



Capturing Culture in Medical Information Security Research

Patricia A. H. Williams*

*SECAU: Security Research Centre, School of Computer and Security Science, Edith Cowan University

Abstract

The definition and deconstruction of culture is an intricate exercise which is multifaceted and multilayered and has at its core, values that drive behaviour and practice often instinctively. One aspect of such culture that is deeply embedded in the medical setting is trust. Researching the influence of culture on security practice is a complex task in this situation, yet information systems research must address such factors if effective information security is to be promoted. In the medical environment this is particularly important as electronic communication is becoming widely adopted and as E-health and shared electronic patient information develops into a focal point for many health services worldwide. Through a series of research projects using traditional methods of investigation, it was identified that trust is a powerful influence on how information security is implemented in primary care medical practices. An underestimation of potential threats coupled with a lack of understanding of security concepts further fosters reliance on trust within this environment. The challenge was to design methods that would investigate the influence of trust within an information systems framework. The methods chosen are a fusion of separate investigative techniques. The combination of methods provides a unique triangulation of interviews, observation and physical artefacts from which to investigate how trust is reported and how it influences practice. The importance of adopting alternative methods within the sphere of information systems research is that it is essential that techniques are used to inform development of effective and contextualised solutions for information security threats in the medical environment.

Keywords: Medical information security, trust, culture, general practice

Introduction

Culture has many definitions yet in the broadest sense is the cultivated behaviour of a group of people. Such behaviour is referred to as 'tradition' and includes patterns of behaviour that are both implicit and explicit. It is a widely held view that the manifestation of culture is predominantly formed by the values that a group of people hold (Hofstede and Hofstede, 2004). In research this presents challenges as such values are frequently unconscious to those who possess them and are therefore difficult to elicit through traditional research

Correspondence: P. Williams, School of Computer and Security Science, Edith Cowan University, Mt Lawley Campus, 2 Bradford Street, Mt Lawley, Western Australia 6050, Australia. Tel.: (61 8) 9370 6299.

E-mail: trish.williams@ecu.edu.au

methods. If we use a multilayer model of cultural theory, comprising of national regional, gender based, generational, social class and corporate stratum (ibid), the establishment of culture in the primary care medical environment is predominantly located at the corporate (organisational) and social class (education/occupational) layers. The identification with the corporate layer is evident as the Australian primary care medical environment is comprised of small, independent, mainly private practices, and thus reflects an autonomous organisational structure. This is similar to other countries, in particular the UK and European countries. Although in these areas much of the primary health care is not privately based, they do retain relatively autonomy in terms of management and operational functionality. In terms of a social class layer, the medical profession has a strong and clearly defined educational and occupational structure. In contrast with cultural research, information systems research does not examine cultural differences; rather it investigates the extent to which certain cultural values influence decisions and practice. It is the integration of knowledge, shared beliefs and customary practice which form the characteristics of social practice (culture, 2009), and thus in the context of information security practices in the medical environment, how information security procedures are formulated and put into practice. Many researchers identify that understanding culture is important in the successful use of IT based information systems (Brooks et al. 2005, Leidner and Kayworth, 2006, Oates, 2006).

Corporate culture shapes how and what action staff take and it exudes a powerful albeit subtle influence on staff and information flows within an organisation (Leidner and Kayworth, 2006). The influence of organisational culture on security practice should not be confused with the creation of a security culture itself within an organisation. Security culture is the integration of information protection into everyday procedures (Thomson et al. 2006). In the medical environment there exists a culture of trust that is both a benefit to the underlying external nature of practice and vulnerability as attention to detail and adherence to basic policy are poor. In Australia, research indicates that primary care medical practices do not take adequate security measures to ensure protection patient information (Schattner and Pleteshner, 2004).

Security research has begun to focus on the human-computer interaction and user perception, primarily because it is not the technical solutions that are ineffective. As Adams and Blanford (2005) suggest, there exists a gap between organisational approaches to security and the end-user perspectives that drive actual practice. It is well documented that whilst some barriers to good security practice lie in the technological challenges, it is the process and people, referred to as the organisational factors that have the greatest influence on security application (Ma et al. 2008). Many researchers have identified that the end-user and the insider are the biggest threat to security through a lack of knowledge and increased access (Aldhizer, 2008, Cole and Ring, 2006, Furnell, 2005, Theoharidou et al. 2005). Whilst privacy may be well understood by medical practitioners, nurses and medical administration staff in terms of handling patient data, the security practices associated with this are inconsistent and in some cases nonexistent (Williams, 2008a). The health industry relies increasingly on technological innovation and has undergone significant transformation with the advent of information systems for administration and patient management and more recently shared electronic medical records. This technological change of itself has significantly affected views of trust in relation to the use of technology (Dearne, 2009).

