UNIVERSITY OF TECHNOLOGY SYDNEY

UTS:

School of Management

Working Paper Series

http://www.business.uts.edu.au/management/index.htm

Investigating the Concept of Information Security Culture

Daniel Oost and Eng Chew

2007

Working Paper No: 2007/6

Investigating the Concept of Information Security Culture

Daniel Oost[a] and Eng Chew[b]

[a]School of Management, University of Technology, Sydney, Australia.

[b]Faculty of Information Technology, University of Technology, Sydney, Australia.

Abstract

The concept of an 'information security culture' is relatively new. A review of published research on the topic suggests that it is not the information security panacea that has been suggested. Instead it tends to refer to a range of existing techniques for addressing the human aspect of information security, oversimplifying the link between culture and behaviour, exaggerating the ease with which a culture can be adjusted, and treating culture as a monolith, set from the top. Evidence for some of the claims is also lacking. The paper finds that the term 'information security culture' is ambiguous and vague enough to suggest the possibility of achieving an almost mystical state whereby behaviour consistent with information security is second nature to all employees, but when probed does not deliver. Instead, future research should be clear about what it considers information security culture to be, should provide evidence for claims, and should take complexity and context seriously.

Key Words: information security culture, organizational culture, phronesis

Correspondence To:

Daniel Oost. School of Management. University of Technology, Sydney, NSW, Australia.

Email Address: daniel.oost@gmail.com

Introduction

Information security culture has been defined in different ways. Some authors see an information security culture as a goal to be achieved. For example, von Solms (2000) calls for the creation of a culture of information security within organizations, "by instilling the aspects of information security to every employee as a natural way of performing his or her daily job" (p. 618). Similarly, Schlienger and Teufel (2002) suggest that "Security culture should support all activities in a way, that information security becomes a natural aspect in the daily activities of every employee" (p. 7). Other researchers with definitions along these lines include Vroom and von Solms (2004) and Thomson et al (2006). In contrast, Ngo et al (2005) allow for information security culture to refer to "how things are done (i.e. accepted behaviour and actions) by employees and the organisation as a whole, in relation to information security" (p. 68), not just a situation where behaviour is 'naturally' consistent with information security principles.

For Martins and Eloff (2002) an information security culture emerges from employee behaviour in relation to information security, which over time ends up being equated with the 'ways things are done around here'. May (2003) equates an information security culture with internal acceptance of the idea that information security is vital for a successful business. Knapp et al (2006) build a security culture construct based on the extent to which employees value the importance of security, how the culture promotes good security practices, whether security has traditionally been considered an important organizational value that fosters security-minded thinking, and whether practicing good security is the accepted way of doing business and a key norm shared by organizational members

As Ruighaver et al (2007) point out some authors' use the term 'information security culture' without clarifying exactly what they mean by it. Despite this criticism Ruighaver et al do not go on to provide a definition. Instead, they declare that the concept of a security culture is too complex to be explained by a single framework, and hence are hesitant to even define it. In place of such a definition, Ruighaver et al recommend the use of Detert et al's (2000) organizational culture framework for studying an organization's security culture. This framework was developed as a synthesis of different organizational culture research, and consists of eight dimensions of organizational culture: 1) the basis of truth and rationality, 2) the nature of time and time horizon, 3) motivation, 4) stability versus change/innovation/personal growth, 5) orientation to work, task, co-workers, 6) isolation versus collaboration/cooperation, 7) control, coordination and responsibility, and 8) orientation and focus – internal and/or external.

The use of Detert et al's framework as a theoretical resource by Ruighaver et al (and Chia et al 2002) is a deviation from the more frequent reference to Edgar Schein's work on organizational culture (e.g. Schein, 1992) by information security culture researchers (e.g. Schlienger and Teufel 2002, 2003a, 2003b; Thomson et al 2006; Thomson and von Solms 2005; Vroom and von Solms 2004; Zakaria 2004). These researchers relate elements of information security culture to Schein's distinction between three aspects of organizational culture: 'artefacts and creations', 'collective values, norms and knowledge', and 'basic assumptions and beliefs'. Each of these aspects is seen as being interrelated with the next, and increasingly difficult for a researcher to access.

