2009

What Does Security Culture Look Like For Small Organizations?

Patricia A. Williams
Edith Cowan University

DOI: 10.4225/75/57b4029530dea
Originally published in the Proceedings of the 7th Australian Information Security Management Conference, Perth, Western Australia, 1st to 3rd December 2009

What Does Security Culture Look Like For Small Organizations?

Patricia A H Williams
secau - Security Research Centre
School of Computer and Security Science
Edith Cowan University

Abstract

The human component is a significant factor in information security, with a large numbers of breaches occurring due to unintentional user error. Technical solutions can only protect information so far and thus the human aspect of security has become a major focus for discussion. Therefore, it is important for organisations to create a security conscious culture. However, currently there is no established representation of security culture from which to assess how it can be manoeuvred to improve the overall information security of an organization. This is of particular importance for small organizations who lack the resources in information security and for whom the culture of the organization exerts a strong influence. A review of multiple definitions and descriptions of security culture was made to assess and analyse the drivers and influences that exist for security culture in small organizations. An initial representation of the factors that should drive security culture, together with those that should only influence it, was constructed. At a fundamental level these drivers are related to a formulated response to security issues rather than a reaction to it, and should reflect the responsibility allocated in a secure environment. In contrast, the influences on security culture can be grouped by communities of practice, individual awareness and organizational management. The encapsulation of potential driving and influencing factors couched in information security terms rather than behavioural science terms, will allow security researchers to investigate how a security culture can be fostered to improve information security in small organizations.

Keywords

Culture, security culture, information security, behaviour, communities of practice

INTRODUCTION

The need for sophisticated attack mechanisms on information is circumvented by poor and ineffective security procedures. Regrettably, the practice of good information security procedures has not kept pace with the rapid development of technological security solutions (McIlwriath, 2006). It is equally unfortunate that an organization's biggest threat to privacy and security are their own staff (Anonymous, 2009; BBC News, 2008; Doherty & Fulford, 2005). The convergence of technology and the proliferation of computing networks mean that computer technologies have become ubiquitous to our work and private life. Consequently, it has been recognized at a national and international level as important to include the behaviour of people, in addition to the sound secure design of information systems and networks, to implement effective security solutions. The behaviour of people is influenced by the culture in which they function.

A culture is defined as shared values, goals and behaviours of a community or group (Allen, 2005). In the use and application of technology culture is a frequently overlooked component of success and failure (Hoffman & Klepper, 2000). Achieving a culture of security will not occur unless people (as the operational level of security and thus the human factor in the equation) can be convinced of its importance to their daily work and private life. In reality this means that all individuals must play a role in the security of their environment as contributors to and participators in the information society. Responsibility lay with each employee to be aware of the security risks that exist in their workplace and the appropriate measures that should be taken. This has become a focus at a national and international level with governments round the world recognizing and promoting its importance by developing their own initiatives (O.E.C.D., n.d.-b). For instance, in Australia a High Tech Crime Centre was established in 2003 to address the issues of cross-jurisdiction cyber crime and the government published a paper on the implementation of a security culture in Australia advocating an inclusive view of security and e-security with particular reference to critical infrastructure protection. Whilst this is important from a national perspective as advisory groups and a focus on defining Australia's national security policy was prompted, it does little to address the integration of a culture of security at the commercial and employee level. "Security must become an integral part of the daily routine of individuals, businesses and governments in their use of ICTs and conduct of online activities" (O.E.C.D., n.d.-a). Whilst government sites such as Stay Smart Online aim to educate small business in Australia, they focus on simple activities to protect online communications only (Australian Government, 2009). What is lacking is the promotion of an overall culture of security.

