Managing Employee Security Behaviour in Organisations: The Role of Cultural Factors and Individual Values

Lena Connolly[1], Michael Lang[1], and Doug Tygar[2]

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

Abstract. An increasing number of information security breaches in organisations presents a potentially serious threat to the privacy and confidentiality of personal and commercially sensitive data. Recent research shows that human beings are the weakest link in the security chain and the root cause of a great portion of security breaches. In the late 1990's, a new phenomenon called "information security culture" has emerged as a measure to promote security-cautious behaviour of employees in organisational settings. The concept of information security culture is relatively new and research on the subject is still evolving. This research-in-progress paper contributes to our understanding of this very important topic by offering a conceptualisation of information security culture. Additionally, this study indentifies factors that instigate adverse employee behaviour in organisations.

Keywords: Information Security, Information Security Culture, Organisational Culture, National Culture, Employee Behaviour, Individual Values.

1 Introduction

With the arrival and the widespread of the Internet and the personal computer, the Information Age has swiftly replaced the era of industrialisation and the knowledge-driven economy transformed the way various industries run their operations. The automobile industry is an obvious illustration of this shift – a new car today is less and less a manufacturing product and more a smart machine that uses computer technology to combine safety, emissions, entertainment and performance. Technological advances rely on knowledge, and knowledge turns into information once it is shared. Therefore, information is a valuable asset for a lot of organisations. As online presence has also developed into a key business value, many companies have been pushed to move their operations on the Web along with this information, stored and managed by computerised information systems.

While online presence entails a myriad of benefits such as reduced costs and an extended customer base, major risks are involved, including the potential loss or violation of vital information. Protecting these assets is the highest ranked priority for

N. Cuppens-Boulahia et al. (Eds.): SEC 2014, IFIP AICT 428, pp. 417–430, 2014.

many businesses as their very existence depends on certain information. The consequences of lost information may vary from a breach of privacy for customers to complete disruption of business operations for organisations. While information predators have become more sophisticated, many legitimate businesses are either not aware or neglect the fact that the consequences of an information security breach can be rather dramatic. A recent attack on Loyaltybuild, a company that manages customer loyalty schemes across Europe, is an evident example of negligence. Attackers exploited enormous weaknesses in Loyaltybuild's security system, leading to the loss of personal information of more than 1.5 million customers. As was revealed later, the company kept sensitive information in an unencrypted form [1].

A number of critical measures to manage information security breaches in organisations have been highlighted within the literature, including reliable internal processes and good corporate governance as well as technical and socio-cultural measures [2]. Historically the use of technical controls has prevailed over socio-cultural solutions in organisational settings. However, in the late 1990s, Information Systems (IS) researchers have brought attention to the latter because technical controls are powerless to manage all types of security violations. For instance, a technical control is unable to prevent employees from writing passwords down. Besides, empirical studies show that although businesses are spending more on technology-based solutions, the number of information security breaches is actually on the rise [3].

In the late 1990's, the new concept of Information Security Culture (ISC) has emerged as a measure that promotes security-cautious behaviour of staff [4]. In a general sense, ISC can be defined as the "behaviour in an organisation that contributes to the protection of data, information and knowledge" [5]. A more comprehensive definition of ISC is that put forward by da Veiga and Eloff [2] as:

> "*attitudes, assumptions, beliefs, values and knowledge that employees/stakeholders use to interact with the organisation's systems and procedures at any point in time*".

Since its arrival, research on the topic of ISC has rapidly expanded. A great number of ISC theories and assessment instruments have been developed by IS scholars. ISC has been described using theories adapted from various disciplines including psychology [6], economics [7], behavioural sciences [8] and management [9]. Most commonly, ISC has been explained using organisational culture theories, Schein's [10] model been the most predominant [2].