The variety of opinions on what defines information security culture, reference to the concept without explaining what is meant by it and the different theoretical resources authors draw upon to investigate it, creates some confusion when trying to review research on the concept. The variety of approaches is not a problem in of itself, as it may well lead to new insights that a single unified way of looking at the concept could not do, but it does leave the question of what is being addressed somewhat in abeyance. In this context, this paper outlines and critiques published research on the relatively new concept of an 'information security culture'. Specifically, it suggests that rather than providing new avenues to address the human aspect of information security, the research tends to refer to a range of existing techniques, oversimplifies the link between culture and behaviour, and exaggerates the ease with which a culture may be adjusted. Further, evidence for the claims made by the authors is frequently lacking. The paper concludes by highlighting the importance of taking context into account in researching information security culture, and points to how a *phronetic* approach to research might one way to do this.

What does information security culture add to the understanding of information security?

Despite information security culture researchers attempting to approach information security problems from new angles, informed by theorists such as Schein and Detert et al, it is questionable whether their suggestions are new or distinctly 'cultural'. Indeed, the normative responses to information security culture needs reflect a range of actions that relate to well established and conventional managerial practices. In some cases the response is to implement new policies. For example in the form of information security management standards (e.g. May 2003) or policies and procedures on how to act securely (Thomson et al 2006; Thomson and von Solms 2005; von Solms and von Solms 2004). Researchers have also promoted particular human resource management solutions, whether they be the provision of education/training on how to behave securely (e.g. Leach 2003; Lewandowski 2005; Schlienger and Teufel 2002; Thomson et al 2006; von Solms and von Solms 2004) or the screening of potential employees (Kuusisto et al 2004; Schlienger and Teufel 2002). Other 'solutions' have included 'motivating' employees to encourage them to behave in a secure way (Leach 2003; Schlienger and Teufel 2002) and emphasising the importance of top management support for information security practices (e.g. Dutta and McCrohan 2002; Knapp et al 2006; Kuusisto 2004; Leach 2003; May 2003; Thomson et al 2006; Thomson and von Solms 2005; von Solms and von Solms 2004). While the actions listed above may well prove to be beneficial to organizations that carry them out, what is questionable is whether it is useful or appropriate to label them as constitutive of a new information security culture project.

The simplicity and lack of innovation inherent in the information security culture approach is exemplified by Schlienger and Teufel's (2003b) statement that "[o]n the basis of internal communication, training, education and exemplary acting of managers, a culture can be developed step by step" (p. 8). The recommended elements – communication, training, education, management support have been associated with good information security practices, long before the notion of 'culture' was mobilized. It is difficult to see what is distinct about the notion of an information security culture from Siponen's (2000) definition of security awareness. Siponen defines this as "a state where users in an organization are aware of – ideally committed to – their security mission (often expressed in end-user security guidelines)" (p. 31). If we compare this with, for example, Thomson et al's (2006) discussion on the cultivation of an organizational information security culture whereby "employees learn about, and integrate, acceptable information security skills into their daily behaviour" (p. 7), the differences are far from significant. Security culture in these terms looks very much like the established notion of information security awareness. Indeed, it is telling that Dhillon (1999) can write about the management and control of computer misuse without invoking the term 'information security culture'. Similarly Nosworthy (2000) suggests a range of ways to "educate the people of the organization to successfully implement the requirements of the information security policy" (p. 337) without mentioning the need for an information security culture. Another example is Trompeter and Eloff's (2001) paper on 'socio-ethical controls' in information security which is also without reference to culture.

To make a case for the distinctiveness of the information security culture approach is particularly difficult if you consider that, as noted above, Ruighaver et al (2007) reviewed the literature on the topic, yet hesitated to provide a definition of a security culture. This is not to claim that all the suggestions by information security culture researchers can be easily folded into prior research on good information security practices, but rather than the notion of culture is not itself the source of distinction or contribution in thinking about information security. This literature on information security culture can thus be best regarded as having made some contribution to understanding how to promote information security; it is just that this contribution is not particularly cultural in character. Key contributions here include:

- Koh et al's (2005) recommendation for the formalisation of social participation activities in relation to security governance – an increase in a sense of responsibility and ownership of security issues by security personnel should result
- Kuusistio's (2004) suggestion that a unified image of how security should be conducted and thought about must be communicated to customers and other organisations
- Leach's (2003) promotion of the creation of a strong psychological contract with the employer
- Schlienger and Teufel's (2002) suggestion to involve the users in security decisions, with the how's and why's to be explained
- von Solms' (2000) call for changing of awareness programs into "continuous corporate information security plans, starting from the moment an employee is taken on board" (p. 618)

Despite these suggestions not being easy to pigeon hole into existing information security research topics, they do not they appear to cohere as distinctly 'cultural'. Even if an argument were made for their unity, the question remains as to what the cultural label adds to the understanding of information security problems, over and above the long recognised 'human factor'. The creation of a new term for an existing problem area does nothing to advance understanding of the existing area, and could potentially create confusion and divide efforts.