Undoubtedly as initiatives in the interconnection of information sources such as e-health become commonplace, a wider national and international view of security is required. Yet, there exists a disconnection between large scale initiatives and smaller organizations. Small organizations often assume that security is not an issue for them. One area of small

business that highlights this issue is in primary health care. In Australian and UK primary care medical practices there is a significance influence of trust and ethics on workflow and thus security is not seen as a significant issue (Williams, 2008). Ironically, it is more important for smaller organizations as staff often have multiple roles and thus access to a variety of financial, organizational, customer, and employee information as well access to multiple services such as the internet and email. Further, in small organizations there is less segregation of duties and thus less control over access to information. Whilst being exposed to the same threats and vulnerabilities as large organisations they do not have access to the same level of resources.

Investigation into security culture is relatively new, whilst some researchers have proposed models for assessing the quality of a security culture based on organizational culture theory, it is difficult to assess when there is no cohesive definition of what it comprises (Ruighaver, Maynard, & Chang, 2007). As Tsohou, Kokolakis, Kardya and Kiountouzis (2008) suggest there are gaps in research into security awareness and its place in security culture. This research is defining this place and considering it as a key element in the definition of security culture. Hence, this paper reviews the definitions of security culture and synthesizes these into an initial picture of what factors should drive a security culture and in contrast, what factors should only influence it.

WHAT IS A SECURITY CULTURE?

There are many definitions of security culture. Security culture

- "exists when every participant in the information society, appropriately to their role, is aware of the relevant security risks and preventative measures, assumes responsibility and takes steps to improve the security of their information systems and networks" (Business and Advisory Committee to the (OECD, 2004).
- is "where the people know their rights and assert them in all situations. Those who belong to a security culture also know what behaviour compromises security and are quick to work with people who exhibit insecure or oppressive behaviour" (security.tao.ca, n.d.);
- Security culture encompasses all socio-cultural measures that support technical security measures, so that information security becomes a natural aspect in the daily activities of every employee (Schlienger & Teufel, 2003).

Expanding on these definitions researchers have identified various components of security culture and associated contextual factors:

- Thompson, vol Solms and Louw (2006) suggest that a security culture is closely associated with organizational culture. As such, training is of paramount importance to ensure staff increase their awareness of security issues and their competence to deal with them. Socialization of the community is also an important factor, as is commitment to one another's learning;
- Sasse, Brostoff and Weirich (2001) specify that security culture can be driven by key behavioural elements including the impact on the business, punishment and security awareness. Their research describes a predominantly fear based approach in order to promote good security behaviour;
- Ruighaver, Maynard and Chang (2007) summarize that the influences on security culture are inclusive of context and often reflect an organization's internal culture;
- Stewart (2005) advocates that a security culture should align with business strategy and be incorporated into normal operational practice. Further, it should encourage staff to be alert for potential security issues and raising awareness is key to this strategy. As with organizational culture, if the promotion of a security culture is not given obvious and clear management support, it will fail. This requires that both staff and management are informed and educated on the issues in security and that the management is made aware of breaches in security. The presentation of a business case backed up by financial models will also promote management support;
- Research by Adams and Blandford (2005) cited that the role of the organization, the usability of security solutions and user perceptions were core to the user view of security. In contrast the security profession and thus organizations still focus on technical solutions which are impracticable and unsuitable in a small organizational environment;
- Significant research into what factors demonstrate and drive an organization to improve its security capability through culture by Carnegie Mellon University's Software Engineering Institute has revealed that promoting a security culture is consistently supported several factors. These are that management understand its responsibility to the organization, its staff and customers; that security is an accepted part of business not an add-on; it has appropriate resources allocated to it; that is it integrated into normal business processes; its measurable and aligned with corporate objectives; is everyone's responsibility; and that "rewards, recognition

and consequences with respect to security policy compliance are consistently applied and reinforced" (Allen, 2005); and

- The OECD (n.d.-a) guidelines divide awareness of security culture into three groups: responsibility, response and risk assessment. They advocate that the individual is responsible for the security of the systems they own including responding to incidents and being aware of the risks, threats and vulnerabilities.