Although prior research on ISC greatly contributes to the body of IS research, a number of areas require further investigation [4,11]. In particular, there is little information about what constitutes or conceptualises security culture [12]. A literature review conducted in the course of this research also has revealed a dearth of quantitative studies in the area of ISC. Furthermore, prior research in the information security area demonstrates that studies that include organisational culture generally lack strong theoretical foundations for linking organisational culture values to information security outcomes [13]. Moreover, Dinev et al. [14] point out to the lack of cross-cultural research in the IS field. This research-in-progress paper aims to address the aforementioned research gaps and accomplish the following objectives:

1. Identify the factors that impact upon employee behaviour with regards to information security in organisational settings using an exploratory research approach.

2. Test the relationships between these factors and employee security behaviour using a confirmatory research approach.

This paper is organised as follows. We first present a theoretical framework that guides this study followed by a definition of culture adopted in this research. This is followed by research methodology and preliminary results of qualitative data analysis. The paper then wraps up by outlining future research directions, and alluding to some of the limitations and challenges that lie ahead for us.

2 Theoretical Framework

We submit that various cultural aspects should be taken in consideration when studying adverse behaviour of employees in organisational settings. Numerous national and organisational culture scholars have demonstrated the effect of cultural aspects on human behaviour. For example, Hofstede [15] compares culture with an onion consisting of multiple layers; values are the inner layer of the onion and the core element of culture. They are invisible until they become evident in behaviour. Furthermore, Hofstede [16] and Spector [17] demonstrate a connection between national culture values and employees' compliance with authority and organisational policies and rules.

Typically, organisational culture researchers define culture as a "set of shared values, beliefs, assumptions and practices that shape and direct members attitude and behaviour in the organisations" [4, p.88]. Kilmann [18] describes culture as a separate and hidden force that controls behaviours and attitudes in organisations. A study conducted by Porter and McLaughlin [19] further demonstrates the significant role that organisational climate plays in shaping employee behaviour.

The notion of ISC culture has been also linked to human behaviour. For instance, Kraemer and Carayon [20] stress that ISC emerges from the way in which people behave towards information and the security thereof. In particular, ISC influences behaviour in such a way that employees develop "good" practices based on security standards and policies of a particular organisation. Schlienger and Teufel [21] emphasise the importance of establishing ISC as important measure to address the "human error" factor.

We propose a theoretical model that combines De Long and Fahey's *taxonomy of organisational culture* [22], Wallach's *organisational culture model* [23], Hofstede's original *taxonomy of national culture* [16] and Schwartz's *Theory of Motivational Types of Values* [24] as presented in Figure 1.

In IS research, organisational and national culture have been predominantly measured in terms of values [25]. Following Leidner and Kayworth's catalogue of organisational and national culture taxonomies [25], a variety of cultural frameworks has been examined in order to choose appropriate models for this research. Wallach's comprehensive *framework of organisational culture* [23] was selected to form the organisational culture part of our model. Wallach identified and defined three distinct organisational cultures, - *bureaucratic*, *innovative* and *supportive*, - covering almost all the values outlined by Leidner and Kayworth [25]. Additionally, Wallach's model has been adapted in quantitative [33] as well as cross-cultural [27] studies in IS research. Wallach's Organisational Culture Index will be used in this research to measure organisational culture.

