An Identification of Variables Influencing the Establishment of Information Security Culture

Emad Sherif[1(✉)], Steven Furnell[1,2,3], and Nathan Clarke[1,3]

[1] Computer Centre for Security, Communications and Network Research,
University of Plymouth, Plymouth, UK
{Emad.Sherif,S.Furnell,N.Clarke}@plymouth.ac.uk
[2] Centre for Research in Information and Cyber Security,
Nelson Mandela Metropolitan University, Port Elizabeth, South Africa
[3] Security Research Institute, Edith Cowan University, Perth, Australia

Abstract. A significant volume of security breaches occur as a result of the human aspects and it is consequently important for these to be given attention alongside technical aspects. Many breaches occur due to human error. Researchers have argued that security culture stimulates appropriate employees' security behavior towards adherence and therefore developing a culture of security can contribute in minimizing or avoiding security breaches. Although, research on the concept of security culture has received little attention this paper aims to address the security culture concept, and it's relation to the national culture. Specifically, it is largely hypothesized that cultivating security culture can have a positive effect on employees' security compliance. The purpose of this paper is to identify variables that influence cultivating a security culture. In order to do so, a comprehensive literature review has been conducted. The outcome of the literature analysis has identified potential variables that influence security culture (e.g. top management support, information security behavior, and awareness), and the paper subsequently outlines a framework for modeling security culture that indicates the relationship between these variables.

Keywords: Security culture · National culture · Organizational culture · Security policies · Security compliance · Security behavior

1 Introduction

Recent research shows that as many as 35 % of global of data breaches happen due to a negligent employee 'human factor' (Ponemon Institute, 2013). Unfortunately, the "user error" has been neglected by small, medium and large organizations (Connolly and Lang, 2013). According to Connolly and Lang (2013), many organizations are investing significant money and time into implementing technical security controls in order to protect their assets, whilst ignoring the human element of the problem, which is often the main cause of data breaches. We therefore, argue that establishing an information security culture can assist organizations to eliminate or minimize such breaches. Similarly, Van Niekerk and Von Solms (2010) argued that establishment of

T. Tryfonas and I. Askoxylakis (Eds.): HAS 2015, LNCS 9190, pp. 436–448, 2015.
DOI: 10.1007/978-3-319-20376-8_39

an organizational sub-culture of information security is key to managing the human factor involved in information security. Although, many researchers have been addressing the concept of 'security culture', there are not any clear views on how to create this organizational culture to support security (Ruighaver, et al. 2007). Therefore, Johnson and Goetz (2007) suggested that security executives should address secure culture when they are considering building security into their organizations. According to Da Veiga and Eloff (2010), "some research shows that a security-aware culture will minimize risks to information assets".

In the literature, security culture has been referred to as a mean to control the 'human factor' to enhance security. Therefore, the intended focus of this paper is to analyze twenty-five related studies in order to identify factors and variables that influence security culture. This discussion covers the concepts of organizational, national, and security cultures, and explores the relationship between them along with exploring the relationship between information security compliance and information security culture. This paper also presents the research model design, which leads to combining three models into a conceptual framework.

2 Literature Review and Theoretical Background

Preliminary literature search has been carried out in order to find out and define the research gaps in the area of information security. Suitable publications including peer reviewed journals and conferences were identified, and the main themes emerging from them are outlined in the sub-sections that follow.

2.1 Culture as a Concept

Most social scientists view culture as consisting primarily of the symbolic, ideational, and intangible aspects of human societies (Connolly and Lang, 2013). In terms of a definition of culture, Damen (1987) suggests it to be "learned and shared human patterns or models for living; day-to-day living patterns". These patterns and models pervade all aspects of human social interaction. Culture is mankind's primary adaptive mechanism. The Intercultural Studies Project at the Center for Advanced Research on Language Acquisition at the University of Minnesota has defined culture as "the shared patterns of behaviors and interactions, cognitive constructs, and affective understanding that are learned through a process of socialization. These shared patterns identify the members of a culture group while also distinguishing those of another group" (CARLA, 2014). A simpler definition is "the unwritten rules of the social game" (Hofstede, 1984). In addition, according to Thomson and Von Solms (2004), "A better way to think of culture is to realize that it exists at several 'levels' and those we must understand and manage the deeper levels". And thus, to summaries; culture exists at several levels, and it is about how people perceive, think, feel about their day to day living patterns of behavior. Culture is not inherited, it can be learnt.