These descriptions, whist helpful, do not clearly defined security culture and the literature reflects a reliance on the intuitive meaning of the term culture when linked to the application of security in 'security culture'. These definitions and descriptions of security culture reflect the general meaning of culture but are specific about the roles and operational aspects of every group members. In many ways these definitions of security culture are more suited to the label of security management. Therefore, a review of the descriptions and definitions are needed to ascertain the aspects that contribute to the creation of security culture. In order to do this it is first useful to establish the links to culture and organizational culture, and what drivers and influences they exert.

Culture and Organizational Culture

Von Solms and von Solms (2004) suggest that culture can be influenced by policy and procedure with the continual reiteration of these. Yet, Sasse, Brostoff and Weirich (2001) point out that in many organizations there is a discrepancy between organizational policies and actual behaviour. This is clearly evidence where policies and procedures are not enforced, disregarded or interfere with workflow.

Schein (1992) indicates that the development of organizational culture relies heavily on the beliefs, thoughts and feelings of the group members. Externally these are expressed as policies and procedures consistent with these beliefs. In contrast Hoffman and Klepper (2000) suggest that organizational culture is ill defined and imprecise. Their work specifies that two factors are significant creating this lack of definition. Firstly, that if a strong relationship between individual group members exists then this can create a disjoint in organizational direction and performance. Secondly, whilst cohesive focus of group members on organizational goals may be beneficial to the organization it can sometimes be to the detriment of the individual group members. The variation in these two factors will affect the impact a culture may have on the organization's objectives. Interestingly, Gregory, Harris, Armenakis and Shook (2009) advocate that organizational effectiveness can be directly attributed to staff attitudes which are themselves shaped by culture. The approach taken by von Solms and von Solms (2004) is prescriptive and top management driven and caution with such an approach should be exercised as organizational culture is different to management (Hoffman & Klepper, 2000). It is argued that the definitions of security culture needs to be more inclusive of the behavioural and less measurable aspects of culture which include awareness, ethics and beliefs. Further, it is necessary to take into account factors of the overarching organizational culture and the environment in which it is situated.

FACETS OF SECURITY CULTURE

It is useful to describe the factors that both drive and influence the formulation of security culture. If a straightforward, definitive characteristic can be constructed of what these factors are, it allows for a comparison of actual security culture in an organization to be made against the accepted factors. This would then identify areas that could be addressed to promote improvement in security culture within an organization. Figure 1 is a suggestion for how security culture could be defined from analysis and extraction of the key points from the definitions and descriptions of security culture presented above. Each of the quadrants in Figure 1 represents an area that is integral to the definition of a security culture: response not reaction, responsibility, community of practice and awareness. The two left hand quadrants represent those aspects that are essential to a security culture and should drive its formation, and the two right hand side quadrants are aspects that should only influence it and are therefore labelled discretionary. This diagram does not reflect any particular organisation as its purpose is to define a model environment for the promotion of security culture. Each quadrant is expanded upon below.

Response and not reaction

The idea of response is closely linked to planning and awareness. Planning involves understanding the value of the information to the organization and others putting in place protective measures corresponding to the value of the information. Any response need to be suitable to the threat posed. For instance, locking and dead bolting a window to keep the rain out when simply shutting the window would have the same effect. Response is also linked to the timeliness of what action is taken – shutting the window after the rain has stopped and has already come in, is too late. With the increasing interconnectedness of systems, it is important to respond rapidly to contain the threat and limit further damage.

Identification of what to protect and its value to the organization are important. *Risk = Value x Threat x Vulnerability* is an accepted risk assessment equation. The greater the value of the information to the organization, the greater the risk of damage to the organization if any threat and vulnerability exist. However, often the perception of threat is over estimated

in relation to the value of the information and therefore a perceived risk is given more credence and attention than is required to protect that information. What should also be considered is the impact of any effective threat particularly in terms of workflow and ability to continue with the organization's primary function. Therefore, a defined process for risk assessment and thus a balanced response to treats needs to be predefined.

