully selected. In this particular study, it was important to interview organisations from a broad range of industries in order to capture data from organisations with various levels of security with the aim to grasp 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 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, overall out of nineteen interviewees, 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’ [15] (Figure 1). 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 (Table 2).

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, selecting interviewees with different levels of knowledge in the area of information security was vital to discover the role of information security awareness. To select suitable organisations, a short questionnaire was conducted over the telephone with potential participants. Subsequently, five interviews were conducted in

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.

Table 2. Results of Phases 1 and 2 in the United States

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

Furthermore, 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 similar to the provisional findings discovered in the US organisations interviewed in Stage 1 of data collection (please refer to Table 2). Therefore, the selection criteria for Stage 4 was similar to the criteria used to choose organisations in the United States for Stage 2. Three organisations located in Ireland (TechCorpIrl, TelCommCorpIrl, and EducOrgIrl) and 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 results have confirmed the associations emerged in Stages 1 and 3 (Table 2). It is important to note that the study's findings are based on the data combined from both data sets.

The next phase of data analysis (Phase 3 - Coding on) involved merging both data sets and further breaking down of 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 [14] argued that theoretical saturation is reached when a researcher is observing phenomena that have been seen before and therefore, incremental learning becomes minimal. In this study, it was determined that the point of theoretical saturation has been reached once 19 interviews were conducted.

5. Research Findings and Discussion

Our findings indicate that procedural security countermeasures tend to increase information security awareness, which, in turn, has a tendency to encourage compliant behaviour.

5.1. Security Education and Information Security Awareness

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..."

In contrast, 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 increase employee information security awareness. The purpose of security training is to educate employees on how to protect vital organisational assets and why a certain set of rules has to be in place. 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 employee 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 information security conscious and therefore, are inclined to follow rules. Furnell et al. [16] 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 Barlow et al. [2], Siponen et al. [28] and Straub [29] 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.

5.2. Information Security Policy and Information Security Awareness

Study informants from CloudSerUS, TechCorpIrl, TechCorpUS, and RetCoUS suggest that a policy is inclined to increase employee security awareness. A Product Manager reveals that information security is a top priority in TechCorpIrl. 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. The Product Manager asserts:

> "I think [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..."

Further, a Software Developer from CloudSerUS 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 increase employee 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. Although Chan et al. [7] and Straub [29] confirmed that the establishment of information security policies in organisations is vital to encourage security compliant behaviour, these studies do not specify that security policies affect employee actions indirectly through information security awareness. However, Lee et al. [22] found that the information security policy has no impact on IS misuse behaviour. This contradicting finding could be explained by the employees' lack of awareness of the security policies existence.

Further analysis revealed that for the security policy to be effective, it must retain certain characteristics. Bulgurcu et al. [5] asserted that the mere presence of the information security policy in an organisation does not lead to desirable actions. Employees must be aware of the document and its content and must understand why certain security measures are in place. The most common way to inform employees about security policies is through security education. Data findings of this study are in accordance with these claims. In particular, study participants from BevCorpIrl, EducOrgIrl, and EducInstUS share that for the policy to have a desired effect, it must be *visible*. For example, an IT Manager from BevCorpIrl reveals:

> "I have definitely seen rules being broken… just to get stuff done... They do not understand the implications of why the rule is in place… There are information security policies but they are hidden away on some website someplace…They are not in front of people's faces. People do not see them".

Furthermore, study participants from CloudSerUS, RetCoUS, and CharOrgIrl assert that security policies must be *up to date*. For example, a Security Executive from RetCoUS suggests that information security policies have to be *updated* regularly because information security is constantly evolving, such as threats are changing and therefore, security controls have to change accordingly:

> "We are updating all of our policies because they are outdated. Information security is always changing, the threats are always changing, the environment is always changing, and so we have to keep policies up to date".

As it stands today, cybercrime is a fully commercialised enterprise with functions identical to legitimate businesses. The fundamental goal of online fraud is to generate profit, although some cyber attacks have a different purpose. Therefore, cybercriminals continuously develop new types of malware in order to deceive computer users, steal valuable information, or pocket funds. As a result, organisational security policies must be updated as regards to new threats and solutions to defeat these threats.

Next, study informants from BevCorpIrl, RetCoUS, and CloudSerUS expressed that *employee feedback* has to be taken in consideration for the information security policy to function properly. In particular, employees have to apply rules outlined in the information security policy in practice and if a certain rule is hard or impossible to utilise, employees will circumvent it. A Security Executive from RetCoUS stresses:

> "Having this open dialogue, employees can change the rules by bringing things up. I have seen it happen in the past. So the policies have been changed based upon the use of the users and them providing that feedback. RetCoUS wants to make sure that information security is implemented to augment the business and not prevent the business from moving forward and so that feedback is really important".