This paper discusses how trust as part of an organisation's culture in the primary care medical practice can be researched within an information systems research methodology. The issue of trust and its affect has arisen as a supplementary factor in research into more fundamental issues in security implementation and capability. However, the results have clearly identified that culture has a strong influence on the acceptance and improvement in security practices. A series of research projects are described where these projects investigate the effectiveness of organisational security practices using predefined established security protocols. These are

inclusive of specific reference to the culture of trust to see if there is direct or indirect impact of trust in information security decisions or activities.

Influence of trust in small organisations.

In cases where the organisational entity is small, particularly when considering associated behaviour in information systems research, investigation is most often linked to 'communities of practice'. A community of practice is the link between work practices and strategic operations (Wenger et al. 2002). Of particular importance are the informal work practices that occur in any organisation. Day-to-day activities, driven by workflow, significantly influence the manner in which activities such as those related to information security are managed and put into effect. In organisations, the complexity of legal requirements means that there is very little consistency between knowing the law and following it (Levin-Rozalis, 2007). What is more common is the behaviour of a community of practice where the social consistency and obligation overrides knowledge of the law. Of course, in meeting the social obligations the law is often adhered to but not necessarily intentionally. Arguably, the level of trust engendered in small primary care medical practices is indicative of a team approach where there are a small number of employees and a direct relationship with management (Fleming, 2007).

The primary care medical practice environment in Australia is akin to small business with privately owned practices typically with 1-10 medical practitioners. Elsewhere in the world, primary care has a similar structure but with a mixture of privately and publicly funded medical practices. Regardless of the funding, a small business structure is applicable to the majority of practices and each organisation is usually self-managed. However, unlike small business they are more complicated in terms of the requirements for their information security practice (Grain, 2005). There are important issues from both ethical and legal perspectives in relation to the sensitivity of information (Meredith, 2005), a lack of understanding of security concepts, and a serious underestimation of genuine threats (Valli, 2006, Valli and Woodward, 2008). It is clear from the literature that technological solutions and software availability for effective information protection are not scarce (Landwehr, 2001, Post and Kagan, 2006, Tsoumas and Tryfonas, 2004). However, approaching information security from a purely technical perspective has not been successful. Disclosures of sensitive medical information have been well documented (Chester, 2003, Doherty and Fulford, 2005, General Practice Computing Group, 2005, Leach, 2003), and these reports indicate that medical information security is not a technical or computer problem, but is a human one.

In the security community it is accepted that standards should drive policy which then informs decision making and practice. In large organisations this does not present major issues in implementation as organisational wide decisions on security are made. However, in small organisations such as primary care medical practices, whilst this is desirable it is rarely put into practice (Williams, 2006) and information security practice is known to be reticently adopted by medical practices. As Karyda et al (2005) concluded, the culture of each organisation affects the formation and implementation of the security policy and thus the security practices are further complicated by the trustful environment that exists in medical practices (Allen, 2000, Kallath, 2005, Williams, 2008b). Further, it is generally recognised that there are significant issues associated with the sensitive nature of patient information. Added to this are fundamental resource problems where the end-user, the general practitioner, is time poor and rarely employ dedicated IT or security staff. Whilst they are consumers of technology, they are not IT or security specialists and the protection of information is not their core business. The autonomous nature of staff in such small organisation reinforces informal and individualised work practices. Frequently such issues can be attributed to a lack of fit between policy and work practice in small organisations (Adams and Blandford, 2005).