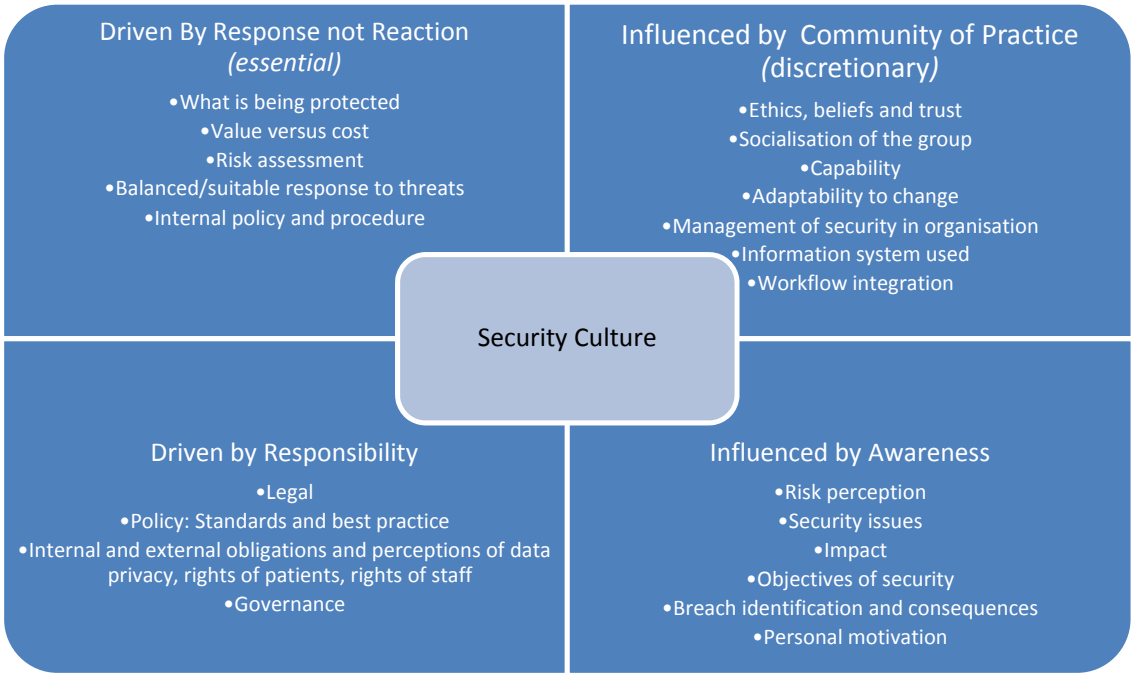

Figure 1- Ideal distribution of factors driving and influencing the promotion of security culture

Responsibility

Responsibility is most often associated with a hierarchy of managerial and supervisory roles. Yet to become part of the cultural fabric, responsibility must be adopted by all group members. Making everyone responsible for security is a difficult task but if couched in terms of responsible within their own role, a better acceptance of this responsibility may be forthcoming. Part of responsibility also includes acceptance of ownership of information (Hall & Schulman, 2009). Associated with this is the issue of litigation and the potential lawsuits where breaches in security occur. Demonstration of compliance and governance will be a major part of defense in such circumstances.

Legally, governments are recognizing that healthcare data is an important set of data that requires special protection (Rode, 2009). In the USA the new American Recovery and Reinvestment Act 2009, which is essentially a law regarding the protection of the US economy, contains some 21 pages on healthcare information privacy. The US leads the world with its HIPAA regulation which is overly stringent. In contrast, Australia is still reliant on its inadequate Data Privacy legislation. Thus, there is reliance on policy, standards and best practice. These are in turn irrevocably linked to internal and external obligations. These obligations reflect data privacy, the rights of customers, the rights of staff; compliance and external perception. An important aspect of security culture is its impact on both internal and external obligations and perception of these. Organisations with any public exposure should be mindful of the public perception of their ability to keep their information safe and secure. Public assurance of the confidentiality and integrity of personal information is paramount for many industries such as banking and healthcare.