Typically, policy makers lack first-hand experience of applying the very same rules they outline in the policies. In particular, policy implementers take in consideration data protection laws and organisation's priorities in terms of the value of information assets, but rarely the applicability of the rules. Consequently, employees repeatedly hit the wall of overly bureaucratic rules. Prior research shows that employees circumvent information security rules if the rules are barrier to productivity [1]. Bulgurcu et al. [5] added that commonly employees perceive information security rules as inconvenience and obstruction to meet daily work requirements. Negative attitude towards rules, in turn, discourage information security compliance [6]. Therefore, employee feedback is vital in developing security policies.

Moreover, interviewees from BevCorpIrl, EducOrgIrl, and EducInstUS point out that policies must be *enforced*. In particular, regular audits have to be in place to check if policies are adhered to. Additionally, employees who break the rules as well as managers on duty must be held accountable. An IT Executive from BevCorpIrl suggests:

> "We have a clean desk policy but it is not adhered at all. It would take a simple check by a manager in the evenings to enforce it but it is not done… It is important to have regular, proper security audits, where people and their managers are held accountable".

Crime occurs despite the rewards and punishments that have been devised to encourage compliance. Although crime is a type of behaviour that is condemned by society, human beings still engage in criminal activities for various reasons. Merriam-Webster dictionary defines crime as "an activity that is against the law". Since security policies can be considered as organisational laws, breaking organisational information security rules is a type of crime. Because crime is inevitable, organisations must have measures in place to control wrongful activities of employees. For example, security policies must be enforced through various mechanisms, including audit checks.

5.3. Information Security Awareness and Employee Security Behaviour

Study participants from CloudSerUS, CharOrgIrl, TechCorpUS, and EducInstUS share that employee awareness as regards information security 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 tends to lead to 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. [5] and D'Arcy et al. [11] 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. [22] reported that degree of security awareness has no impact on employees' actions, our results show the opposite.

6. Conclusion

The extant security research tends to focus on technical issues as opposed to behaviour of individual users [9]. Our study builds on general deterrence theory to make an empirical contribution, which takes its place amongst the very few studies in Behavioural InfoSec research that investigate how procedural security countermeasures 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. While IS scholars argue that the ultimate purpose of procedural security countermeasures is to increase information security awareness [2], empirical evidence that supports these claims is lacking. Also, there are calls in the IS literature for studies that investigate factors that lead to information security awareness since information security awareness plays the key role in employees' compliance behaviour [5]. Finally, IS scholars report contradictory results in terms of the effect of information security awareness on employee security behaviour (e.g. Bulgurcu et al. [5] vs. Lee et al. [22]). The findings of this research project fill the aforementioned gaps and demonstrate that procedural security countermeasures tend to lead to compliant behaviour indirectly, through information security awareness. These insights extend general deterrence theory in a novel way. In particular, the deterrent effect of procedural security countermeasures tends to increase 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 [12]. The focus of this study is both negative and positive behaviours, which further extends general deterrence theory.

Our findings confirm that a simple presence of security policies in organisations may not have a desired effect. For an information security policy to be effective, it must retain certain characteristics. In particular security policies must be *up to date* and *visible*. The most common way to introduce employees to security policies is through security education. Additionally, policies must be *enforced*, such as employees have to be checked if they follow the rules and held accountable if not. Furthermore, managers on duty have to be held accountable if rules are not adhered to. Finally, *employee feedback* is important when designing and implementing information security policies. Since employees have the practical experience of applying information security rule (as opposed to policy analysts), they are aware which rules are realistic to use and which are not. If a certain rule prevents employees from completing other tasks, they may try to circumvent it.

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. [9], however, brought attention to the methodological challenges of quantitative methods and called for more studies that employ alternative methods, including qualitative. Moreover, Straub [29] 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.

Our results also make an important practical contribution. 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 important characteristics a security policy must retain to properly function and fulfil its purpose.

In terms of study limitations, qualitative data is prone to subjective interpretations. Although various techniques were employed to avoid research bias (e.g. member checks, peer debriefing), there is still a possibility that data interpretations had some element of subjectivity. 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 the uniqueness within study's context. Furthermore, our research would benefit from a secondary data source. However, the access to organisational documents was not possible as it is often the case with studies that investigate sensitive issues. Nevertheless, our study provides some interesting insights on how procedural security countermeasures tend to affect employee security behaviour in organisational settings and answer the research question.