Information systems research, which is often used for the investigation of security practice, includes facets of cognitive science and behavioural psychology which are used to explain security behaviour. Yet information systems research does not attempt to investigate these from the cognitive or behavioural research perspectives; they are used as they apply to the information system under investigation. A more comfortable concept for information systems research is that of communities of practice and their influence on behaviour. Vaast (2007) suggests that it is the communities of practice that influence information systems security based on the social constructs that they produce. As with any community with diverse membership, it has a unique socio-cognitive perspective due to individual community members' differing knowledge and experience. Thus, a community of practice is inclusive of individual perspectives whilst sharing a specific view. Hence, using the premise that end-user perceptions of security are linked to the function of their professional or industry (Goodhue and Straub, 1991) supports the socio-organisational influence on the awareness and implementation of information security.

Culture in information systems research

Interestingly, the lack of awareness and perception of potential security issues by end-users has not altered greatly since Goodhue and Straubs' (1991) initial research (D'Arcy et al. 2009, Furnell, 2007). In order to research the influence of a trustful culture within an information systems research approach, mixed methods are used to report and confirm security practice and identify any community of practice driving forces. Whilst there is a considerable body of knowledge on the impact of culture on behaviour and organisational effectiveness, more is needed on the effects on specific context domains (Gregory et al. 2009). Although understanding the motivation of the community of practice is helpful, using research techniques such as repertory grid analysis or cognitive mapping are not appropriate for this investigation. Whilst important, the complex interaction between the information systems used and the staff in this specific work context is not being investigated. Similarly, more intricate construction of social actions performed using a socio-pragmatic approach to further explore the relationship between information systems and their function in work practices may be helpful (Goldkuhl and Agerfalk, 2005), however this approach fails to isolate the facet of trust with a view to modifying action based on the findings.

Existing research indicates that using novel conceptual approaches to IT-cultural research, which are traditionally separate research streams, can be effective in meeting the disparity between the research methods (Leidner and Kayworth, 2006). It is evident that to date no single methodology has been established as preferable to study the eclectic and complex information systems-cultural issue. Further, many cultural theorists report that in a values based approach to cultural analysis, multiple and competing subgroups in an organisation, possessing differing values, can cause conflict and interruption to information systems effectiveness (Robey and Boudreau, 1999).

To undertake research in this area, consideration also needs to be given to the potential issues regarding access to information assets as part of workflow, perception, responsibility and education within each community of practice (Ruighaver et al. 2007). Indeed, the community of practice influence may also confirm research by Hoffman and Klepper (2000) which suggests that organisations with high levels of networking and sociability usually results in poor assimilation with technology, Thus, the methodology used in this research addresses the need for a balance between the culture of trust and effectiveness of information security practice in the specific primary care medical practice environment.

Research methods

Existing research: A series of research projects undertaken in 2006-2008 identified trust as a notable influencing factor in decisions and procedures related to information security in primary care medical practices in Australia and the UK (Williams, 2008b). This preliminary research into information systems security in the medical environment was not undertaken with the influence of culture in mind; the research was to assess the factors that contributed to poor security practice with a view to finding ways to improve this. Research into changing physician behaviour (Bauchner et al. 2001) indicates that passive dissemination of new information and guidelines are not effective, whilst implementation of these measures through organizational (practice) routes can be effectual. Initial research into the factors that contribute to information security practice was undertaken using traditional interview methods to obtain a rich source of information on practices, and perceptions. An action research methodology was employed in these original research projects. Using traditional methods resulted in an indication of an underlying problem in using security in the medical practice environment which was related to a culture of trust. During the process of action research substantial reflection was made on the themes in the original data set. It was identified that aspects of security practice reflect an underlying theme of trustfulness that was not explicitly reported by the participants. This identification was incidental to the main research, which primarily investigated information security practices to inform formulation of an effective information security governance process.

The analysis of the interviews resulted in seven themes. Whilst capability and knowledge of staff, together with cost and lack of time were themes which were anticipated, the occurrence of trust and reliance on software, technology, staff and medical authorities was unexpected. Further, this reliance had a considerable impact on the inconsistencies found between what was believed to be good security practice and what was actually implemented (Williams, 2008b). Further analysis of the interviews in relation to trust revealed that two-thirds of all trust is based on staff and the software implemented in the practice. The trust placed in software, in conjunction with poor implementation, are serious matters for concern. Reliance on third parties was also identified as an issue since uncontrolled access to information is given to those who commonly provide computer assistance and support. Such interaction with the computer systems and confidential information are not monitored by the practices themselves nor are the third parties required to give any written assurances of confidentiality.

