Investigation of Employee Security Behaviour: A Grounded Theory Approach

Lena Connolly, Michael Lang, J. Tygar

Investigation of Employee Security Behaviour: A Grounded Theory Approach

Lena Connolly[1], Michael Lang[1], J.D. Tygar[2]

[1]Business Information Systems, National University of Ireland Galway, Ireland
y.connolly1@nuigalway.ie
[2]Electrical Engineering and Computer Science, University of California, Berkeley, USA

Abstract. At a time of rapid business globalisation, it is necessary to understand employee security behaviour within diverse cultural settings. While general deterrence theory has been extensively used in Behavioural Information Security research with the aim to explain the effect of deterrent factors on employees' security actions, these studies provide inconsistent and even contradictory findings. Therefore, a further examination of deterrent factors in the security context is required. The aim of this study is to contribute to the emerging field of Behavioural Information Security research by investigating how a combination of security countermeasures and cultural factors impact upon employee security behaviour in organisations. A particular focus of this project is to explore the effect of national culture and organisational culture on employee actions as regards information security. Preliminary findings suggest that organisational culture, national culture, and security countermeasures do have an impact upon employee security behaviour.

Keywords: Employee Security Behaviour, Security Countermeasures, Organisational Culture, National Culture

1 Introduction

The majority of modern organisations are heavily relying on computerised information systems (IS). These systems store the sensitive data necessary to run businesses efficiently, including financial, customer, and product records. Therefore, managing risks associated with the loss of this vital information is essential. Threats can come from external as well as internal sources. External attacks are typically initiated by hackers who are seeking political or financial gain. The common way to prevent external attacks is an implementation of technical security controls, including firewalls, anti-malware software, and authentication controls. These measures are widely employed by organisations and are largely effective.

On the other hand, an insider threat refers to an intentional or unintentional misuse of an organisation's IS by employees that may negatively affect the confidentiality, integrity, or availability of that organisation's vital information. Maintaining employees' compliance with information security rules is a more problematic matter as technical controls are unable to prevent all human blunders. For instance, employees tend to write passwords down, share them with colleagues or send

confidential information in an unencrypted form. It is estimated that at least half of information security breaches are made by internal personnel [1]. Posey et al. [2] argue that deviant behaviour is best managed with a combination of technical and social measures.

Overcoming the issue of "human error" has received considerable attention in Behavioural Information Security (InfoSec) research. Various approaches designed to improve employee security behaviour have been suggested by IS scholars. These range from security awareness programmes [3] and security education and training [4] to approaches that take into account deterrent [5] as well as cognitive [6, 7] factors.

However, a comprehensive literature review conducted for this research revealed that a number of areas in Behavioural InfoSec research require further investigation. To begin with, while IS researchers demonstrate the influence of security countermeasures on employee security behaviour, the results of these studies are inconsistent and therefore require further clarification [8]. Several IS researchers suggested that the influence of deterrent factors may vary under the impact of other aspects [9]. A literature review conducted for this project revealed a limited amount of studies that investigate the influence of deterrent factors in combination with cultural aspects. Furthermore, cross-cultural studies are particularly rare in Behavioural InfoSec research, although prior research shows that national culture (NC) has an effect on organisational behaviour [10, 11]. Finally, Hu et al. [5] report that there is a general lack of studies that examine the effect of organisational culture (OC) on employee security behaviour and existing studies fail to illustrate strong theoretical foundations for linking OC and behaviour.

This research in progress addresses the aforementioned literature gaps and attempts to answer the following research questions:

1. How do organisational culture values affect employee security behaviour?
2. How does national culture affect employee security behaviour?
3. How do security countermeasures affect employee security behaviour?