2.2 Organizational Culture

Research by Hofstede (1984) has found that organizational cultures distinguish different organizations within the same country or countries. Hofstede's research has shown that organizational cultures differ mainly at the level of practices (symbols, heroes and rituals). Thomson and Von Solms (2004) argued that there is a relationship that exists between the fields of corporate governance, information security and organizational culture. And thus, to summaries; the concept of organizational culture is similar to the concept of culture however it differs at the level of practices (symbols, heroes and rituals). It also refers to shared patterns in employees' behavior in firms, and to the existing relationship between organizational culture and information security. According to Schein (1999), "due to the nature of beliefs and values they cannot be measured accurately, which is why a company culture is often referred to as just the way we do things around here". Furthermore, according to Fagerstrom (2013), a widely accepted way of thinking about company culture is to look at the different levels at which it exists. These levels are; Artifacts: "Artifacts are what can be seen, heard and felt, in an organization", Espoused Values: "How the espoused values are interpreted and implemented depends heavily on the shared tacit assumptions of the employees", Shared Tacit Assumptions: "These are the beliefs, assumptions and values shared and taken for granted by the organization's employees and form the essence of that organization's culture", and Knowledge: "Employees need to have the required knowledge to perform their everyday tasks securely".

2.3 National Culture

Research by Hofstede (1984) and others has shown that national cultures differ in particular at the level of, usually unconscious, values held by a majority of the population. The Hofstede dimensions of national cultures are rooted in our unconscious values, because values are acquired in childhood, national cultures are remarkably stable over time (Hofstede, 1984). Furthermore, according to O'Brien, et al. (2013), a recent study was conducted with regards to national culture that applied Hofstede's framework; Power Distance: "A measure of the equitable distribution of power", Long-term orientation: "Degree of traditions in a specific culture and to what extent these traditions are connected to their past and future", Masculinity/Femininity: "Degree to which social roles are separated on a gender basis", Individualism: "Measure of the balance between tasks over relationships", and Uncertainty Avoidance: "Measure of degree to which cultural members are threatened by uncertain risks". Although the study discusses the important cultural differences between developing and Western countries and how these relate to information security, an area for further research would be to take the step further and investigate how different cultures relate to security compliance (O'Brien, et al., 2013). And thus; the concept of national culture is similar to the concept of culture however it differs at deeper level of unconscious values that held by majority and it affects an organization's business strategies as well as practices in the global environment.

2.4 Information Security Culture

In general and according to Roer (2014), security culture can be defined as "the ideas, customs, and social behavior of a particular people or society, that helps them being free from danger or threat". According to Ross (2011), "no security policies, standards, guidelines or procedures can foresee all of the circumstances in which they are to be interpreted". Therefore, if stakeholders are not grounded in a culture of security, there is potential for improper actions (Ross, 2011). However, according to Malcolmson (2009), "a culture of security is not an end in itself, but a pathway to achieve and maintain other objectives, such as proper use of information". Some aspects of an organization's security culture have evolved as a logical response to security threats, and are espoused by the management of the organization. These manifest themselves in the security practices and policies of the organization, the level of compliance with and understanding of those practices and policies, and the acknowledgement and awareness of security threats to the organization (Malcolmson, 2009). And thus, to summaries; the concept of security culture is similar to the concept of culture with the focus on being free from danger or threat in terms of human and improper actions, however, security culture have evolved as a logical response to security threats, and are espoused by the management of the organization.

3 Research Model Design

This paper is seen as a part of a wider research activity that aims to address security culture. Based on the results of the literature review, we therefore postulated:

- H1: Identifying factors that influence security compliance positively influences the establishment of an information security culture.
- H2: Organizational and national cultures influence the establishment of an information security culture.

3.1 Instrumentation

We used a hypothetical scenario in which items have been adopted from various peer-reviewed sources during the literature review. A main step in developing the models in our study was to make sure that these models were realistic based on the findings of the sources listed in Table 1.