This was the first instance that the accepted culture and trustful nature of the medical environment was identified as a potentially significant factor in information security practices. It was evident that the perception of security as it related to the medical practices significantly affected security practice. Subsequent research into the capability of a practice to implement information security measures revealed further evidence that culture affects information security practice. The second research project looked at the capability of practices to assess their security capability, the maturity of their security process whilst also identifying incremental improvement. Again action research and in-depth interviews were used. The results of this project also indicated that assumptions in capability and actual practice are regularly made based on trust in staff, software and third party support providers.

These two research projects did not set out to assess or measure the effect of culture however they clearly resulted in evidence of how a trustful culture can impact security practice. Consequently, there was a need to design research methods to investigate this phenomenon and to measure the extent of the influence of this culture on how security is undertaken in primary care medical practices. As a result, two subsequent research projects have incorporated methods to investigate the factors related to trust such as implementation actions and detractors and promoters of good security practice. This is undertaken by looking at the methods of implementation rather than the type of organisation in which they are applied (which is a common method for

security research). The results of these studies will be used to create more effective implementation related to security capability protocols, rather than try to address a change in culture. These protocols would be generalisable in any medical context since they will influence the implementation of security and not try to change the culture itself.

Current research: To enable sufficient information on the presence and effect of the trustful culture to be gathered, an alternative methodology needed to be employed. It is not suitable at this juncture to try to influence the trust culture through the research, as too little is known about the extent of the influence it has. Hence, the investigations consider the extent to which the culture impacts security decisions and actions. The ultimate objective is to improve security practice in this specific context and since culture is only one facet of this the research does not solely concentrate on this.

Such research therefore requires a multi-faceted and non-traditional approach. The design of the research is based on two stages. Firstly, a review of existing literature to identify cases relating to the implementation of information security in primary care medical practices is undertaken. This allows a cross-case analysis to identify information security implementation issues and promoters within this context and may provide an insight into those factors which are directly related to trust. The analysis and evaluation is then based on effectiveness of implementation. The unit of analysis is each implementation and the evaluation is the specified method of information security implementation rather than the organisation. This critical analysis informs the assembly of each security protocol activity to promote relevancy and contextual application to the primary care medical practice environment. Secondly, eliciting implicit behaviours is problematic and potentially limiting using interview methods alone. The research uses multiple case studies and practice-based research to record the experience of the participants and, more critically, the context of their actions. Data is collected through traditionally disparate information systems research techniques: self-reporting interviews, observations and physical artefact investigation. These methods will capture specific information security practice as well as the contextual complexity of the environment as each case will reflect one community of practice. Analysis of qualitative interview data, together with observation of actual practice and investigation of physical artefacts and the electronic/computer systems used will result in a rich set of data. Initial analysis will compare the external assessment (observations by the researchers) to the self-assessment by the participants. This comparison will assess the reliability of verbal reports against the observed behaviours in the practices, and will address the limitations of self-reporting and identify any discrepancy in the self-reporting method. Using triangulation of the multiple communities of practice, the qualitative analysis will identify gaps in relevancy and implementation and more importantly these findings will inform the revision of the information security protocols by considering any potential causes of failure or success in relation to social and organisational factors. This will also highlight and provide evidence of social and contextual barriers in practice arising from the community of practice accepted norms.

It is envisaged that investigating potential discrepancies by testing the reliability of self-assessment will identify the strengths and weaknesses in process affected by the contextually inherent trust factors. This identification can then contribute to contextualizing recommendations for immediate and long term improvement. The resulting findings will inform procedural changes and not attempt to influence the culture itself. The use of triangulation of methods within a multiple case study approach is innovative as their purpose is to inform procedural changes to improve practice. It has the objective of influencing practice while accommodating rather than necessarily changing culture.

Future research: As a post project investigation, possible mapping to cultural theory may be examined from secondary analysis of the data. This would be expected to give an explanation and contrasting viewpoint on the effect of culture on information security practice. Subsequent research will analyse the data to ascertain if

it reflects on the many values based approaches to cultural theory. This will be undertaken to discover if it is possible to predict success in information security practice based on the values of a specific community of practice. There is little research in this area related to the medical context and such research may enhance our ability to effect change in information security practice by delineating the difference between task-oriented and people-oriented communities of practice. Further, it is important to identify areas of conflict that may impact actions and workflow with respect to the trust factor in culture and the use of information security measures.