This is a cross-cultural study conducted in the USA and Ireland. As is commonly the situation with comparative international studies, the initial choice of these two countries was more opportunistic than deliberate, arising as it did out of a research exchange programme which necessitated the lead author spending extended periods of time in both countries. Nevertheless, although the cultures of both Ireland and the USA are often referred in the extant literature as "Western", these two countries have similar as well as contrasting cultural characteristics [12] and therefore are worthy of comparison. Additionally, Ireland is an important commercial gateway between the USA and Europe, it being the location of the European headquarters of several American multinational corporations. Ireland is situated at the interface of two rather different perspectives on privacy and data protection (i.e. EU versus USA), which is a further reason why a cross-cultural study between Ireland and the USA is a useful undertaking.

2 Theoretical Context

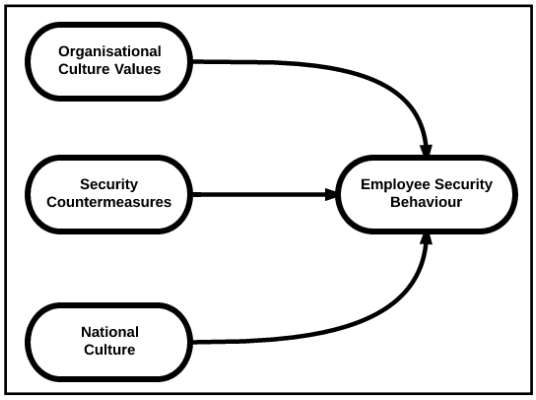

Fig. 1. Theoretical framework.

2.1 Culture

The study of culture is rooted in sociology, social psychology, and anthropology [13]. Culture has been studied for over a hundred years in various disciplines. As a result, numerous definitions, conceptualisations, and dimensions of culture have been produced by researchers. For example, Kroeber and Kluckhohn [14] identify 164 definitions of culture. They range from simple to complex, incorporate and extend previous definitions, and even contradict prior definitions. Consequently, viewpoints on culture vary significantly. For example, some scholars perceive culture as a hidden or partly hidden force and therefore culture is problematic to assess as it is not directly observable [15]. In contrast, DeLong and Fahey [16] argue that culture embraces explicit and observable artifacts and therefore can be assessed.

The two most commonly used theoretical frameworks of culture are the socio-cultural system and the individual system [13]. Taking the socio-cultural perspective, Mead [17] defines culture as "shared patterns of behaviour". This definition implies that "culture is a group-level construct, situated between the personality of individuals and the human nature that is common to all of us" [13, p. 549]. Groups like societies, organisations and professions are considered to have their own cultures. Hence, studying culture entails more than observing and describing behaviour. On the other hand, the individual perspective treats culture as "an individual's characteristic way of perceiving the man-made part of one's environment" [18, p.3]. This definition assumes that culture can be assessed by analysing an individual's behaviour [13].

For the purpose of this research, culture is regarded as follows:

1. Culture is explicit and therefore can be observed.
2. Culture can be assessed by analysing an individual's behaviour.

2.2 Organisational Culture and Security Behaviour

Prior research shows that OC affects behaviour. For example, Kilmann [19] describes culture as a separate and hidden force that controls behaviours and attitudes in organisations. Furthermore, Philips [20] portrays culture as a set of tacit assumptions that guide acceptable perceptions, thoughts, feelings, and behaviour among members of the group. Finally, Baker [15] emphasises the importance of OC as a power that can lead a company to success or weaken its vitality because OC directly affects employee behaviour in an organisation. While the aforementioned studies show a link between OC and behaviour, this subject area has received very little attention in Behavioural InfoSec research. A literature review conducted for this study revealed a general lack of OC studies in the security context.

2.3 National Culture and Security Behaviour

Various academic works show that NC influences organisational behaviour. In particular, Hofstede [21] argues that organisations are bound by national cultures and underlines the cross-national differences in the functioning of organisations and people in them. He compares culture with an onion consisting of multiple layers, values being the inner layer of the onion, which are invisible until they become evident in behaviour. Ali and Brooks [13] define NC as a shared set of core values, norms and practices in a society that shapes individuals' behaviour within that society. However, cross-cultural research in Behavioural InfoSec is particularly scarce and urgent calls for more studies have been made [10]. For example, Dinev et al. [11] report differences in user behaviour toward protective information technologies in the USA and South Korea. Flores et al. [22] state that the effect of behavioural information security governance factors on the establishment of security knowledge sharing differs between Swedish and the USA organisations.