Although, we listed some sources' findings without samples, here are the highlights of the other adopted samples/instruments:

Surveys. Different types of surveys that of relevance have been examined as outlined below. Some of these surveys were conducted by large security companies such as; Symantec, others were conducted by government agencies, whereas, some surveys were conducted by scholars themselves.

- According to Furnell and Clarke (2005), "the DTI Information Security Breaches Survey 2004, which found that 89 % of the teams responsible for security lacked

Table 1. Summary of current proposed variables

Variables	Source
Security compliance; *Security behavior*	Vroom and von Solms (2004)
	Herath and Rao (2009)
	Alfawaz et al. (2010)
	Greene and D'Arcy (2010)
	Gabriel and Furnell (2011)
	Padayachee (2012)
Organisational culture; *Top management support*	Ngo et al. (2005)
	Johnson and Goetz (2007)
	Ruighaver et al. (2007)
	Dojkovski et al. (2007)
Organisational culture; *Top management support & Security policy & Security acceptance & Security awareness*	Thomson and von Solms (2005)
Organizational culture; *Security acceptance*	Furnell and Thomson (2009)
Organizational culture; *Security behavior*	VanNiekerk and VonSolms (2010)
	Da Veiga and Eloff (2010)
Top management support & Security policy & Security awareness	Chipperfield and Furnell (2010)
Top management support & Security behavior	Ashenden (2008)
	Moyano et al. (2011)
Organizational & National cultures; *Security policy & Security acceptance & Security behavior*	Furnell and Rajendran (2012)
Security compliance; *Security acceptance & Security behavior*	Alfawaz et al. (2010)
Security behavior & Security policy & Security awareness	Cheng et al. (2013)
Organizational & National cultures; *Security behavior*	Connolly and Lang (2013)
Top management support & Security awareness	Furnell and Clarke (2005)
	Fagerström (2013)
Organizational culture; *Security policy & Security awareness*	O'Brien et al. (2013)
National culture; *Security behavior*	Flores et al. (2014)

security qualification”. Furnell and Clarke (2005) have concluded that an important element in establishing a culture of security is the security awareness and training that is run by teams that should have the appropriate background and skills.

- According to Chipperfield and Furnell (2010), “findings from the survey conducted by European Network and Information Security Agency suggest that only 42 % of organizations compare the level of information security awareness pre and post-programme”. Chipperfield and Furnell (2010) have concluded that the security awareness program needs to be shaped to fit individual’s roles, their level of interest.
- According to Furnell and Rajendran (2012), “UK’s biennial Information Security Breaches Survey series show a significant rise in the proportion of organizations claiming to at least have information security policies”. Furnell and Rajendran (2012)

have concluded that despite having security policies in place, there are various influence factors within and outside of an organization can have an impact upon an employee, such as; factors that influence compliance behavior.

- According to Padayachee (2012), "the global security survey found that 79 % of participants cite the human factor as the root cause for failure". Padayachee (2012) suggested that identifying and studying the factors that influence compliance behavior contributes in preventing security policy violation intentions.
- According to Connolly and Lang (2013), "recent survey shows that 39 % of security breaches happen due to user error". Connolly and Lang (2013) suggested that understanding of the various variables that influence individual security behavior can have a positive impact towards the cultivation of a security culture.
- According to Flores, et al. (2014), "Global State of Information Security Survey conducted by PWC Advisory Services & Security in 2013 found that 54 % of North American firms conduct background checks of individuals before employing them and have implemented employee security awareness training programs, while 42 % of European firms have implemented the same information security measures". Flores, et al. (2014) has concluded that the effect of behavioral security as a variable on the establishment of security culture differs between Swedish and US organization. Therefore, we argue that national culture influences the establishment of an information security culture.