An oversimplified link between culture and behaviour

One effect of referring to an information security culture is to give the impression that if you know an organization's security culture you will know how its members will behave in relation to security issues. However, the idea that organizational culture should only be conceptualised as something so uniform and deterministic has been criticised by organization studies researchers.

Martin (2002) distinguishes three perspectives on organizational culture. The first is the integration perspective. This perspective

> focuses on those manifestations of a culture that have mutually consistent interpretations. An integration portrait of a culture sees consensus (although not necessarily unanimity) throughout an organization. From the integration perspective, culture is like a solid monolith that is seen the same way by most people, no matter which angle they view it (p. 94).

Second, the differentiation perspective

> focuses on cultural manifestations that have inconsistent interpretations, such as when top executives announce a policy and then behave in a policy-inconsistent manner. From the differentiation perspective, consensus exists within an organization – but only at lower levels of analysis, labelled "subcultures." Subcultures may exist in harmony, independently, or in conflict with each other. Within a subculture all is clear; ambiguity is banished to the interstices between subcultures (p. 94).

Third, the fragmentation perspective

> conceptualises the relationship among cultural manifestations as neither clearly consistent nor clearly inconsistent. Instead, interpretations of cultural manifestations are ambiguously related to each other, placing ambiguity, rather than clarity, at the core of culture. In the fragmentation view, consensus is transient and issue specific (p. 94).

Martin advocates examining all of the perspectives in a single study in order to gain a fuller understanding of the complexities involved in studying organizational culture. Despite this, the literature on information security culture is dominated by the integration perspective. Following Martin, this suggests not only that the information security culture literature is lacking in distinctiveness, but also that it is blinded to the possibility of differences and ambiguities that are inherent in cultural phenomena.

Suggestive of a bias towards avoiding ambiguity, the assumption that an employee only belongs to one culture has been highlighted by Straub et al (2002). However, some information security culture researchers highlight the possibility of multiple cultures existing within one organization (e.g. Helokunnas and Kuusisto 2003; Kuusito 2004). Acknowledgement of this complexity suggests a more realistic treatment of the possibility (or otherwise) of creating an information security culture. There is still, however, the danger recently highlighted by Leidner and Kayworth (2006):

> the assumption that all individuals within a given cultural unit will respond in a consistent fashion based on the group's cultural values. The potential problem with this view is it does not take into account the possibility for individual differences within the particular cultural unit that may lead to different behavioural outcomes (p. 381)

An example of this assumption is Thomson and von Solms (2005) statement that:

> Since, the corporate culture of an organisation determines the behaviour of employees in an organisation; it should be used to influence these behaviour patterns of employees towards the protection of information as envisioned by the Board of Directors (p. 72)

The possibility that an organization has a variety of subcultures that do not share the same view of information security, and that even within these culturally consistent groups some individuals may respond differently to the same stimulus seems lost in this simplistic view whereby culture determines behaviour. Culture trumping individual agency is a peculiar conceptual problem within a discipline that deals with the problem of the 'insider', the disgruntled or devious employee who takes advantage of their position to break the rules, who surely epitomises the exercise of agency in the face of structures set to limit it. Creating awareness of information security policies is one thing, consistently determining what an employee will do with this awareness seems quite another. Even if a consistent organization-wide set of responses to stimuli that related to information security (potentially a wide range of stimuli) could be instituted, this also raises the question of what happens to employees' innovative and creative instincts which by definition transcend existing rules. Perhaps information security research that considers consistent responses to stimuli should be confined to that which deals with hard measures that leave little room for the exercise of agency. For example, more than merely a desire to break policy is required to decrypt a file without the required credentials.