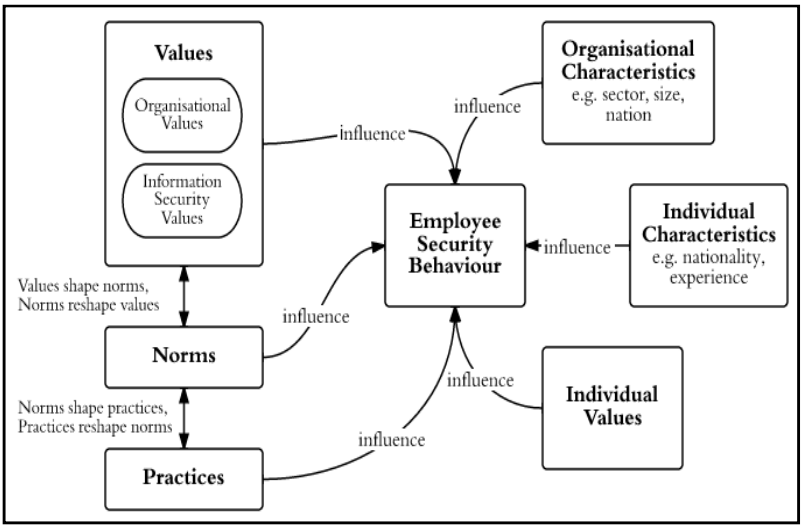

Fig. 1. Theoretical framework

To date, Hofstede's taxonomy of cultural values [16] has been the most popular conceptualisation of national culture. Hofstede defines culture in terms of four values – *power distance*, *uncertainty avoidance*, *individualism-collectivism* and *masculinity-femininity*. Hofstede's scores of cultural values will be used as the measure of culture because they have been subject to more checks of internal validity, external validity and reliability than the measures used in any other cross-cultural study. Additionally, Hofstede's research is the largest study of cultural values ever undertaken both in terms of number of countries and number of respondents [28]. National culture needs to be considered in terms of its impact on organisations and also individuals.

To test the influence of individual values on behaviour with regards to information security, the *Theory of Motivational Types of Values* by Schwartz [24] was chosen. Schwartz's model is viewed as the most comprehensive approach, covering 56 values grouped into 10 categories. The *Theory of Motivational Types of Values* demonstrates strong generalisability as it has been successfully tested in more than 60 countries [26].

2.1 Culture

For the purpose of this research, culture is viewed as a phenomenon that can be observed at multiple levels in an organisation. Culture is reflected in three levels – values, norms and practices [22].

At the deepest level, culture consists of values, which are embedded tacit preferences about what the organisation should strive to attain and how it should do so. For instance, if an organisation values customer confidentiality, employees will treat customer information with extra caution by following data protection requirements outlined by this organisation.

Norms generally stem from values, but they are more observable [22]. For instance, if rules with regards to customer confidentiality are breached, a termination of employment may be a norm in an organisation that puts high emphasis on customer confidentiality.

Practices are the most visible symbols and manifestations of a culture. In the context of information security, this level is related to the implemented security measures and processes [29].

Values, norms, and practices are interrelated: values are revealed in norms that, in turn, shape specific practices. While values shape norms and practices, sometimes managers will change practices and norms in an attempt to reshape values over time. Values, norms and practices directly influence employee behaviour [22].

3 Research Methodology

This study follows Clark and Creswell's [30] Sequential Exploratory Mixed Method approach consisting of a qualitative phase to be subsequently followed by a quantitative phase. Data collection for the qualitative phase of this study was carried out using semi-structured interviews. The interview guide was built on Wallach's taxonomy of organisational culture. Additionally, general questions about ISC were asked in order to tease out ISC values. Interview guide topics including corresponding values and questions are demonstrated in Table 1.

Table 1. Interview guide topics

Topics	Values	Examples of questions
Information Security Culture values, norms and practices	unknown	What information security values are promoted in your organisation? In your opinion how well confidential information is protected in your organisation?
Orientation to rules	Procedural, regulated, cautious	Is it acceptable to break rules in your organisation?
Hierarchy vs. Equality	Hierarchical, power-oriented, ordered, structured vs. equality, collaboration, personal freedom	Is it common in your organisation to socialise with management?
Competitive environment	Driving, challenging, enterprising	Is competition between colleagues promoted in your organisation?
Employee welfare	Stimulating, encouraging	How satisfied are you with a benefit system provided by your organisation?
Friendliness vs. Pressure	Relationships-oriented, trusting, good place to work vs. results-oriented, pressurised	Is it acceptable to have non-work related chats in your organisation?
Sociability	Sociable	Do you socialise with your colleagues?

Overall seven organisations were interviewed, all based within the United States. Initially, we planned to conduct two interviews in each organisation – one with an executive and another with an employee to gather various views. However, the subject of information systems security is rather sensitive, therefore access to potential interviewees was restricted. In total, nine interviews were conducted. All interviews were recorded and transcribed using a professional service. To preserve confidentiality, all companies have been assigned aliases when referred to herein.