Questionnaires. Four related sources have been cited as follows:

- According to Furnell and Thomson (2009), from 1007 UK businesses questioned by (Business Enterprise and Regulatory Reform), "it was revealed that 62 % believed the cause of their worst security incident had been internal rather than external". Furnell and Thomson (2009) have found that management can begin cultivating a culture of security firstly by recognizing the current levels of security acceptance.
- According to Herath and Rao (2009), "data was collected using 312 responses from 77 different organizations in Western New York". Herath and Rao (2009) have found that security behaviors can be influenced by both intrinsic and extrinsic motivators, such as; perceived contribution by individual actions and information security policy compliance intentions.
- According to Gabriel and Furnell (2011), "a group of 20 employees & managers working within the technology sector was recruited to participate in a series of security assessments & personality tests". Gabriel and Furnell (2011) suggested that personality test results may possess a predictive value for security behavior.
- Cheng, et al. (2013) presented data that was collected by using a sample of 185 usable questionnaires that were distributed to employees in 10 organizations in Dalian, China; they have found that job satisfaction and security acceptance can positively prevent employees' information security policy violation intentions. And thus, this positively influences employees' security compliance intentions. Therefore, we argue that job satisfaction and acceptance may positively influence employees' behavior toward compliance with an organization's security policies.

3.2 Scenario Design

Additionally, twenty five studies were analyzed in Table 1. However, Table 2 summarizes the candidate variables for modeling information security culture. In the following section we lay the overall framework for modeling information security culture (see Fig. 1) and hypothesize the relationship between cultures and security compliance. Based on the literature review analysis we identified five top candidate variables as follow:

Table 2. Summary of the candidate variables

Variable	No. of times cited/25	Variable ranking
Information security behavior	15	1
Top management support	10	2
Security education & awareness	6	3
Information security policy	5	4
Information security acceptance	4	5

Management. According to Thomson and Von Solms (2004), the corporate information security policy should describe the vision and goals of senior management in relation to information security. Also, Furnell and Clarke (2005) concluded that management of the organization needs to appreciate where their problems lie, and what each awareness or education option could do to help.

Information Security Policy. According to Thomson and Von Solms (2004), the corporate information security policy should describe the vision and goals of senior management in relation to information security. However and with regards to information security policy violations, Cheng, et al. (2013) concluded that the empirical results of their study suggest the importance of deterrence and social pressure factors in preventing security policy violation.

Information Security Awareness. Furnell and Clarke (2005) suggested that management of the organization needs to appreciate where their problems lie, and what each awareness or education option could do to help. Also, Chipperfield and Furnell (2010) concluded that many organizations do not naturally think to check whether awareness is getting through. However and according to Furnell and Clarke (2012), human aspects can have a significant role in ensuring the overall security of systems and data, and effort is needed to help them become part of the solution.

User Acceptance. Furnell and Thomson (2009) argued that cultivating security culture starts by recognizing the current levels of security acceptance. However, Furnell (2010) suggested that getting individual users to a point where they can accept and act upon their security responsibilities can influence the cultivation of a culture of security. However, “the fact that achieving security acceptance is a multi-stage process can of course represent a challenge in its own right” (Furnell, 2010).

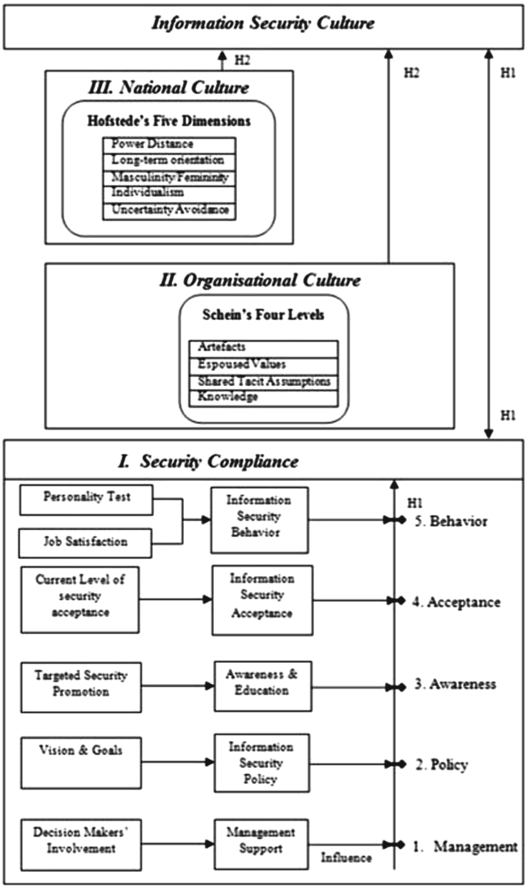

Fig. 1. A conceptual framework for modeling information security culture

Security Behavior. Alfawaz et al. (2010) developed a framework of information security practices that could contribute to information security management by identifying behaviors related to different modes of information security practice. However, Moyano, et al. (2011) developed an integrated framework with which to approach the behavioral study of threats and attacks on information and computer systems in organizations.