Ease with which to change a culture exaggerated

Another implication of the current literature on information security culture is that it gives the impression that culture is a variable that can be adjusted by management, which will in turn lead to a consistent and uniform change in employee behaviour that reflects organizational security policy. As an example, Ernst & Young's 2004 Global Information Security Survey contains statements that reflect this sentiment: "We expect that incidents – particularly internal ones – will proliferate unless senior management makes information security a core management and governance function – a cultural imperative" (p. 3). This assumption of the cultural potency of senior managers continues throughout the report: "There is no factor more influential than senior management setting the tone that information security is important and that individuals – including senior and middle management – will be held accountable for their actions" (p. 6). The received wisdom is that senior management "must lead the charge in creating a security-conscious culture based on individual awareness and personal accountability for conduct" (p. 7).

Whilst Ernst and Young's report can be expected to appeal to the perceived needs and axieties of their managerial clients, information security culture researchers have drawn similar conclusions. For example, Ruighaver et al's (2007) comment that "[i]nformation security is, in general, a management problem and the security culture reflects how management handles this problem" (p. 56). von Solms and von Solms (2004) provide another example when they claim:

> if management wants their employees to act in a specific way that is beneficial to the organization, they need to dictate the behaviour of the employees. This can be done by expressing collective values, norms and knowledge, through defining specific policies and procedures. These policies and procedures should reflect the underlying assumptions and beliefs of management (p. 277)

Perhaps the best example of an information security researcher suggesting security culture can be adjusted by management is provided by Leach (2003) when he writes that: "It is a simple matter of leadership. Strong leadership creates a strong culture, and a strong culture gives clear direction to staff at all levels" (p. 692)

These statements are reminiscent of the over-simplified promises that some organizational researchers started offering in the 1980s. As Martin (2002) critiques:

> Organizations could supposedly develop 'strong' cultures, becoming havens of harmony in which employees shared their leader's beliefs, assumptions, and vision for the company […] It offered a leader-focused way to achieve agreement, on issues where it mattered most, in organizational domains that seemed riddled with misunderstanding, confusion, unspoken dissent, and sometimes, overt conflict (p. 8)

Martin describes this as a Lazarus of an idea that is periodically resurrected, despite its oversimplified and managerial fad nature, the lack of evidence for some claims, and the financial woes that beset the companies initially held up as exemplars of strong culture success. Complexity and ambiguity are ignored in favour of the integrative view of culture, as discussed in the previous section. This is not to suggest that management does not have an important part to play in influencing the behaviour of employees, but rather that is problematic that management can 'control' culture unilaterally. Indeed Knapp et al (2006) have found survey based evidence for their impact on 'security culture' (as they construct it). What is warranted, however, is caution when deciding whether to accept statements that propose that an information security culture is a 'simple matter of leadership' (e.g Leech, 2003). If there is a safe assumption, it is that culture is not simple.

The need for caution is also pertinent in the face of research by Leidner and Kayworth (2006) which found that: "the overwhelming focus in both national and organizational culture IS research has been to treat culture as being stable, persistent, and difficult to change" (p. 370). Indeed, several information security publications have given primacy to existing organizational culture by suggesting security policies be adapted to suit it. For example, Dhillon (1999) writes: "Since the security policy of an enterprise largely depends on the prevalent organizational culture, the choice of individual elements is case specific" (p. 174). Another example is contained within ISO 17799, a de jure information security management standard (Backhouse et al 2006). This standard refers to "an approach and framework to implementing, maintaining, monitoring, and improving information security that is consistent with the organizational culture" (p. ix) as a critical success factor. Some further examples include: Nosworthy's (2000) claim that culture can determine what is practical or otherwise to implement in terms of information security policy, Siponen's (2000) suggestion that creating information security awareness (arguably security culture related) is dependent on the organization in question, and requires an understanding of its culture, and

Spurling's (1995) description of the need for computer security awareness and commitment efforts to suit the culture of his organization

If organizational culture is typically difficult to change and not as monolithic as some researchers assume, then suggestions on how to go about building a security culture should be quite nuanced and complex. Despite this, researchers continue to claim that cultural management is quite simple. For example May (2003) suggests that "[i]f security is gradually incorporated into the daily processes and procedures it becomes part of the culture of the business and not an expensive overhead" (p. 12) and, as referred to previously, Schlienger and Teufel (2003b) suggest that "[o]n the basis of internal communication, training, education and exemplary acting of managers, a culture can be developed step by step" (p. 8). An extreme example of this tendency can be found in Vroom and Von Solms' (2004) claim that:

> [O]rganizational culture can be changed. Firstly, organizational behaviour is used to change the shared values and knowledge of the group. Once group behaviour begins to alter, it would influence the individual employees and likewise have an eventual effect on the formal organization. The artifacts of the organization would reflect these changes that have been put in place. Slowly but surely, by changing one aspect, it will filter through the organization at a formal and individual level and the culture will eventually change into a more secure one (p. 197)

Note that 'organizational behaviour' is the key to changing organizational culture according to Vroom and Von Solms, yet what they mean by either term is unclear, hence any potential complexity is glossed over. The examples of information security researchers suggesting that information security culture is a variable to be tweaked by top management given previously are similarly simplistic. When compexities are acknowledged, it is commonly in respect to the length of time that cultural change can be expected to take. For example, Kuusito et al (2004) note that even if organisational members share the same values it could take a few years to form a united security culture. Ngo et al (2005) look closer at the change process, suggesting that beyond establishing, fostering and managing information security culture there is also a need to understand the transition process.

It is also worth commenting that given the days of lifelong employment at a single organization are over for most people, the time organisations have to impose a culture has been reduced. As Dhillon (1999) discussed: "Traditionally, employees of a particular concern had strong ties with the principle concern employing them, as opposed to today where employees may have strong ties with other outside organizations and businesses" (p. 173). Both of these factors suggest increased difficulty involved in security culture indoctrination.

Given the difficulties discussed above, empirical evidence for how to create or modify an information security culture is particularly needed. However, empirical evidence within information security culture papers tends to be limited to small case studies of existing information security cultures (e.g. Chia et al 2002; Koh et al 2005; Kuusisto et al 2004; Schlienger and Teufel 2003a, 2003b, 2003c; Zakaria 2004; Zakaria 2006), often published as conference papers. Put simply, the existing literature does not provide evidence for declarations on how a security culture might be transformed into one where all employees share information security awareness as second nature in their daily activities. Despite this, as noted above, the possibility of an ideal information security culture is claimed or implied, and in some cases instructions for how to go about obtaining one are given. Empirical evidence for information security related research in general is limited, in part due to the sensitivities involved (Kotulic and Clark 2004). Given this, making the case for information security culture research as a unique niche splits an already small pie of empirical research. Justification for this split needs to be provided, above and beyond the current state of information security culture research.

The need for context to be taken seriously

In this paper, we have argued that the current literature on information security culture is limited by its lack of conceptual clarity, its lack of unique contribution, and its assumption that cultural change is simple and programmatic. What this calls for is a more complex, empirically informed and nuanced understanding of how culture is actually practiced in relation to information security. Following Flyvbjerg (2001), one methodological direction that can be pursued in order to remedy this situation is to study information security culture in relation to phronesis – that is the 'practical wisdom' that informs people's actions and behaviour.

For Flyvberg, studying objects which are also subjects (i.e. self reflexive people) will never result in the types of context-independent predictive theory currently favoured in information security culture research. Aiming for such theories is ultimately a fruitless exercise due to the contingent nature of social circumstance – it is always dependent upon context. Nevertheless, research on information security culture tends not to take context into account, particularly those that come to definitive conclusions without reference to empirical evidence. The search for a general theory of information security culture – how to consistently predict information security related behaviour, and how to tweak this determining force to suit the needs of management no matter the situation – is hoping for a lot, particularly given that others' attempting similar general theories over time have persistently failed. As an alternative Flyvbjerg develops Aristotle's concept of *phronesis* as an appropriate approach for the social sciences, given their inability to successfully produce cumulative predictive theory, in contrast to the physical sciences. The development of the concept has been recognized as a legitimate approach to academic research (see Greenwood and Levin 2005).

To understands what we mean by phronesis, it needs to be considered in relation to what Aristotle identified as the intellectual virtues: *episteme*, *techne,* and *phronesis*. *Episteme* is equated with scientific knowledge, and *techne* is considered technical know-how, and phronesis with practical widom. Flyvbjerg suggests that the study of people should aim for *phronesis*, a virtue equated with commonsense, or prudence. Flyvbjerg defines Aristotle's three intellectual virtues as follows:

> *Episteme* Scientific knowledge. Universal, invariable, context-independent. Based on general analytical rationality. The original concept is known today from the terms "epistemology" and "epistemic."
>
> *Techne* Craft/art. Pragmatic, variable, context-dependent. Oriented towards production. Based on practical instrumental rationality governed by a conscious goal. The original concept appears today in terms such as "technique," "technical," and "technology."
>
> *Phronesis* Ethics. Deliberation about values with reference to praxis. Pragmatic, variable, context-dependent. Oriented toward action. Based on practical value-rationality. The original concept has no analogous contemporary term. (p. 57).