Cross-Cultural Dimensions. Hofstede's [12] original taxonomy describes culture in terms of four dimensions – *power distance*, *uncertainty avoidance*, *masculinity vs. femininity*, and *individualism vs. collectivism*. The score difference between the USA and Ireland's *individualism vs. collectivism* dimension is 21. Thus, it may be possible to explain the effect of NC on employee security behaviour from the perspective of the national trait of *individualism*. According to Hofstede [12], the United States has a highly individualistic culture, which affects relationships between individuals. For example, in the USA people typically take care of themselves and their immediate family. On the contrary, Irish people normally take into consideration group as well as individual interests. Propensity towards individualism or collectivism in a society can have an impact on organisational affairs. For example, Zhang et al.'s [23] study conducted in the United States and China, reveal that the level of *majority influence* (i.e. the attempt by the majority of group members to impose their common position on group dissenters during group decision making) on *group minorities* appears to be stronger in collectivist societies. Furthermore, Hofstede [12] points out that the level of individualism in society will affect the organisational members' reasons for

complying with organisational rules and regulations. For example, in Ireland, *peer pressure* may have a stronger effect on employee security behaviour than in the USA.

Furthermore, Hofstede [12, p.217] claims that national characteristics have a strong affect on the "nature of relationships between a person and the organisation to which she or he belongs". Regardless of the nature of business, organisations in different countries vary in terms of organisational structures and processes [12]. Mintzberg [24] stresses that five distinct coordinating mechanisms explain the fundamental ways in which organisations manage their work, including *mutual adjustment*, *direct supervision*, *standardisation of work processes*, *standardisation of work outputs*, and *standardisation of worker skills*. These mechanisms form an organisational structure. Hofstede [12] argues that typically Irish organisations employ a *mutual adjustment* mechanism for coordinating activities and form a structure of *adhocracy*, in which the support staff is the key part. *Mutual adjustment* achieves the coordination of work by a simple process of informal communication and control of the work rests in the hands of the doers [24]. On the other hand, the structure of the United States organisations takes a *divisionalised form*, based on *standardisation of outputs*, in which the middle line is the key part. Typically, American firms standardise outputs by setting specific goals and results [12]. Prior studies show that employees tend to circumvent security rules when put under pressure to meet deadlines [25]. Therefore, factors that impel employees to break security rules may be different in the United States and Ireland due to different organisational structures.

2.4 Security Countermeasures and Security Behaviour

With the increasing occurrence of computer abuse by employees, organisations are searching for improved ways to deter it. According to the General Deterrence Theory (GDT), organisations can increase employee compliance with information security rules by implementing deterrence mechanisms, including *technical controls*, *information security policies*, and *security education, training and awareness programmes* [3, 4]. Deterrence theory is one of the most widely applied theories in IS security research [10]. Rooted in criminology [26], the classic deterrence theory posits that individuals weigh costs and benefits before committing a crime. If an individual believes that the risk of getting caught is high and that penalties will be applied if caught, then GDT states that the individual will not commit the crime.

D'Arcy et al. [3] present an extended deterrence theory model and report that security countermeasures such as *security policies*, *awareness programmes*, and *computer monitoring* influence perceived *severity of formal sanctions*, which leads to reduced intention to misuse IS, while *certainty of formal sanctions* does not have any effect on intention to misuse IS. Furthermore, Lee et al. [4] show that deterrence-based countermeasures, including *information security policy*, *security education and training awareness programmes*, and *security systems*, directly influence security behaviour in organisations. In contrast, Herath and Rao [27] report that *perceived severity of penalties* has significant but negative effect on *security policy compliance intention*. Additional studies inform that deterrence constructs do not have a significant influence on employee behaviour [28]. Overall, the extant literature

provides inconsistent findings for deterrence theory in the information security context. Therefore, an additional examination of the influence of deterrence measures on actual behaviour is needed.