Ultimately, responsibility is core to governance and as small organizations become integral to larger national and international initiatives such as e-health, there is a greater emphasis on these organizations to demonstrate a governance process with respect to the information under their control (Fernandes & O'Connor, 2009). This governance relates to the quality, integrity, confidentiality and availability of information otherwise all aspects of information security.

Community of Practice

In small organizations there is often a high level of trust in the organizational culture and this trust in not conducive to effective security particularly when certain attack strategies are reliant on trust, such as social engineering (Scott, 2009). The effect of ethics, beliefs and trust should not be underestimated. For instance, the influence of occupational culture

(May, 2006), has frequently been excluded from discussions on the correlation between technology and social studies. Yet, the relationship between a context, its core function and the communication between group members is fundamental to dynamics of a workplace and how it operates. The acceptance that professional philosophy plays a major part in the creation of a culture is essential. In addition, an individual's ideas on security may vary over time and with different situations, which further complicates group culture (Wright et al., 2009). Linked to this is the ability of the group and individual to adapt to change. Other factors such as capability of the workforce in implementing security should be considered. A major detractor fro good security is also the level to which its practice is integrated into normal workflow. This is integral to the management of security in the organization. Further, the methods used in the management of security are key influences. These include the level of monitoring of systems and staff, the cost and resources allocated the reliability, functionality and usability of the security solutions, and the overarching model of security employed such as multilayered or reactionary.

Lastly, the community of practice can be heavily influenced by the information systems that it uses. The variation in information systems used creates variability in the effectiveness of complementary security management techniques, where multiple systems use disparate operational protection procedures. It is apparent that reliance on the electronic and computer systems used influences other security practices (Williams, 2008). Much of this reliance is unfounded and inaccurately based, creating further vulnerabilities.

Awareness

Awareness is the cornerstone of a security culture. People will make mistakes; forget to log off, passwords are not changed, and files are not updated. These are the realities of working in the computerized information society. The recognition of failures in security is vital in the protection of a system. This, together with consciousness of both internal and external risks, is important to drive behaviour and thus influence the security culture. Whilst awareness includes education and training, this is not the totality of it. It requires behavioural adaptation to create the appropriate response to the protection of information commensurate with its value to the organization.

The use of standards to drive practice is accepted as good practice yet whilst there are standards for technical security (i.e. ISO 17799) there are no standards or guidelines for driving awareness. It is however recognized as a significant factor in the development of a security culture (OECD, 2002). Other elements that comprise awareness include risk perception where decisions are based on knowledge and the perception of the risk (or lack of perception in most cases) are made. Further, the types of security issues themselves and the impact of these are fundamental to awareness. Another fundamental aspect of awareness is breach identification and its consequences. The awareness by staff of the detection of information breaches and the ramifications of these will influence how seriously individuals take their responsibility. If there are no apparent consequences to either poor or no detection of breaches, due to ineffective or unenforced ramifications of information breaches, then this creates a relaxed attitude to security. Whilst using deterrents as a security measure is not preferable to changing behaviour and attitudes. It can be effective and should be one part of a multi-layered approach to security. The perception of lower risk means staff will ignore certain procedures and policies. This poor compliance may not be from malicious intent; it may merely be to work faster or more efficiently.

DISCUSSION OF PROPOSED MODEL

The model is an initial synthesis of the current body of knowledge on creating a culture of information security and is therefore a work in progress. It suggests that certain factors are essential to how a security culture can be facilitated and others are desirable. The influences on security practice may differ from organisation to organisation and may have differing impact from organisation to organisation. As such they are described as discretionary as some may exist and exert influence and others not. The influence factors will be dependent on the communities of practice that exist in the organisation. The model aims to explain many of the factors that are problems for small organisations in building a security conscious culture.