References

1. Albrechtsen, E.: A qualitative study of users' view on information security. Computers & Security. 26 (4), 276-289 (2007)
2. Barlow, J.B., Warkentin, M., Ormond, D., Dennis, A.R.: Don't make excuses! Discouraging neutralization to reduce IT policy violation. Computers & Security. 39 (Part B), 145-159, (2013)
3. Blumstein, A., Cohen, J. and Nagin, D.: Deterrence and incapacitation: Estimating the effects of criminal sanctions on crime rates. In: Bridges, G., Crutchfield, R., Weis, R. L. (eds.) Crime and Society: Reading in Criminal Justice, Vol. 3, pp. 96-100. Thousand Oaks, Pine Forge Press (1996)
4. Boss, S.R., Kirsch, L.J., Angermeier, I., Shingler, R.A. and Ross, R.W.: If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security. European Journal of Information Systems. 18 (2), 151-164 (2009).
5. Bulgurcu, B., Cavusoglu, H. and Benbasat, I.: Information security policy compliance: An empirical study of rationally-based beliefs and information security awareness. MIS Quarterly, 34 (3), 523-548 (2010)
6. Cavallari, M.: A conceptual analysis about the organizational impact of compliance on information security policy. In: Proceedings of 3rd International Conference on Exploring Services Science, pp. 101-114, Springer, Berlin (2012)
7. Chan, M., Woon, I. and Kankanhalli, A.: Perceptions of information security at the workplace: Linking information security climate to compliant behaviour. Journal of Information Privacy and Security. 1 (3), 18-41, (2005)
8. Chen, Y.K. Ramamurthy, K. and Kuang-Wei, W.: Organizations' information security policy compliance: Stick or carrot approach? Journal of Management Information Systems, 29 (3), 157-188 (2012)
9. Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M. and Baskerville, R.: Future directions for behavioral information security research. Computers & Security, 32, 90-101 (2013)
10. D'Arcy, J. and Hovav, A.: Deterring internal information systems misuse. Communications of the ACM. 50 (10), 113-117, (2007)

11. D'Arcy, J., Hovav, A., and Galletta, D.: User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. Information Systems Research. 20 (1), 1-20, (2009)
12. D'Arcy, J., and Herath, T.: A Review and Analysis of Deterrence Theory in the IS Security Literature: Making Sense of the Disparate Findings. European Journal of Information Systems. 20 (6), 643-658, (2011)
13. D'Arcy, J., Herath, T. and Shoss, M.K.: Understanding employee responses to stressful information security requirements: A coping perspective. Journal of Management Information Systems. 31 (2), 285-318, (2014)
14. Eisenhardt, K.M.: Building theories from case study research. Academy of Management Review. 14 (4), 532-550, (1989)
15. Ferguson, M., Sheehan, M., Davey, J. and Watson, B.: Drink Driving Rehabilitation: The Present Context – Road Safety Research Report. Centre for Accidental Research and Road Safety, Brisbane, Australia, http://eprints.qut.edu.au/7379/1/Alc_Rehab_2.pdf. Accessed November 10, 2016
16. Furnell, S.M., Gennatou, M., and Dowland, P.S.: A prototype tool for IS security awareness and training. International Journal of Logistics Information Management. 15 (5), 352-357, (2002)
17. Glaser, B. G., Stauss A. L.: The Discovery of Grounded Theory. Aldine, Chicago (1967)
18. Guo, K.H.: Security-related behavior in using information systems in the workplace: A review and synthesis. Computers & Security, 32, 242-251 (2013)
19. Hovav, A. and D'Arcy, J.: Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U.S. and South Korea. Information & Management. 49 (2), 99-110, (2012)
20. IBM: 2015 Cyber Security Intelligence Index. Research Report. IBM, Somers, New York, http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=SEW03073USEN&attachment=SEW03073USEN.PDF. Accessed March 10, 2017
21. Karlsson, F., Goldkuhl, G. and Hedström, K.: Practice-based discourse analysis of InfoSec policies. In: Proceedings of the 30th IFIP TC-11 SEC 2015 Conference, pp. 297-310. Springer, Hamburg (2015)
22. Lee, S.M., Lee, S.G., & Yoo, S.: An integrative model of computer abuse based on social control and general deterrence theories. Information & Management. 41 (6), 707-718, (2004)
23. Lee, Y. and Larsen, K.R.: Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software. European Journal of Information Systems. 18 (2), 177-187 (2009)
24. Matavire, R. and Brown, I.: Profiling grounded theory approaches in information systems research, European Journal of Information Systems, 22 (1), 119-129 (2013)
25. Maykut, P. and Morehouse, R.: Beginning Qualitative Research: A Philosophic and Practical Guide. The Falmer Press, London (1994)
26. Quazi, M.M.: Effective drug-free workplace plan uses worker testing as deterrent. Occupational Health Safety. 62 (6), 26-31, (1993)
27. Sacco, V.F.: Shoplifting prevention: The role of communication-based intervention strategies. Canadian Journal of Criminology. 27 (1), 15-29, (1985)
28. Siponen, M., Mahmood, M. A., and Pahnila, S.: Are employees putting your company at risk by not following information security policies? Communications of the ACM. 52 (12) p. 145-147 (2009)
29. Straub, D.W.: Effective IS security: An empirical study. Information Systems Research. 1 (3), 255-276, (1990)
30. Straub, D.W., Welke, R.J.: Coping with systems risk: security planning models for management decision making. MIS Quarterly. 22 (4), 441-469, (1998)
31. Willison, R., Warkentin, M.: Beyond deterrence: An expanded view of employee computer abuse. MIS Quarterly. 37 (1), 1-20, (2013)