3 Research Methodology

The methodology adapted for this study draws on the *analytical grounded theory* (AGT) approach [29], employing the *constant comparative method* of Maykut and Morehouse [30]. This methodological framework draws on the work of Lincoln and Guba [31]. While none of the grounded theory principles were directly employed, nevertheless this project adapts a grounded theory approach insofar as the findings of this study are entirely rooted in the data. The AGT is the method of applying grounded theory analytical techniques (constant comparative method) to analyse data without a necessity to follow grounded theory principles. For example, a researcher may start with prior theory, then go on to collect empirical data, and analyse it using grounded theory coding techniques.

The *constant comparative method* is particularly appropriate for this research project because both OC and NC can be investigated within a single study. Due to similar characteristics, it may be hard to separate traits of OC and NC. For example, hierarchy in an organisation could be a result of a bureaucratic culture within the organisation [32] or the effect of a NC trait of high power distance [12]. A *constant comparative method* allows to overcome this challenge by first performing *in-case analysis* to analyse data within each country and then *cross-case analysis* to compare results between two research settings.

Data collection was carried out using semi-structured *in-person* interviews. Interviews are suitable to study behaviour [30] because interview participants are given an opportunity to describe their past experiences and incidents. Company selection for this project was partly opportunistic. Organisations from a diverse set of industries were selected. Using personal connections, seven companies were interviewed in the United States from September to November 2012, and eight companies in Ireland from June to August 2013. Details about US and Irish companies are given in Table 1 and Table 2.

Table 1. Facts about US companies

Name (aliases)	**Industry type? When founded, size?**	**Number of people interviewed and their organisational roles**
CloudSer	IT; 1998; large	One person – a software developer
RetCo	Finance; 1932; large	One person – a security executive
CivEngCo	Civil Engineering; 1945; SME	One person – a civil engineer
TechCorp	IT; 1968; large	Two security researchers
EducInst	Education; 1868; large	Two people – an administrator and a lecturer with substantial industry experience in the security field
FinCo	Finance; 1982; large	One person – a security consultant

PublCo	Publishing; 2005; SME	One person – a business owner

Table 2. Facts about Irish companies

Name (aliases)	Industry type? When founded, size?	Number of people interviewed and their organisational roles
TechCorp	IT; 1968; large	Two people – a product manager and an IT executive
CharOrg	Charity; 1883; large	One person – a data protection officer
BevCorp	Food and Beverage Manufacturing; 1944; large	One person – an IT executive
PublOrg	Publishing; 2000; SME	One person – a chief editor
EducOrg	Education; 1845; large	Two people – an administrator and a lecturer with substantial experience in information security research
TelCommCorp	IT; 1984; large	One person – a software developer
ResReg	Energy Regulation; 1999; SME	One person – a policy analyst
BankOrg	Finance; 1982; large	One person – a security executive

The interview guide was constructed following a thorough analysis of the literature. The guide included questions about OC values and security countermeasures and their relationships with employee security behaviour. A list of the most prominent OC frameworks used in IS research was borrowed from Leidner and Kayworth's [33] work. Due to the evident similarity, these values were grouped into categories, including Solidarity, Sociability, People-Orientation, Task-Orientation, Rule-Orientation, and Hierarchy.

With regards to security countermeasures, various classification have been offered by IS researchers on deterrent mechanisms. This research adapts D'Arcy et al.'s [3] taxonomy of security countermeasures, suggesting the following four topics for the interview guide – Employee Awareness, Information Security Policy, Information Security Training, and Technical Controls. Interview guide topics including corresponding references and questions are illustrated in Table 3.