The methodology adopted for the qualitative phase of this study is based on the constant comparative method according to Maykut and Morehouse [31] who draw on the work of Glaser and Strauss [32] and Lincoln and Guba [33] in their development of this methodological framework. "In the constant comparative method the researcher simultaneously codes and analyses data in order to develop concepts; by continually comparing specific incidents in the data, the researcher refines these concepts, identifies their properties, explores their relationships to one another, and integrates them into a coherent explanatory model" [34].

4 Findings

In the first phase of qualitative data analysis, Open Coding, we identified and labeled discrete incidents of data related to cultural values, norms and practices. An example of our coding is shown in Table 2.

Table 2. Interview guide topics

Example excerpt from interview at RetCo, October 2012	**Open Coding**
We use several different levels of rules in the organisation. We have policies that are very high level statements and those are informed by our kind of company values and then we have below the policies we have standards, so information security standards and privacy standards, that we follow and then underneath that we have specific practices and procedures and those are very rigid, those are if you're going to do a certain thing you need to follow a procedure and those are all published and accessible to all of our employees on an intranet website so there's no question about if people want to learn how to do something or learn what those are that's readily available in addition to a lot of training that informs employees about them as well. So that's kind of the hierarchy and then in some cases we have even published and maintained some guidelines on how to do certain things and recommendations on security, not just at work but in the home too, so employees are given information on how to protect themselves at home on information security and those are more guidelines of course because we don't have controls over what people do at home but we feel that if people are practising good safe practices at home it's going to translate over at the work environment as well	Values: • *Information Security* • *Individual Privacy* *Norms*: • *Keeping information secure* • *Following procedures* Practices: • *Policy* • *Education*

In further data analysis, the initial codes were grouped into organisational and information security values, norms and practices following De Long and Fahey's *taxonomy of organisational culture* [22]. Consistent with Wallach's *model of organisational culture* [23], eight organisational values have been identified: *hierarchy*, *rule-orientation*, *pressure*, *stimulation*, *sociability*, *relationships*, *equality*, and *drive*. In accordance with Schwartz's *Theory of Motivational Types of Values*, three individual values have been defined: *achievement*, *benevolence*, *conformity*, and *self-direction*. Additionally, a self-defined classification of Information Security Culture has emerged containing four values: *information security* (high vs. low), *information confidentiality* (high vs. low), *rule-orientation*, and *equality*. Each of these ISC values are briefly described below, along with examples of how these values are manifested in interview data.

4.1 Information Security Culture Taxonomy

Information Security (High). Modern organisations accumulate huge volumes of information including sensitive information. The breach of this information first leads to its exposure and then may result in a breach of privacy and financial losses. Security of a computer-based information system should, by design, protect the confidentiality, integrity, and availability of the system that contains sensitive information [35].

CloudSer is a software company that provides cloud and virtualisation software and services. Therefore, protecting customer information is a high priority for this organisation. A Software Engineer of CloudSer was clear about the company's standpoint with regards to information security:

> "Everybody understands that security is a big concern from a lot of aspects, so I would tend to think they [information security rules] are working … Information security is a central function across the organisation."

RetCo, a company that manages retirement and health plans, also puts high emphasis on information security due to sensitive nature of the information they store. A RetCo Security Officer states:

> "We use several different levels of rules in the organisation. We have policies that are very high level statements and those are informed by our company values, and then below the policies we have standards. So we have information security standards and privacy standards that we follow, and then underneath that we have specific practices and procedures, and those are very rigid … And then in some cases we have even published and maintained some guidelines on how to do certain things and recommendations on security, not just at work but in the home too, so employees are given information on how to protect themselves at home on information security, and those are more guidelines, of course, because we don't have controls over what people do at home, but we feel that if people are practising good safe practices at home, it's going to translate over at the work environment as well."