3.3 A Conceptual Framework for Modeling Information Security Culture

Figure 1 depicts the proposed variables and factors that influence information security culture.

The concepts are clustered into three models: National & Organizational cultures, and security compliance that form the framework. Model I consists of parent variables and its sub-variables that have been identified with regards to their role in influencing intention to comply with security policies. Model II comprises the organizational culture levels, plus the required knowledge of information security that employees need to do their job in a way that is consistent with good information security practices. Model III comprises the five dimensions that describe the cultural differences between countries that need to be taken into account when organizations operate in a global environment and how these relate to information security.

4 Discussion

We were able to identify variables that influence cultivation of a security culture, by integrating these variables into a conceptual framework that will address the research gap, this study investigated the relationship between these variables as follows:

4.1 Organizational Culture vs. Security Culture

According to Van Niekerk and Von Solms (2010), “in ‘normal’ definitions of organizational information security culture, the relevant job-related knowledge is generally ignored, because it can be assumed that the average employee would have the required knowledge to do his/her job”. In the case of information security, the required knowledge is not necessarily needed to perform the employee’s normal job functions. And thus, knowledge of information security is generally only needed when it is necessary to perform the normal job functions in a way that is consistent with good information security practices (Van Niekerk and Von Solms, 2010). Therefore, security culture should be viewed as a part of organizational culture. Also, information security culture is part of the organizational culture (Ngo, et al., 2005).

4.2 National Culture vs. Security Culture

Many researchers view a connection between national culture and employees’ as well as organizational culture in terms of compliance (Hofstede, 1984). Also, and according to Gulev (2009), “organizational cultures do emulate national culture characteristics along three finely defined dimensions: knowledge sharing, traditions, and behavior”. Flores, Antonsen and Ekstedt (2014) found that national culture should be taken into consideration in future studies in particular when investigating organizations operating in a global environment and understand how it affects behaviors and decision-making. Therefore, with regards to organizational culture vs. security culture; information security aims and objectives need to be aligned with formal organizational culture as well as national culture.

4.3 Security Compliance (Security Behavior) vs. Security Culture

Information security behavior could involve adherence to an organisation’s policies, additionally, it can evolve over time as the security culture becomes more established (Da Veiga and Eloff, 2010). Although, researchers argued that security behavior and security compliance influence the establishment of information security culture, the question is what should organizations do to influence individual behavior and improve security compliance (Fagerstrom, 2013). Therefore, this section is divided into two subsections; information security behavior and information security compliance that can be influenced by behavior as outlined below.

Security Behavior. Furnell and Thomson (2009) suggested that organizations need to recognize the level of security culture, and take steps to enhance it. Thus, there is a clear case for promoting security culture within organizations to ensure that the necessary practices become part of the natural employee behavior. For example, according to Da Veiga and Eloff (2010), "Implementing security components impact the interaction of employees with information assets, and employees consequently exhibit certain behavior referred to as security behavior. The objective is to instill security behavior that is conducive to the protection of information assets based on the organization's policies. Such behavior could involve the reporting of security incidents, or adherence to a clear desk policy. In time, this security behavior evolves as the way that things are done in the organization and security culture is therefore established".