Table 3. Interview guide topics

Topics	Reference	Examples of questions
Organisational Culture		
Solidarity	Goffee and Jones [34]	Do you ever voluntary work overtime in order to complete some important task?
Sociability	Goffee and Jones [34]	Is it common to have non-work related chats with your colleagues during work hours?
People-orientation	Cooke and Lafferty [35]	How satisfying is the you are working for with respect to employee benefits?
Task-orientation	Cooke and Lafferty [35]	Do you think management expects you to put company goals before your personal goals?
Rule-orientation	Denison and Mishra [36]	Is it acceptable to break rules in your organisation?
Hierarchy	Ouchi [37]	Is it common in your organisation to disagree with your superior's opinion/decision?

Deterrent Security Countermeasures		
Technical Controls	D'Arcy et al. [3]	What information security rules and practices are utilised in your organisation?
Information Security Policy	D'Arcy et al. [3]	Is there an information security policy in your organisation?
Information Security Training	D'Arcy et al. [3]	Did you ever have to attend information security training?
Employee Awareness	D'Arcy et al. [3]	What information security values exist in your organisation?

4 Preliminary Findings

Data analysis is currently ongoing but a number of interesting preliminary results have emerged:

4.1 Organisational Culture Values and Security Behaviour

So far, preliminary results suggest that OC impacts upon employee security behaviour. CivEngCo is a bureaucratic organisation where rules and discipline prevail, and segregation between management and regular employees exists. Employees in this organisation generally comply with rules. A Civil Engineer, who is also an ambitious and creative individual, informs:

> "…typically, employees conform with information security rules".

However, this is an organisation with established procedures and practices and normally higher management is reluctant to except new ideas and change traditional ways of conducting business. A motivated and striving employee would find it hard to survive in this type of environment. The same Civil Engineer shares her disappointment:

> "I remember, one time I really wanted to change the design methodology…the manager of the project did not accept it but I had my supervisor backing me up… so we made a big meeting-fight…it was a very tough meeting…and finally I could convince them to change their approach... the type of practice they do is too old… and these old managers…it is so hard to change their minds…"

Furthermore, the same Civil Engineer adds that the fact that she cannot challenge management's decision discourages her and negatively affects every aspect of her job, including compliance with information security rules:

> "…If I lose my motivation, it affects everything, in particular the quality of job that I do, such as how I archive things, how I back up things, how I care about everything, including organisation in general and security in particular. Of course, it affects everything".

EducOrg demonstrates similar traits of organisational culture, where ambitious employees are not encouraged to strive because promotions are scarce and some managers have a reputation of treating employees improperly. Since a promotion may entail a migration to a different department managed by an unfair manager, staff is reluctant to apply. Additionally, due to internal politics, promotions are not distributed justly. As a result, this atmosphere creates a lax attitude towards information security:

> "…For the last few years there have not been too many opportunities to be promoted…but if a promotion is coming up, I feel I don't stand a chance…I am happy in the place I am at the moment…if I go somewhere else, it might be like walking on a frying pan…Right now there is an opportunity for a promotion but I would not go there because a lot of managers in this department have a reputation of treating staff really, really, really badly. And this atmosphere creates a lax attitude towards sensitive information…the attitude is "it's not my job".

On the contrary, in CloudSer there is an environment where employees are welcome to express their opinions and contribute to various aspects of company's functioning. Employees are encouraged to provide feedback regarding information security rules and in some instances, they are trusted to make independent decisions as this organisation does not have rigid rules and procedures. A Software Developer reveals:

> "…a security team designs and implements an information security policy…however, there have been instances when software engineers did not agree with certain aspects of the policy…for example, two-factor authentication…but there is a communication channel…we talked it out and agreed that two-factor authentication is vital… but if I felt a requirement was too restrictive and I could not challenge it, I would really view my security policy differently…but the fact that I can challenge, changes my opinion…I feel I can contribute…I feel it is participative…I do not feel excluded…"

> "…in terms of security rules, nobody has tried to violate the rules…we have a fairly relaxed environment in terms of security rules…there is a lot of trust which is placed on the employees to make the right choices..."