Information Security (Low). On the contrary, EducInst, a higher education institution, has a different attitude towards information security. Although the organisation seems to have in place various security measures, e.g. technical controls, education and training, and ISP, information security is not a priority in EducInst. For instance, although ISP exists, employees are not aware of its presence, and education and training is poorly organised. The interviewee commented:

> "There is a formal set of rules and practices are online, and they're far too detailed to discuss here … [For example, we have] very specific rules about personally identifiable information such as a social security number. So if you send me a resumé, it's got lots of personally identifiable information on it, I have to be very careful to protect that and not store it in an unencrypted form on my computer, otherwise I'm in breach of those rules. And that's actually a State law, so it's not just an EducInst rule. A State law that's largely ignored by most people here, but it's on the books … In EducInst, information security values are way, way, way down on the list. People give lip service to it … What's officially on the books and what the actual practice is, those are two different things."

Information Confidentiality (High). Understandably, companies that acquire and store confidential information, must prioritise information confidentiality. An unauthorised use and disclosure of confidential data leads to dramatic consequences for individuals and organisations. The goal of confidentiality is to ensure that information is not accessed by an unauthorised person [36].

CloudSer has a large customer base and retains confidential information of their clients. Keeping this information secure is of most important value as its disclosure may damage companies' ability to run business. A Software Engineer of CloudSer says:

> "…any company which is providing software, which other companies rely on or possesses, like details about company, the customers enterprise deployment, you need to value that trust, so you can't break some rules with respect to that. We have 300,000 customers, some of those customers are competitors of the other guys. So let's just hypothetically say I have Pepsi and Coke as my customers, right…I can't tell Pepsi what Coke is doing, I can't tell Coke what Pepsi is doing. So our customers trust us with that information knowing that we might as well be serving Pepsi. So, yeah, there are certain rules that you cannot break without getting fired."

Due to its nature of business, RetCo holds a lot of personally identifiable information (PII). Therefore, information confidentiality is highly prioritised by this organisation as stated by their Security Officer:

> "We have security standards and practices around encryption, such as what type of encryption is approved to use in the environment, what has to be encrypted, and to what level, and also how these encryption keys are handled and managed in the organisation. We have policies

> and practices around physical access to the computer room, and so we have certain levels of access and certain approval processes in place like who can access our protected areas, and what levels of approval have to happen, and we have things in place like not just card key electronic access, but we have things like Iris scanner technology to get in to the computer rooms and things of that nature, and, of course, we've got these practices and procedures and processes that are in place to support that physical access."

Information Confidentiality (Low). Although EducInst also possesses PII, our informant revealed that this organisation is not particularly concerned about information confidentiality of their customers:

> "As I said, I think things tend to be fairly casual in terms of protecting people's privacy. For example you know, let me give an example. So protecting credit card numbers, right. So people's credit card numbers are floating all around this organisation. If you were interested in stealing a lot of credit card numbers, it would be so easy to do in this organisation. Again, just because of the casualness with which people treat information … Let me give you an example, at EducInst we are rolling out a new system for paying disbursements. We have a chief privacy officer who is supposed to be in charge of protecting privacy at EducInst. But my secretary was able to use that system to find out things like the Provost's credit card number, or names of all the students who'd been treated for genital warts, or the names of a police officer who had to undergo a psychological help after an incident. She pointed these problems out to the chief privacy officer, and the chief privacy officer could do squat about them … So my point is that we have all the stuff on the book, and there's State laws about it, but it's largely ignored because it's not a value of the organisation."