Other research into the overarching process of security governance in the medical environment is occurring concurrently, and the findings of this research will be integrated into the facets of governance that are affected by the trustful culture already identified. Additionally, research will be undertaken to investigate how a security culture may be fostered in the medical context where a balance between organisational trust can coexist with effective information security practice.

Discussion

There exists research into information systems trust which looks at the level of trust that humans put into the interaction with information systems. This forms the body of knowledge on trust theory and models, however there is little research into the trust in information systems themselves by users. Despite information security incidents occurring users continue to place an unmitigated trust in their information systems (Biros, Fields and Gunsch, 2003). Trust is central to business and social interactions between people and organisations. In the medical environment this is particularly strong between patients and doctors. Yet, there is perhaps a misplaced trust in the electronic information systems that are integral to many of these interactions (Sasse, 2004). Humans are generally goal-driven and therefore information systems are used to assist in making processes efficient. As such, reliance on the information system assumes that in the work environment the risks are provided for. This is a major flaw in any trustful culture that renders such information systems at greater risk. The reasons for this can be traced to a lack of understanding of the risks and a lack of awareness of security issues by individuals and the organisation. However, as Sasse (2004) points out security is a supporting task to the mainstream processes of workflow and therefore the trust in the information systems may be misplaced if the supporting task of security is not undertaken effectively.

The inclusion of trust in technology acceptance modeling is also apparent in interpersonal and inter-organisational trust which is the focus of research into e-commerce and networked electronic information systems (Xin, Valacich and Hess, 2004). Researchers such as Lippert and Swiercz (2005) have considered the inherent technology trust that exists in the use of specific information systems. Technology trust is defined as the extent to which an individual's expectations of the information systems' ability correlate with their trust in the system. This is based on the technology's perceived predictability, reliability and utility and can be used for prediction of implementation success of information systems. This area of research includes reference to behavioural science in understanding the relationship between humans and inanimate (machine) objects. Interestingly, it is also inclusive of organizational culture, organizational communities and the influence of organizational trust and leadership. Another area of trust in information systems is the increasingly important use of cryptography in trusted communications. This is a technical use of the term trust and is not related to human factors or cultural influences. It relates to distributed information systems and secure communications. This type of trust is a necessary component in today's information systems as it reinforces human confidence in the reliability on systems to perform critical functions. It also fosters information exchange protocols to ensure trustworthy and secure communications.

Whilst this discussion highlights the importance of trust in information systems, it is not trust in the information systems itself that is solely under consideration in this research. This facet of trust does however form part of the construction of trust in the medical environment as indicated in the original seven themes discussed earlier, specifically related to trust and reliance in technology.

The research projects described reflect the premise that ‘no one approach to information systems research can provide the richness that information systems, as a discipline, needs for further advancement’ (Kaplan and Duchon, 1988). What is required is context specific investigation with communities of practice indicators, rather than standard security and information systems measures. The evaluation and capture of the environmental culture is a vital component in improving information security in the medical setting. The research will provide an explanation of the cultural impact of trust on information security practices. It will also show in what forms it presents in daily workflow and management of the environment.

The innovation occurs in accommodating for culture rather than attempting to shape it as is often the case with information systems and technology implementation. In this interpretive research, where experimental control is not a feature, the context is essential to developing an understanding of the phenomenon. The social systems involved in the community of practice using the information system are a significant aspect of research. More traditional security and information systems research omit the social interactions, political issues and negotiations that occur in the work environment (Leidner and Kayworth, 2006). Applying the suggested research method provides an immersion in the context and strengthens the basis of the resulting interpretive perspective. In addition, the cross-validation of results using triangulation of different sources and kinds of data further strengthen the findings. Where culture, and in particular ‘trust’, is under investigation it is vitally important to understand how the participants conceptualise information security as this may influence an individual’s behaviour.

The research methods described also address the problems first identified by Kaplan and Duchon in 1988 in regard to the lack of effectiveness of information systems research methods. They identified that whilst interactions of users are commonly studied, the interrelationships between the effectiveness of the information systems and the community of practice and associated workflow are not. This remains an issue for research into information systems and security today (D’Arcy et al. 2009).