RetCo is a financial organisation, where employees also are encouraged to provide feedback regarding security rules and changes have been made in the past based on this feedback. Staff are proud to work for this organisation. Subsequently, employees comply with organisational rules. A Security Executive Officer reports:

> "…I think in our organisation some of those unwritten assumptions would be that everybody matters in the organisation, so everybody has an opinion and equal voice…people are very proud to work here…and as a result, there is this assumption that everybody is going to conduct themselves in a manner that is appropriate for that value...they are happy to be there and working there…"

> "…I have not heard personally of any instance where somebody has broken a rule, a fixed rule…"

The above analysis leads us to conclude that OC affects employee security behaviour. A flat organisational structure and employees' involvement in a company's life have a positive effect on employee compliance with information security rules. However, employee-management segregation, poor management, and an unjust treatment of employees lead to disappointment and ultimately to a lax attitude towards information security.

4.2 National Culture and Security Behaviour

Although findings reveal that employees break rules in organisations in both countries, group non-compliance with rules in Ireland is more prevalent than in the United States. Besides, a larger amount of incidents was recorded in Irish organisations than in the United States. A Security Executive of an Irish financial institution shares the following:

> "…I would like to be a bit stricter on some of the rules. Sometimes, after implementing a certain security measure, someone in a managerial position may ask to have an access to something that is forbidden to access…the rules should be there for everybody…and they are not…once certain people ask, I have to circumvent the rule…the rule is broken then. At the moment, really senior people want to have access to Twitter…that will be another battle…"

An IT manager from BevCorp further confirms that rules get broken collectively in Ireland:

> "…I think breaking rules is kind of an Irish thing…'sure that rule does not apply to me because I have a good excuse or I can reason myself out of why I did not follow the rules'… I have definitely seen rules being broken…and the level of acceptance for that from peers…it is not like one person did it and everyone was shocked…they are not going to tell on somebody as well…"

Finally, a Software Developer at TelCommCorp verifies that Irish employees break rules as a group:

> "…One of my colleague's laptop was stolen from her work desk…I think there is a policy that if you leave your laptop at work, you are supposed to chain it to the desk…she did not anyway and I never do…I leave my laptop there every evening and I do not lock it…and a lot of people leave their laptops at work without locking them…the general attitude is: 'if it is robbed, it is not my problem…it is company's security is lacking' "

In the United States, however, employees seem to be breaking rules individually and collectively. A Civil Engineer from CivEngCo shares:

> "…If I like the organisation, then I follow their security rules, of course. If I get disappointed with the organisation, then I don't care about anything, one of them would be security"

A Security Researcher from TechCorp adds:

> "…My laptop is sitting on my desk upstairs and I am not supposed to leave it…so this is an example of a rule I have broken today…My laptop should be in a hibernated mode…I don't hibernate it, I usually just suspend it, so this is a violation of the policy"

Finally, a Professor from EducInst adds:

> "…At EducInst we break rules all the time…When was the day I didn't break a rule?...Let me give you an example…a student needs a resource…there is a lot of rules about handling and allocating…I might just cut through them and make sure that a student gets the resource…and I am not interested about whether the right form is being filled out"

As can be seen from the above quotes, in Irish organisations breaking rules at a group level is more prevalent than in the United States.

4.3 Security Countermeasures and Security Behaviour

Results show that security countermeasure, including *security training*, *policies* and *awareness programmes*, inform employees about organisational security rules and encourage appropriate behaviour. A Software Developer from CloudSer shares:

> "...educating employees to make the right choices is very important…employees should understand why they should not go to certain sites or why they should not do something within the corporate firewall…"

A Security Researcher from TechCorp reveals:

> "Information security policy dictates things like what should I do with registered secret documents and I have to follow those rules… and this is one rule [related to secret documents] I would not want to break because if something happens, it is bad. Information security policy definitely affects what I do".

A Security Consultant from FinCo adds:

> "…I think information security policy creates a framework that people shape their day-to-day work around".