The epistemological status of the answers provided by *phronetic* research is purposefully context-dependent. Context-dependent does not mean relativistic or nihilistic. Flyvbjerg suggests that the main objective of such research is to "produce input for ongoing social dialogue and social praxis rather than definitive, empirically verifiable knowledge, even though rigorous empirical study and verification of data are central" (p. 115). Confirmation, revision and rejection of such research is still very much possible; one interpretation is not just as good as any other – validity still needs to be established and defended. Challenges to an interpretation must seek to provide a *better* explanation:

> If a better interpretation demonstrates the previous interpretation to be "merely interpretation", this new interpretation remains valid until another,

> still better interpretation is produced which can reduce the previous interpretation to "merely" interpretation (p. 131).

In phronesis based research, rules for identifying the "ultimate" or "final" interpretation based on fundamental values and facts do not yet exist, and this will likely remain the case – rules must be interpreted by subjects, they cannot provide for their own (single) interpretation (Clegg 1989). In the absence of such rules, the process described above of interpretations competing on the basis of testable validity claims is the only basis for discriminating between interpretations. The goal of phronetic research is "to produce input into the ongoing social dialogue and praxis in a society, rather than to generate ultimate, unequivocally verified knowledge" (p. 139). Perhaps a phronetic approach to the study of information security culture (or 'awareness', or 'the human problem of information security', or however it happens specifically to be defined), closely tied to detailed empirical evidence and context, will result in more fruitful research on the topic.

Conclusion

In our review of the literature we have found that the term 'information security culture' is ambiguously defined. Despite this, such research offers the exaggerated promises that culture is a means of predicting security related behaviour, which can be unproblematically adjusted to suit the needs of management. Perhaps this ambiguity concerning what an 'information security culture' is allows it to promise so much, given that the mechanisms by which such promises might be delivered are not clear. Indeed, as this review has shown, in many cases it is difficult to distinguish what is new about the term at all. On the basis of such limitations, we propose that future research needs to be clear about what it considers information security culture to refer to, and how this is distinct from or additional to existing research on the human factor of information security, often couched in terms of 'security awareness'. If the research is closely tied to empirical research, this may avoid researchers treating the concept in an ambiguous way. As a means of addressing this, we have suggested that it might help researchers to take context and complexity into account and that the *phronetic* approach to research as explained by Flyvbjerg (2001) may result in more useful (yet less arrogant and sanguine) outcomes.

Martin's (2002) warning seems apt:

> An oversimplified theory, however comforting and appealing, is not likely to be useful if it ignores important complexities in the world it attempts, imperfectly, to represent. Application of an oversimplified theory is not only a potential waste of organizational resources; it can also undermine society's shaky commitments to the academic enterprises of education and research (p. 9)

Presenting practitioners, who are faced with a complex context dependent reality every day, with a simplistic information security culture theory does not serve anyone's purposes: the theory will not deliver results, and the esteem with which researchers are held will suffer.

References

Backhouse J, Hsu CW, Silva L. Circuits of power in creating *de jure* standards: shaping an international information systems security standard. MIS Quarterly 2006;30:413-38.

Chia PA, Maynard SB, Ruighaver AB. Understanding Organizational Security Culture. In: Hunter MG, Dhanda KK, editors. Information systems: the challenges of theory and practice. Las Vegas, USA: Information Institute; 2003. p. 335-65.

Clegg SR. Frameworks of Power. London: Sage; 1989.

Detert J, Schroeder R, Mauriel J. A framework for linking culture and improvement initiatives in organisations. The Academy of Management Review 2000;25(4):850-63.

Dhillon G. Managing and controlling computer misuse. Information Management and Computer Security 1999;7(4):171-5.

Dutta A, McCrohan K. Management's role in information security in a cyber economy. California Management Review 2002;45(1):67-87.

Flyvbjerg B. Making social science matter: why social inquiry fails and how it can count again. Cambridge: Cambridge University Press; 2001.

Greenwood DJ, Levin M. Reform of the social sciences and of universities through action research. In N. K. Denzin NK, & Y. S. Lincoln YS, editors. Handbook of qualitative research, 3rd ed. London: Sage; 2005. p. 43-64.