Conclusion

The challenge for information systems research is the integration of information security into existing information infrastructures that are strongly affected by culture and informal community of practice processes. The transparent integration of information security into daily procedures means combining constituent elements/activities into a coordinated, complete and compliant whole (‘integration’, n.d.). This addresses the socio-technical dilemmas of behaviour in this particular community of practice, where both the staff and the systems are stakeholders in the information system (Bygstad, 2006). The outcome of this is that all stakeholders in this complex and dynamic environment must work together to ensure the security of sensitive information from a social and technical competence perspective and well as an internal and external compliance perspective.

It is clear that the trustful culture in the medical environment is strong and influences decisions, understanding and actual practice. Further, what is required is research into the extent of influence this has on security practice for the medical environment where little IT or security expertise is employed. It is essential that a security culture is fostered in medical practices and supported by education and integration with work

processes. This will only occur if we can investigate the drivers and address the impact that a trustful culture has on security practices in the medical environment.

The innovation in the research is in using a multi methods data collection technique within traditional methodology, and where the subsequent analysis is based on information systems ideology rather than a behavioural one. Further, the impact of the research is in the ability of the research findings interpretation to result in improvements in information security practices within the complex medical environment. Approaching culture from an information systems perspective rather than from a cognitive and behavioural perspective allows potential contextualised improvement to be made appropriate to the technologies and processes of information security. This research will uncover the behaviours of staff in relation to information security and how their values and trust guide their decisions and actions.

Whilst it is acknowledged that perception of information security will alter as the environment changes, and other factors such as changes in the law and development of technology occurs, this perception does not occur automatically. It is the influence of the communities of practice that exert a stronger force. Ultimately changing the culture means reframing the beliefs of staff which of itself can meet with resistance unless it is managed with sensitivity and can be shown to be beneficial to those who are required to change.

References

- (n.d.), Integration. Available online at: <http://dictionary.reference.com/browse/integration> (accessed September 15 2009).
- Adams, A. and Blandford, A. (2005) 'Bridging the Gap between Organizational and User Perspectives of Security in the Clinical Domain', *International Journal of Human-Computer Studies*, Vol. 63, No. 1-2, pp. 175 - 202.
- Aldhizer, G. R. (2008) 'The Insider Threat: Automated Identity and Access Controls Can Help Organizations Mitigate Risks to Important Data (Risk Watch)', *Internal Auditor*, Vol. 65, No. 2, pp. 71 - 73.
- Allen, P. (2000) 'Clinical Governance in Primary Care: Accountability for Clinical Governance: Developing Collective Responsibility for Quality in Primary Care', *British Medical Journal*, Vol. 321, No. 7261, pp. 608 - 611.
- Bauchner, H., Simpson, L. and Chessare, J. (2001) 'Changing Physician Behaviour', *Archives of Disease in Childhood*, Vol. 84, No. 6, pp. 459 - 462.
- Biros, D.P., Fields, G., and Gunsch, G. (2003) 'The effect of external safeguards on human-information system trust in an information warfare environment', in *Proceedings of the 36th Annual Hawaii International Conference on Systems Sciences*, 10pp. IEEE Computing Society.
- Brooks, L., Davis, C. J., and Lycett, M. (2005) 'Organisations and Information Systems: Investigating Their Dynamic Complexities Using Repertory Grids and Cognitive Mapping', *International Journal of Technology and Human Interaction*, Vol. 1, No. 4, pp. 39 - 55.
- Bygstad, B. (2006) 'Managing Socio-Technical Integration in Iterative Information System Development Projects'. *International Journal of Technology and Human Interaction*, Vol. 2, No. 4, pp. 1 - 15.
- Chester, M. (2003) 'Abused by the NHS: Patient Consent and Confidentiality', *Consumer Policy Review*, Vol. 13, No. 2, p. 38.

Cole, E. and Ring, S. (2006) *Insider Threat: Protecting the Enterprise from Sabotage, Spying, and Theft*. Syngress Publishing: Available online.

Culture (2009) Merriam-Webster Online Dictionary. <http://www.merriam-webster.com/dictionary/culture>, Accessed, August 30, 2009

D'arcy, J., Hovav, A., and Galletta, D. (2009) 'User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach'. *Information Systems Research*, Vol. 20, No. 1, pp. 79 - 98.