Finally, Security Executive from RetCo further confirms:

> "…training affects employees' behaviour…an alternative way to educate employees is to remind them of the safe security practices by sending notifications and bulletins…I think this is another way employees interact with information security policy and it affects how they do their jobs…"

Generally, the above quotes suggest that procedural security countermeasures positively affect employee security behaviour in organisational settings.

5 Conclusion

Preliminary results indicate that security countermeasures, OC, and NC impact upon employee security behaviour in organisational settings. In terms of OC, in the organisations where employees are empowered to make changes and express their opinion, staff compliance with security rules is prevalent. However, in organisations where employees are discouraged to implement new ideas and employee-management segregation exists, security rules get broken. Wallach [32] labels culture based on power and control as bureaucratic. Organisations, where bureaucracy prevails, are resistant to implement changes. Therefore, a strong bureaucratic culture is unlikely to attract and retain creative and ambitious people [32]. On the contrary, in companies with supportive culture, employees are involved in organisation's matters and are given power to speak up. Supportive culture promotes employee autonomy, which leads to improved overall performance of an organisation [38]. Hence, if an organisation explicitly states that information security is its vital function, employees will be inclined to comply with rules.

Regarding NC, employee security behaviour in organisations in the United States and Ireland shows slightly different patterns. In particular, in the United States, employee security actions are driven by a combination of factors, including individual interests and group aspects. However, in Ireland, collective disobedience with security rules is more prevalent. The influence of peer pressure may be stronger in Ireland as opposed to the United States due to the difference in the score on *individualism*. Interestingly, Zhang et al.'s [23] work demonstrate that in collectivist China the pressure from group's *majority influence* on *minorities* is stronger than in the United States. Therefore, security practitioners may need to focus on *group participant-led security trainings* in collectivist countries as oppose to computerised security tests performed individually.

Security countermeasures, including *security policy*, *awareness programmes*, and *security training* encourage employee compliance with security rules. These deterrent countermeasures serve as important guidelines for employees to distinguish between appropriate and inappropriate actions. When employee are aware of company's security etiquette, they are less likely to engage in illicit behaviour, which is consistent with results reported by D'Arcy et al. [3]. Hence, companies are advised to have in place deterrent countermeasures. Overall, based on the aforementioned

findings, this research in progress has a potential to make a valuable contribution to research and practice.

References

1. Spears, J.L., Barki, H.: User participation in information systems security risk management. MIS Quarterly, 34 (3), 503-522 (2010).
2. Posey, C., Bennett, R. & Roberts, T.L.: Understanding the mindset of the abusive insider: an examination of insiders' causal reasoning following internal security changes. Computers & Security, 30 (6-7), 486-497 (2011).
3. 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).
4. Lee, S.M., Lee, S.G., and Yoo, S.: An integrative model of computer abuse based on social control and general deterrence theories. Information & Management, 41 (6), 707-718 (2004).
5. Hu, Q., Dinev, T., Hart, P., and Cooke, D.: Managing employee compliance with information security policies: the role of top management and organizational culture. Decision Sciences, 43 (4), 615-660 (2012).
6. Hu, Q., Xu, Z., Dinev, T. and Ling, H.: Does deterrence work in reducing information security policy abuse by employees? Communications of the ACM, 54 (6), 54-60 (2011).
7. Ifinedo, P.: Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Computers & Security, 31, 83-95 (2012).
8. D'Arcy, J. & 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), pp. 643-658 (2011).
9. Son, J-Y.: Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. Information & Management, 48 (7), 296-302 (2011).
10. Pavlou, P.A. and Chai, L.: What drives electronic commerce across cultures? A cross-cultural empirical investigation of the theory of planned behavior. Journal of Electronic Commerce Research, 3 (4), 240-253 (2002).
11. Dinev, T., Goo, J. Hu, Q. and Nam, K.: User behaviour towards protective information technologies: the role of national culture differences. Information Systems Journal, 19 (4), 391-412 (2009).
12. Hofstede, G.: Culture's Consequences: International Differences in Work-related Values. Sage Publications, Thousand Oaks, CA (1980).
13. Ali, M. and Brooks, L. Culture and IS: National Cultural Dimensions within IS Discipline. In: Proceedings of the 13th Annual Conference of the UK Academy for Information Systems, pp.1-14 (2009).
14. Kroeber, A.L. and Kluckhohn, C.: Culture: A critical review of concepts and definitions. Peabody Museum, Cambridge, United States (1952).
15. Baker, E.L.: Managing organizational culture. Management Review, 69, 8-13 (1980).
16. DeLong, D.W., and Fahey, L.: Diagnosing cultural barriers to knowledge management. Academy of Management Executive. 14 (4), 113-127 (2000).
17. Mead, M.: National character. In: S. Tax, eds. 1962. Anthropology Today. Chicago: University of Chicago Press, 396-421 (1962).
18. Triandis, H.C.: The Analysis of Subjective Culture. Wiley, New York (1972).