Global information security survey. Ernst & Young LLP; 2004.

Helokunnas T, Kuusisto R. Information security culture in a value net. In Proceedings of the International Engineering Management Conference, New York, USA; November 2003.

ISO/IEC 17799, 2005. Information technology – Security techniques –

Code of practice for information security management.

Knapp KJ, Marshall TE, Rainer RK, Ford FN. Information security: management's effect on culture and policy. Information Management and Computer Security 2006;14(1):24-36.

Koh K, Ruighaver AB, Maynard SB, Ahmad A. Security governance: Its impact on security culture. In: Proceedings of the third Australian information security management conference, Perth, Australia; September 2005.

Kotulic AG, Clark JG. Why there aren't more information security research studies. Information and Management 2004;41(5):597-607.

Kuusisto R, Nyberg K, Virtanen T. Unite security culture: May a unified security culture be plausible? In: Proceedings of the 3rd European conference on information warfare and security, London, United Kingdom; 2004.

Leach J. Improving user security behaviour. Computers and Security 2003;22(8):685-92.

Leidner D, Kayworth T. A review of culture in information systems research: toward a theory of information technology culture conflict. MIS Quarterly 2006;30(2):357-99.

Lewandowski, JO. Creating a culture of technical caution: Addressing the issues of security, privacy protection and the ethical use of technology. In: Proceedings of the 33rd annual ACM SIGUCCS conference on user services, Monterey, USA; 2005.

Martin J. Organizational culture: mapping the terrain. London: Sage; 2002.

Martins A, Eloff, J. Information security culture. In: IFIP TC11 international conference on information security, Cairo, Egypt; 7-9 May 2002.

May C. Dynamic corporate culture lies at the heart of effective security strategy. Computer Fraud and Security 2003;(5):10-13.

Ngo L, Zhou W, Warren M. Understanding transition towards information security culture change. In: Proceedings of the third Australian information security management conference, Perth, Australia; 30 September 2005.

Nosworthy JD. Implementing information security in the 21st century – do you have the balancing factors? Computers and Security 2000;19(4):337-47.

Ruighaver AB, Maynard SB, Chang S. Organisational security culture: Extending the end-user perspective. Computers and Security 2007;26(1):56-62.

Schein E. Organisational culture and leadership. 2nd ed. San Francisco: Jossey-Bass; 1992.

Schlienger T, Teufel S. Analyzing information security culture: increased trust by an appropriate information security culture. In: 14th International workshop on database and expert systems applications (DEXA'03), Prague, Czech Republic; 2003a.

Schlienger T, Teufel S. Information security culture – from analysis to change. In: Proceedings of the 3rd Annual Information Security South Africa Conference (ISSA 2003), Johannesburg, South Africa; 9-11 July 2003b.

Schlienger T, Teufel S. Information security culture – the socio-cultural dimension in information security management. In: IFIP TC11 international conference on information security, Cairo, Egypt; 7-9 May 2002.

Siponen, MT. A conceptual foundation for organizational information security awareness. Information Management and Computer Security 2000;8(1):31-41.

Spurling P. Promoting security awareness and commitment. Information Management and Computer Security 1995;3(2):20-6.

Straub D, Loch K, Evaristo R, Karahanna E, Strite M. Toward a theory-based measurement of culture. Journal of Global Information Management 2002;10(1):13-23.

Thomson K, Von Solms R. Information security obedience: a definition. Computers and Security 2005;24(1):69-75.

Thomson K, Von Solms R, Louw, L. Cultivating an organizational information security culture. Computer Fraud and Security 2006;(10):7-11.

Trompeter CM, Eloff JHP. A framework for the implementation of socio-ethical controls in information security. Computers and Security 2001;20(5):384-91.

Von Solms B. Information security – the third wave? Computers and Security 2000;19(7):615-20.

Von Solms R, Von Solms B. From policies to culture. Computers and Security 2004;23(4):275-79.

Vroom C, Von Solms R. Towards information security behavioural compliance. Computers and Security 2004;23(3):191-198.

Zakaria O. Internalisation of information security culture amongst employees through basic security knowledge. In: IFIP TC11 international conference on information security, Karlstad, Sweden; 22-24 May 2006.

Zakaria O. Understanding challenges of information security culture: a methodological issue. In: Proceedings of the second Australian information security management conference, Perth, Australia; 26 November 2004.