Dearne, K. (2009, 5 Sept) 'Fears over Sharing of Medical Data', *The Weekend Australian*, p.12 Professional Section.

Doherty, N. F. and Fulford, H. (2005) 'Do Information Security Policies Reduce the Incidence of Security Breaches: An Exploratory Analysis', *Information Resources Management Journal*, Vol. 18, No. 4, pp. 21 - 40.

Fleming, S. (2007) 'Implicit Trust Can Lead to Data Loss', *Information Security Journal: A Global Perspective*, Vol. 16, No. 2, pp. 109 - 113.

Furnell, S. (2005) 'Why Users Cannot Use Security', *Computers and Security*, Vol. 24, No. 4, pp. 274 - 279.

Furnell, S. (2007) 'Making Security Usable: Are Things Improving?', *Computers and Security*, Vol. 26, No. 6, pp. 434 - 443.

General Practice Computing Group (2005) *Real Security Breaches in GP*. <http://www.gpcp.org.au>, Accessed November 09, 2005.

Goldkuhl, G. and Agerfalk, P. J. (2005) 'It Artefacts as Socio-Pragmatic Instruments: Reconciling the Pragmatic, Semiotic, and Technical', *International Journal of Technology and Human Interaction*, Vol. 1, No. 3, pp.29 - 44.

Goodhue, D. and Straub, D. W. (1991) 'Security Concerns of System Users: A Study of Perceptions of the Adequacy of Security', *Information and Management*, Vol. 20, No. 1, pp. 13 - 27.

Grain, H. (2005) 'Information Systems in the New World: An Emerging National Approach', *Australian Health Review*, Vol. 29, No. 3, pp. 292 - 296.

Gregory, B. T., Harris, S. G., Armenakis, A. A., and Shook, C. L. (2009) 'Organizational Culture and Effectiveness: A Study of Values, Attitudes, and Organizational Outcomes', *Journal of Business Research*, Vol. 62, No. 7, pp. 673 - 679.

Hoffman, N. and Klepper, R. (2000) 'Assimilating New Technologies: The Role of Organizational Culture', *Information Systems Management*, Vol. 17, No. 3, pp. 1 - 7.

Hofstede, G. H. and Hofstede, G. J. (2004) *Cultures and Organizations: Software of the Mind: Intercultural Cooperation and Its Importance for Survival*, 2nd edition. McGraw Hill: London.

Kallath, D. (2005) 'Trust in Trusted Computing - the End of Security as We Know It', *Computer Fraud and Security*, Vol. 2005, No. 12, pp. 4 - 7.

Kaplan, B. and Duchon, D. (1988) 'Combining Qualitative and Quantitative Methods in Information Systems Research: A Case Study', *MIS Quarterly*, Vol. 12, No. 4, pp.571 - 586.

Karyda, M., Kiountouzis, E., and Kokolakis, S. (2005) 'Information Systems Security Policies: A Contextual Perspective', *Computers and Security*, Vol. 24, No. 3, pp. 246 - 260.

Landwehr, C. E. (2001) 'Computer Security', *International Journal of Information Security*, Vol. 1, No. 1, pp. 3 - 13.