19. Kilmann, R.H.: Managing your organization's culture. The Nonprofit World Report, 3 (2), 12-15 (1985).
20. Phillips, M.E.: Industry mindsets: Exploring the cultures of two macro-organizational setting. Organization Science, 5 (3), 363-383 (1994).
21. Hofstede, G.: Culture's Consequences. Comparing Values, Behaviors, Institutions, and Organizations Across Nations.3rd Edition. Sage Publications, Thousand Oaks (2001).
22. Flores, W.R., Antonsen, E. and Edstedt, M.: Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. Computers & Security, 43, 90-110 (2014).
23. Zhang, D., Lowry, P.B., Zhou, L. and Fu, X.: The Impact of Individualism-Collectivism, Social Presence, and Group Diversity on Group Decision Making under Majority Influence, Journal of Management Information Systems, 23 (4), 53-80 (2007).
24. Mintzberg, H.: Structure in fives: Designing effective organizations. Prentice-Hall Int., Englewood Cliffs (1983).
25. Besnard, D. & Arief, B.: Computer security impaired by legitimate users. Computers & Security. 23 (3), 253-264 (2004).
26. Beccaria, C.: On Crimes and Punishment. Macmillan, New York (1963).
27. Herath, T. and Rao, H.: Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness. Decision Support Systems, 47 (2), 154-165 (2009).
28. Siponen, M., Vance, A.: Neutralization: new insights into the problems of employee information systems security policy violations. MIS Quarterly, 46 (5), 487-502 (2010).
29. Matavire, R. and Brown, I.: Profiling grounded theory approaches in information systems research, European Journal of Information Systems, 22 (1), 119-129 (2013).
30. Maykut, P. and Morehouse, R.: Beginning Qualitative Research: A Philosophic and Practical Guide. The Falmer Press, London (1994).
31. Lincoln, Y. and Guba, E.: Naturalistic Inquiry. Sage Publications: Beverly Hills (1985).
32. Wallach, E.J.: Individuals and organizations: The cultural match, *Training and Development Journal*, 37 (2), 28-36 (1983).
33. Leidner, D.E., Kayworth, T. Review: A review of culture in information systems research: Toward a theory of information technology culture conflict. MIS Quarterly 30, 357-399 (2006)
34. Goffee, R., and Jones, G.: What holds the modern company together? Harvard Business Review, 74 (6), 133-148 (1996).
35. Cooke, R.A. and Lafferty, E.: Organizational Culture Inventory. Human Synergistics, Plymouth (1987).
36. Denison, D.R., and Mishra, A.K..: Toward a theory of organizational culture and effectiveness. Organization Science, 6 (2), 204-223 (1995).
37. Ouchi, W.: Theory Z: How American business can meet the Japanese challenge. Addison-Wesley Publishing Company, Reading (1981).
38. Shrednick, H.R., Stutt, R.J. and Weiss, M.: Empowerment: key to is world-class quality, MIS Quarterly, 16 (4), 491-505 (1992).