Problems with creating culture in small organization.

Aspects of security considered fundamental to those with a certain level of security awareness and obvious to those in the security professions (such as keeping anti-virus data files up to date and continually active, and the secrecy of authentication codes and passwords), are the basis of a culture of security. Such basic aspects become intuitive and automatic in an established security culture. However, there are barriers to this establishment. In small organizations the problem of creating a security culture include:-

- a reluctance by organizations to invest in non-technological solutions i.e. staff training;
- a lack of control over third parties;
- limited resources and expertise (doing more with less); and

- a lack of appropriate security knowledge.

Whilst in small organizations it is easier to direct staff to follow policy and procedure because the levels of management are generally fewer and communication is usually more direct (von Solms & von Solms, 2004), it can still be problematic to establish a balance between monitoring, control and responsibility. As Chia, Maynard and Ruighaver (2002) report it is difficult to promote a culture of security when there is a lack of management and financial support to improve the security position in an organization. When it is paid lip service as important but neither time nor resources are allocated to address it, security is not perceived as important or something to be adopted intrinsically into daily work practice. This is not necessarily due to a lack of concern rather a lack of recognition of the importance of security and its consequences. Further, there is little doubt that small organizations are significantly impacted by the information systems they use and the constraints they are operationally under. This creates more challenges in maintaining privacy and confidentiality of the information they are responsible for.

CONCLUSION

Many in the security profession agree that to achieve an improvement in information security the issue of human factors must be addressed. This may be addressed by training, education and increasing awareness but ultimately is only sustainable if a security culture can be promoted and adopted. The weakest link the security chain is still the human factor. What is required is not only to put good security procedures in place, but to create a community around practices that support sustainable change and adoption of best practice. In essence what is needed is the creation of an intuitive security culture. As a security profession we are thus charged with facilitating this change. Arguably, this a harder challenge than implementing sophisticated technical solutions.

If we do not actively engage staff in the protection of information then breaches will occur. Education, reinforcement and integration with day to day activities are essential to its success. Creating an environment where every staff member sees them self as a valuable part of the security culture will ensure its sustainability and increase the protection of important information. A balance between responsibility and monitoring needs to occur. The objective in attempting to create or improve security culture is an organization into ensure appropriate behaviour in regards to security sustained long after training in security has ceased.

The diagrammatic representation of the factors which ideally drive and influence security culture is a preliminary step in investigating how security culture can be manipulated to promote improvement in information security practice. It provides a basis for discussion and a template from which an existing culture can be benchmarked and areas for change identified. This research is the starting point for investigation into this area and a more formal systematic review of the body of knowledge on security culture will be undertaken. Further research into methods to cultivate such a security culture and how to assess the maturity of organizations in relation to the development of security culture is planned.

REFERENCES

Adams, A., & Blandford, A. (2005). Bridging the gap between organizational and user perspectives of security in the clinical domain. *International Journal of Human-Computer Studies, 63*(1-2), 175-202.

Allen, J. (2005). *How do I know if I have a culture of security?* Retrieved Oct 01, 2009 from http://www.cutter.com/content-and-analysis/resource-centers/enterprise-risk-management/sample-our-research/erm050428.html

Anonymous. (2009). Sanction Guidelines for Privacy and Security Breaches. *Journal of AHIMA, 80*(5), 57-62.

Australian Government (2009) *Stay Smart Online.* Retrieved Oct 20, 2009 from http://www.staysmartonline.gov.au/.