Security Compliance. According to Cheng, et al. (2013), information security policy is a written statement that defines the requirements for the organizational security management. It is the employees' responsibility and obligations, sanctions and countermeasures for non-compliance. Even more, Vance, et al. (2012) have discussed that perceived severity positively affects employees' intention to comply with information security policies, as well as, practitioners need to ensure that employees recognize information security threats and the risks. Also, Cheng, et al. (2013) have discussed that perceived certainty of sanctions will be negatively related to employees' information security policy violation intention, as well as, the empirical results of their study suggest the importance of deterrence, social bond and social pressure factors in preventing information security policy violation (influencing compliance/security behavior). Furthermore, O'Brien, et al. (2013) has concluded that the knowledge retained within the people working for an organization are the real assets, balancing the fine line between the end user's demands and the security risks posed is where organizations should focus their efforts. However and according to Ubelacker (2013), "national culture needs to be taken into account, but it is not changeable".

5 Conclusion

In the literature, security culture has been referred to as a mean to control 'human factor' in order to enhance security compliance.

With regard to employee behavior and awareness, Furnell and Thomson (2009) proposed that organizations need to recognize the level of security culture, and take steps to enhance it. And thus, there is a clear case for promoting security culture within organizations to ensure that the necessary practices become part of the natural employee behavior. However, Furnell and Clarke (2005) concluded that security culture also implies that security issues are considered as part of organizational operations, and therefore awareness and understanding of security is fundamental to establishing a successful security culture. Furthermore, cultural change is needed in order to implement and cultivate a newly developed security culture.

This paper is considered as a contribution study to a wider research study that aims to investigate the role of culture in influencing employees' security compliance. However, there are some recognized limitations to be addressed in future research. Firstly, although adopting findings from peer-reviewed sources were used to enhance the trustworthiness of the research, the study at this stage has not used any self-collected data. A second limitation is lack of prior empirical research studies on the topic. The concept of information security culture is new. Finally, this study suggests that there is a relationship between culture's values and security compliance's factors, which raises the question of whether the proposed framework can be analyzed and tested.

Finally, researchers have argued that culture influences employees' behavior and therefore developing a culture of security can contribute in minimizing or avoiding security breaches. It has been hypothesized that cultivating security culture can have a positive effect on employees' security compliance. As such, the proposed framework that will contribute in cultivating an information security culture, along with considering national and organizational cultures as well as security compliance variables within organizations, can be adopted, studied, investigated and tested in future research. Thus, from an information security research point of view, this paper fills an important gap in the literature.

References

Alfawaz, S., Nelson, K.: Information security culture: a behaviour compliance conceptual framework. In: AISC, vol. 105 (2010)

Ashenden, D.: Information Security management: A human challenge?, Information Security Technical report, 13(4), 195–201 (2008). Accessed 16 Sep 2014

CARLA: What is Culture? University of Minnesota (2014). http://www.carla.umn.edu/culture/definitions.html. Accessed 16 Sep 2014

Cheng, L., Li, Y., Li, W., Holm, E., Zhai, Q.: Understanding the violation of IS security policy in organizations: an integrated model based on social control and deterrence theory. Comput. Secur. **2013**(39), 447–459 (2013)

Chipperfield, C., Furnell, S.: From security policy to practice: sending the right messages. Comput. Fraud Secur. **2010**(3), 13–19 (2010)

Connolly, L. Lang, M.: Information systems security: the role of cultural aspects in organisational settings. In: AIS SIGSEC pre-ICIS Workshop on Information Security and Privacy (WISP) Milan, Italy, 14 December 2013

Veiga, Da, Eloff, J.H.P.: A framework and assessment instrument for information security culture. Comput. Secur. **29**(2), 196–207 (2010)

Damen, L.: Culture Learning The Fifth Dimension on the Language Classroom. Addison-Wesley, Reading (1987). http://www.carla.umn.edu/culture/definitions.html. Accessed 22 Aug 2014

Dojkovski, S., Lichtenstein, S., Warren, M.J.: Fostering Information Security Culture in Small and Medium Size Enterprises: An Interpretive Study in Australia, pp. 1560–1571 (2007)

Fagerstrom, A.: Creating, maintaining and managing an information security culture. MSc thesis, Arcada Finland (2013)

Flores, W., Antonsen, E., Ekstedt, M.: Information security knowledge sharing in organizations: investigating the effect of behavioural information security governance and national culture. Comput. Secur. **43**, 90–110 (2014)

Furnell, S.: Jumping security hurdles. Comput. Fraud Secur. **2010**(6), 10–14 (2010)