- Leach, J. (2003) 'Improving User Security Behaviour', *Computers and Security*, Vol. 22, No. 8, pp. 685 - 692.
- Leidner, D. E. and Kayworth, T. (2006) 'Review: A Review of Culture in Information Systems Research: Toward a Theory of Information Technology Culture Conflict', *MIS Quarterly*, Vol. 30, No. 2, pp. 357 - 399.
- Levin-Rozalis, M. (2007) 'Playing by the Rules: Social Representations of 'Law' as the Socio-Cognitive Mediating Mechanism between Law and Society', *Theory Psychology*, Vol. 17, No. 1, pp. 5 - 31.
- Lippert, S. and Swiercz, M. (2005) 'Human Resource Information Systems (HRIS) and Technology Trust', *Journal of Information Science*, Vol 31, No. 5, pp. 340 - 353.
- Ma, Q., Johnston, A. C., and Pearson, J. M. (2008) 'Information Security Management Objectives and Practices: A Parsimonious Framework', *Information Management and Computer Security*, Vol. 16, No. 3, pp. 251 - 270.
- Meredith, B. (2005) 'Data Protection and Freedom of Information', *British Medical Journal*, Vol. 330, No. 7490, pp. 490 - 491.
- Oates, B. J. (2006) 'Discussion on Paper 1: Exhausted by the Struggle? Methods for Socio-Technical Systems', *International Journal of Technology and Human Interaction*, Vol. 2, No. 4, pp. 15 - 17.
- Post, G. V. and Kagan, A. (2006) 'Information Security Tradeoffs: The User Perspective', *EDPACS: The EDP Audit, Control and Security Newsletter*, Vol. 34, No. 3, pp. 1 - 10.
- Robey, D. and Boudreau, M.C. (1999) 'Accounting for the Contradictory Organizational Consequences of Information Technology: Theoretical Directions and Methodological Implications', *Information Systems Research*, Vol. 10, No. 2, p. 167.
- Ruighaver, A. B., Maynard, S. B., and Chang, S. (2007) 'Organisational Security Culture: Extending the End-User Perspective', *Computers and Security*, Vol. 26, No. 1, pp. 56 - 62.
- Sasse, A. M. (2004) 'Usability and Trust in Information Systems', *Cyber-Trust and Crime Prevention Project*, Office of Science and Technology, <http://www.dius.gov.uk/~media/publications/F/file15320>
- Schattner, P. and Pleteshner, C. (2004) *GPCG Computer Security Project: Final Report*. Melbourne: Monash University, Department of General Practice.
- Theoharidou, M., Kokolakis, S., Karyda, M., and Kiountouzis, E. (2005) 'The Insider Threat to Information Systems and the Effectiveness of Iso17799', *Computers and Security*, Vol. 24, No. 6, pp. 472 - 484.
- Thomson, K.L., Von Solms, R., and Louw, L. (2006) 'Cultivating an Organizational Information Security Culture', *Computer Fraud and Security*, Vol. 2006, No. 10, pp. 7 - 11.
- Tsoumas, V. and Tryfonas T. (2004) 'From Risk Analysis to Effective Security Management: Towards an Automated Approach', *Information Management and Computer Security* Vol. 12, No. 1, pp. 91 - 101
- Vaast, E. (2007) 'Danger Is in the Eye of the Beholders: Social Representations of Information Systems Security in Healthcare', *Journal of Strategic Information Systems*, Vol. 16, No. 2, pp. 130 - 152.
- Valli, C. (2006) 'The Insider Threat to Medical Records; Has the Network Age Changed Anything?', in H. R. Arabnia and S. Aissi (editors), *The 2006 World Congress in Computer Science, Computer Engineering, and Applied Computing - Sam'06 - the 2006 International Conference on Security and Management: Monte Carlo Resort, Las Vegas, Nevada, USA* .
- Valli, C. and Woodward, A. (2008) 'The 2008 Australian Study of Remnant Data Contained on 2nd Hand Hard Disks: The Saga Continues', in C. Valli and A. Woodward (editors), *Proceedings of the 6th Australian Digital Forensics Conference*, School of Computer and Information Science, Edith Cowan University: Perth, Western Australia.

Wenger, E., McDermott, R., and Snyder, W. M. (2002) *Cultivating Communities of Practice: A Guide to Managing Knowledge*. Harvard Business School Press: Boston, Mass.

Williams, P. A. H. (2007) 'Medical Data Security: Are You Informed or Afraid?', *International Journal of Information and Computer Security*, Vol. 1, No. 4, pp. 414 - 429.

Williams, P. A. H. (2008a) 'How Addressing Implementation Issues Can Assist in Medical Information Security Governance', in N. L. Clarke and S. M. Furnell (editors), *Second International Symposium on Human Aspects of Information Security and Assurance*, Centre for Information Security and Network Research, University of Plymouth: Plymouth, UK.

Williams, P. A. H. (2008b) 'When Trust Defies Common Security Sense', *Health Informatics Journal*, Vol. 14, No. 3, pp. 211 - 221.

Xin,L., Valacich, J.S., and Hess, T.J. (2004) 'Predicting User Trust in Information Systems A Comparison of Competing Trust Models', in *Proceedings of the 37th Annual Hawaii International Conference on Systems Sciences*, 6-9 Jan, Vol, 8,pp. 80259b. IEEE Computing Society.