Equality. CloudSer and RetCo are two companies that emphasise employee input with regards to information security measures. At CloudSer and RetCo, employees are encouraged to provide feedback about information security rules. According to both interviewees, based on employees' comments, rules can be changed. In these organisations everyone has equal voice and ability to speak up regardless of rank or position. It's a highly collaborative and opinionated environment where employees at all levels are easy to approach [23]. A Software Engineer at CloudSer explained that:

> "For the security measures they bring about, they introduce it to the employees before its roll out, they test it out, and then they take employee feedback to see if it's too intrusive or too restrictive for that matter. So it's generally participative, but I haven't really seen any security measure being repealed because employees do not like it … Generally, people do accept that [security rules are] there for a good reason, unless it's like prohibitively restrictive which it's not the case in my company"

A Security Officer at RetCo adds:

> "I think a lot of times employees having this open dialogue, they can change the rules by bringing things up. I've seen it happen in the past, where the enterprise will make a decision to lock computers, the keyboards on computers, after a certain amount of time, when the computer is idle, and that's because people may get up and walk away from their computer, and they want to lock the screen and make sure that nobody else can walk by and access the information. So employees feeling empowered to challenge or to at least bring up the issues, have made a lot of changes in their user environments because of that. So, for example, if it's 10 minutes of inactivity and the computer locks, the screen lock, employees have complained and said, 'you know, it's really closer to 20 before we really are not working on it', and so the policies have been changed based upon the use of the users and them providing that feedback."

Rule-Orientation. In the rule-oriented organisations, rules are very important and are not allowed to break. These companies are procedural, regulated, and cautious and put high emphasis on following information security policies and procedures [26]. A Security Officer at RetCo reveals:

> "It's not acceptable to break rules in our organisation. Mostly because most of our rules are derived from regulations and laws so that's something that is not normally accepted in the organisation …We use several different levels of rules in the organisation. We have policies that are very high level statements, and those are informed by our company values, and then below the policies we have standards, so information security standards and privacy standards, that we follow, and then underneath that we have specific practices and procedures, and those are very rigid, those are if you're going to do a certain thing, you need to follow a procedure."

A Security Consultant at FinCo adds:

> "If there is a rule in place, the rule is in place for a reason and you don't break it, you request an exception and you have to talk to the right people to request an exception. So you never just break a rule … The security practices are fairly extensive for SOX and GLBA compliant environment, so we have to be audited for both of those on a yearly basis, although actually we go through audits I think twice a year. And then we have an internal audit office that basically does audits twice a year as well, to make sure that we're going to be able to pass those Federal Mandated Audits … So we pretty much follow best practices that are mandated."

4.2 Interpretation and Further Propositions

In most organisations interviewed for this study, employees circumvent information security rules. Following De Long and Fahey's [22] framework of organisational culture, organisational values, norms and practices have to be aligned and this alignment encourages behaviour that is in accordance with organisational values. However, in companies where dysfunctional behaviour was recorded, our results are inconsistent with De Long and Fahey's framework. For instance, while these organisations put high value on information security, conflicting practices (e.g. *lack of education)* and norms (e.g. *casualness in terms of protecting confidential information*, *circumventing rules*, *nobody ever reads policy because it is too big*, *policy is not taught*, *rules are hard to implement*, and *screw-ups are tolerated*) were recorded. Based on this analysis, we suggest that:

Proposition 1: *A misalignment between values, norms and practices leads to employee non-compliance with an organisation's information security rules and practices.*

Further analysis revealed that clash of organisational culture values may also lead to employee adverse behaviour. For instance, TechCorp encourages employees to take risks and at the same time puts high emphasis on following procedures. In CivEngCo, higher management enforces hierarchical structure and utilises power and control in managing employees while front-line managers value equality and collaboration. Therefore, whilst employees' various opinions and new ideas are supported by lower level management, executives are resistant to except initiatives and change old processes. As a result, ambitious employees lose motivation and respect for the organisation and circumvent information security rules. Therefore, we propose that:

Proposition 2: *A conflict between organisational culture values leads to employee non-compliance with an organisation's information security rules and practices.*

Moreover, we observed that possibly employees' individual values influence behaviour with regards to information security. For instance, two employees who work for the same organisation and share identical status and nature of work, have different attitude towards information security rules. IT Corp is bureaucratic in nature and enforces religious obedience to procedures which sometimes hurt employees' productivity. Employee 1 is ambitious and hard-working but still accepts the procedure-oriented environment (individual value of *conformity*). On the contrary, Employee 2 circumvents information security rules because they are too restrictive (individual value of *self-direction*). Therefore, we conclude that incongruence between organisational and individual values leads to employee non-compliance with security rules and hence, the following proposition is derived:

Proposition 3: *A conflict between individual values and organsiational values leads to employee non-compliance with an organisation's information security rules and practices.*

5 Conclusions and Future Work

In the literature, human beings have been referred as "the weakest link in the security chain". While the importance of technical controls to prevent the "human error" factor is absolutely undeniable, technology is unable to manage all types of human violations. A socio-cultural approach addresses this problem by having a direct affect on human behaviour. Prior research has emphasised the significance of socio-cultural measures. However, there are areas that require further enquiry. This research-in-progress is an attempt to address a research gap in the area of ISC.

In the next stage of our research, we conduct further qualitative data analysis (based on a European sample, for comparative purposes), and will then develop a survey instrument based on qualitative findings. The original purpose of the qualitative phase is to develop research hypothesis, which then can be tested in the quantitative phase. In the near future, we also to plan extend this research by adding other environments including important emerging digital economies in regions such as East Asia, the Indian subcontinent, Brazil, and the former Easter Bloc. This work may allow us to better model the notion of adversarial behaviour in different regions. Therefore, from the standpoint of information security, this research has potential to make a valuable contribution to theory and practice.

In terms of shortcomings and limitations, studies that involve culture tend to be rather complex. As Straub et al. [37] put it, "culture has always been a thorny concept and an even thornier research construct". Furthermore, studies that include several cultural aspects tend to be even more complex. In particular, it may be hard to separate effects of national and organisational cultures in organisational settings due to similar characteristics. For example, hierarchy in an organisation can be a result of a bureaucratic culture of this organisation or a societal norm of the country where this organisation is located. Quantifying the concept of culture is another challenge that is anticipated in this project. In order to measure culture in a meaningful way, a value-based approach will be employed. Taking in consideration the aforementioned complexities, we would therefore welcome feedback and suggestions from other researchers who may have encountered this same difficulty or are contemplating similar avenues of enquiry.

References

1. Pope, C., Edwards, E.: Over 1.5 million affected by Ennis data breach. The Irish Times (2013), http://www.irishtimes.com/news/consumer/over-1-5-million-affected-by-ennis-data-breach-1.1592128
2. Da Veiga, A., Eloff, J.H.P.: A framework and assessment instrument for information security culture. Computers & Security 29, 96–207 (2010)
3. Von Solms, B.: Information Security – The Third Wave? Computers & Security 19, 615–620 (2000)
4. Lim, J.S., Chang, S., Maynard, S., Ahmad, A.: Exploring the Relationship between Organizational Culture and Information Systems Security Culture. In: Proceedings of the 7th Australian Information Security Management Conference, pp. 87–97. Edith Cowan University (2009)