BBC News (2008). *Nearly 100 medical records 'lost'.* Retrieved Aug 13, 2008 from http://news.bbc.co.uk/2/hi/uk_news/northern_ireland/7555165.stm

Business and Advisory Committee to the OECD. (2004). *Securing your business. An companion for small or entrepreneurial companies to the 2002 OECD Guidelines for the security of networks and information systems: Towards a culture of security*: OECD. International Chamber of Commerce: OECD

Chia, P. A., Maynard, S. B., & Ruighaver, A. B. (2002). *Exploring Organisational Security Culture: Developing a comprehensive research model*. Paper presented at the IS ONE World Conference, Las Vegas, 4-5 April 2002. Retrieved May 10, 2007 from http://disweb.dis.unimelb.edu.au/staff/seanbm/research/ChiaCulturePaper.pdf

Doherty, N. F., & Fulford, H. (2005). Do Information Security Policies Reduce the Incidence of Security Breaches: An Exploratory Analysis. *Information Resources Management Journal, 18*(4), 21-40.

Fernandes, L., & O'Connor, M. (2009). Data Governance and Data Stewardship. *Journal of AHIMA, 80*(5), 36-39.

Gregory, B. T., Harris, S. G., Armenakis, A. A., & Shook, C. L. (2009). Organizational culture and effectiveness: A study of values, attitudes, and organizational outcomes. *Journal of Business Research, 62*(7), 673-679.

Hall, M. A., & Schulman, K. A. (2009). Ownership of Medical Information. *JAMA, 301*(12), 1282-1284.

Hoffman, N., & Klepper, R. (2000). Assimilating New Technologies: The Role of Organizational Culture. *Information Systems Management, 17*(3), 1 - 7.

May, T. (2006). The missing middle in methodology: occupational culture and institutional conditions. *Methodological Innovations Online, 1*(1).

McIlwraith, A. (2006). *Information Security and Employee Behaviour*. Aldershot, Hampshire, UK: Gower.

O.E.C.D. (n.d.-a). Culture of security for information systems and networks. Retrieved 01 October, 2009, from www.oecd.org/sti/cultureofsecurity

O.E.C.D. (n.d.-b). Initiative by country. Retrieved 01 October, 2009, from http://www.oecd.org/document/63/0,3343,en_21571361_36139259_36306559_1_1_1_1,00.html

Rode, D. (2009). Recovery and Privacy. *Journal of AHIMA, 80*(5), 42-45.

Ruighaver, A. B., Maynard, S. B., & Chang, S. (2007). Organisational security culture: Extending the end-user perspective. *Computers & Security, 26*(1), 56-62.

Sasse, M. A., Brostoff, SB., & Weirich, D. (2001). Transforming the 'weakest link' -- a human/computer interaction approach to usable and effective security. *BT Technology Journal, 19*(3), 122-131.

Schein, E. (1992). *Organizational culture and leadership* (2nd ed.). San Francisco: Jossey-Boss.

Schlienger, T., & Teufel, S. (2003). *Analyzing information security culture: increased trust by an appropriate information security culture.* In the proceedings of 14th International Workshop on Database and Expert Systems Applications, IEEE.

Scott, D. (2009). Social Engineering: Hacking the Wetware! *Information Security Journal: A Global Perspective, 18*(1), 40 -46.

security.tao.ca. (n.d.). *Security culture.* Retrieved 25 Aug, 2009, from http://security.resist.ca/personal/culture.shtml

Thomson, K.-L., von Solms, R., & Louw, L. (2006). Cultivating an organizational information security culture. *Computer Fraud & Security, 2006*(10), 7-11.

Tsohou, A., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2008). Investigating Information Security Awareness: Research and Practice Gaps. *Information Security Journal: A Global Perspective, 17*(5), 207-227.

von Solms, R., & von Solms, B. (2004). From policies to culture. *Computers & Security, 23*(4), 275-279.

Williams, P. A. H. (2008). When trust defies common security sense. *Health Informatics Journal, 14*(3), 211-221.

Wright, D., Gutwirth, S., Friedewald, M., De Hert, P., Langheinrich, M., & Moscibroda, A. (2009). Privacy, trust and policy-making: Challenges and responses. *Computer Law & Security Report, 25*(1), 69-83.

COPYRIGHT