Furnell, S., Clarke, N.: Organisational security culture: embedding security awareness, education and training. In: Proceedings of the 4th World Conference on Information Security Education (WISE 2005), Moscow, pp. 67–74 (2005)

Furnell, S., Clarke, N.: Power to the people? The evolving recognition of human aspects of security. Comput. Secur. **31**(8), 983–988 (2012)

Furnell, S., Rajendran, A.: Understanding the influences on information security behaviour. Comput. Fraud Secur. **2012**(3), 12–15 (2012)

Furnell, S., Thomson, K.L.: From culture to disobedience: Recognising the varying user acceptance of IT security. Comput. Fraud Secur. **2009**(2), 5–10 (2009)

Gabriel, T., Furnell, S.: Selecting security champions. Comput. Fraud Secur. **2011**(8), 8–12 (2011)

Greene, G., D'Arcy, J.: Assessing the impact of security culture and the employee-organization relationship in IS security compliance. In: Proceedings of the 5th Annual Symposium on Information Assurance, New York, pp. 42–49 (2010)

Gulev, R.: Are national and organizational cultures isomorphic? evidence from a four country comparative study. Managing Glob. Transitions **7**, 259–279 (2009)

Herath, T., Rao, H.R.: Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness. Decis. Support Syst. **47**(2), 154–165 (2009)

Hofstede, G.: National cultures and corporate cultures. In: Samovar, L.A., Porter, R.E. (eds.) Communication Between Cultures. Wadsworth, Belmont (1984). http://www.carla.umn.edu/culture/definitions.html. Accessed 28 Sep 14

Johnson, M.E., Goetz, E.: Embedding information security into the organization. IEEE Secur. Priv. Mag. **5**(3), 16–24 (2007)

Malcolmson, J.: What is Security Culture? Does it differ in content from general Organisational Culture? IEEE Cody Technology Park, Farnborough, Hants (2009)

Martinez-Moyano, I.J., Conrad, S.H., Andersen, D.F.: Modeling behavioral considerations related to information security. Comput. Secur. **30**(6-7), 397–409 (2011)

Ngo, L., Zhou, W., Warren, M.: Understanding transition towards information security culture change. In: Proceedings of 3rd Australian Information Security Management Conference, pp. 67–73 (2005)

O'Brien, J., Islam, S., Bao, S., Weng, F., Xiong, W., Ma, A.: Information Security Culture: Literature Review. Unpublished Working Paper, University of Melbourne (2013)

Padayachee, K.: Taxonomy of compliant information security behavior. Comput. Secur. **31**(5), 673–680 (2012)

Ponemon Institute: 2013 Cost of Data Breach Study: Global Analysis. Symantec (2013). https://www4.symantec.com/mktginfo/whitepaper/053013_GL_NA_WP_Ponemon-2013-Cost-of-a-Data-Breach-Report_daiNA_cta72382.pdf. Accessed 28 Sep 14

Roer, K.: How to build and maintain security culture (2014). http://roer.com/2014/04/08/build-maintain-security-culture/. Accessed 19 Sep 2014

Ross, S.J.: Creating a Culture of Security. In: ISACA (2011). http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Creating-a-Culture-of-Security.aspx. Accessed 19 Sep 2014

Ruighaver, A.B., Maynard, S.B., Chang, S.: Organisational security culture: extending the end-user perspective. Comput. Secur. **26**(1), 56–62 (2007)

Thomson, K.-L., von Solms, R.: Information security obedience: a definition. Comput. Secur. **24** (1), 69–75 (2004)

Schein, E.: The Corporate Culture Survival Guide. Jossey-Bass Inc, San Francisco (1999)

Übelacker, S.: Security-aware organisational cultures a starting point for mitigating socio-technical risks socio-technical risk management/motivation. In: RiskKom Workshop INFORMATIK 2013, Koblenz, Germany (2013)

Van Niekerk, J.F., Von Solms, R.: Information security culture: A management perspective. Comput. Secur. **29**(4), 476–486 (2010)

Vance, A., Siponen, M., Pahnila, S.: Motivating IS security compliance: insights from habit and protection motivation theory. Inf. Manag. **49**, 190–198 (2012)