5. Kuusisto, T., Ilvonen, I.: Information security culture in small and medium size enterprises. Frontiers of E-Business Research (2003), http://www.ebrc.info/kuvat/431-439.pdf
6. Boss, S.R., Kirsch, L.J., Angermeier, I., Shingler, R.A., 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, 151–164 (2009)
7. Van Niekerk, J.F., von Solms, R.: Information security culture: A management perspective. Computers & Security 29, 476–486 (2010)
8. Ajzen, I.: Attitudes, Personality, and Behavior, 2nd edn. Open University Press, Berkshire (2005)
9. Ray, C.A.: Corporate Culture: The Last Frontier of Control? Journal of Management Studies 23, 287–297 (1986)
10. Schein, E.H.: Organizational Culture and Leadership: The Dynamic View. Jossey-Bass, San Francisco (1985)
11. Malcomson, J.: What is security culture? Does it differ in content from general organisational culture? In: Proceedings of the 43rd Annual International Carnahan Conference on Security Technology, pp. 361–366 (2009)
12. Alnatheer, M., Chan, T., Nelson, K.: Understanding and measuring information security culture. In: Proceedings of Pacific Asia Conference on Information Systems (2012)
13. Hu, Q., Dinev, T., Hart, P., Cooke, D.: Managing employee compliance with information security policies: The critical role of top management and organizational culture. Decision Sciences 43, 615–660 (2012)
14. Dinev, T., Goo, J., Hu, Q., Nam, K.: User behaviour towards protective information technologies: the role of national cultural differences. Information Systems Journal 19, 391–412 (2009)
15. Hofstede, G.: Culture's Consequences: International Differences in Work-related Values. Sage Publications, Thousand Oaks (2001)
16. Hofstede, G.: Culture's Consequences: International Differences in Work-related Values. Sage Publications, Thousand Oaks (1980)
17. Spector, P.E.: Behavior in Organizations as a Function of Employee's Locus of Control. Psychological Bulletin 91, 482–497 (1982)
18. Kilmann, R.H.: Managing Your Organization's Culture. Nonprofit World Report 3, 12–15 (1985)
19. Porter, L.W., McLaughlin, G.B.: Leadership and the organizational context: Like the weather? The Leadership Quarterly 17, 559–576 (2006)
20. Kraemer, S., Carayon, P.: Computer and Information Security Culture: Findings from Two Studies. In: Proceedings of the Human Factors and Ergonomics Society 49th Annual Meeting, pp. 1483–1487 (2005)
21. Schlienger, T., Teufel, S.: Information security culture: The socio-cultural dimension in information security management. In: Proceedings of the IFIP TCII 17th International Conference on Information Security, pp. 191–201 (2002)
22. De Long, D., Fahey, L.: Diagnosing cultural barriers to knowledge management. Academy of Management Executive 14, 113–127 (2000)
23. Wallach, E.D.: Individuals and Organizations: The Cultural March. Training and Development Journal 37, 29–36 (1983)
24. Schwartz, S.H.: Universals in the content and structure values: Theoretical advances and empirical tests in 20 countries. Advances in Experimental Social Psychology 25, 1–65 (1992)

25. 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)
26. Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., Vance, A.: What Levels of Moral Reasoning and Values Explain Adherence to Information Security Rules? An Empirical Study. European Journal of Information Systems 18, 126–139 (2009)
27. Lok, P., Crawford, J.: The effect of organisational culture and leadership style on job satisfaction and organisational commitment: A cross-national comparison. Journal of Management Development 23, 321–338 (2004)
28. Shane, S., Venkataraman, S., MacMillan, I.: Cultural Differences in Innovation Championing Strategies. Journal of Management 21, 931–952 (1995)
29. Vroom, C., von Solms, R.: Towards Information Security Behavioural Compliance. Computers & Security 23, 191–198 (2004)
30. Clark, V.L.P., Creswell, J.W.: The Mixed Methods Reader. Sage Publications, Thousand Oaks (2008)
31. Maykut, P., Morehouse, R.: Beginning Qualitative Research: A Philosophic and Practical Guide. The Falmer Press, London (1994)
32. Glaser, B.G., Stauss, A.L.: The Discovery of Grounded Theory. Aldine, Chicago (1967)
33. Lincoln, Y., Guba, E.: Naturalistic Inquiry. Sage Publications Inc., Beverly Hills (1985)
34. Taylor, S.J., Bogdan, R.: Introduction to Qualitative Research Methods: The Search for Meanings. Wiley, New York (1984)
35. Gordon, L.A., Loeb, M.P.: The Economics of Information Security Investment. ACM Transactions on Information and System Security 5, 438–457 (2002)
36. Joshi, J.B.D., Aref, W.G., Ghafoor, A., Spafford, E.H.: Security models for Web-based Applications. Communications of the ACM 44 (2001)
37. Straub, D., Loch, K., Evaristo, R., Karahanna, E., Strite, M.: Toward a theory-based measurement of culture. Journal of Global Information Management 10, 13–23 (2002)