

Association for Information Systems AIS Electronic Library (AISeL)

WISP 2012 Proceedings

Pre-ICIS Workshop on Information Security and
Privacy (SIGSEC)

Winter 11-14-2013

Information Systems Security: The Role of Cultural Aspects in Organizational Settings

Lena Connolly

National University of Ireland, Galway, y.connolly1@nuigalway.ie

Michael Lang

National University of Ireland, Galway

Follow this and additional works at: <http://aisel.aisnet.org/wisp2012>

Recommended Citation

Connolly, Lena and Lang, Michael, "Information Systems Security: The Role of Cultural Aspects in Organizational Settings" (2013). *WISP 2012 Proceedings*. 30.

<http://aisel.aisnet.org/wisp2012/30>

This material is brought to you by the Pre-ICIS Workshop on Information Security and Privacy (SIGSEC) at AIS Electronic Library (AISeL). It has been accepted for inclusion in WISP 2012 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

Information Systems Security: The Role of Cultural Aspects in Organizational Settings

Lena Connolly¹

National University of Ireland, Galway, Ireland

Michael Lang

National University of Ireland, Galway, Ireland

ABSTRACT

An increasing number of security breaches in organizations present a potentially serious threat to individual privacy and the security of corporate data. Many security breaches happen due to so-called “human error”. Recent research shows that information security culture encourages security-vigilant behaviour of employees and therefore can help to avoid human-related security breaches. The concept of information security culture is relatively new and research on the subject is still in its infancy. In particular, the impact of national culture on information security culture has received very little attention in the literature. Our research-in-progress aims to address this gap.

Keywords: information systems Security, information security culture, organizational culture, national culture, Employee behavior.

INTRODUCTION

Recent research shows that as many as 39% of security breaches happen in organizations due to “human error” (Ponemon Institute 2012, p.7). Unfortunately, the “human error” factor has been largely neglected by many organisations. A lot of organisations believe that technical

¹Corresponding author: y.connolly1@nuigalway.ie.

controls will magically take care of their security problems. As a result, they are investing a lot of time and money into technical tools to protect their valuable information assets while ignoring the “human factor” problem, which often is the very root cause of security breaches. Some contemporary research shows that establishing an organizational information security culture (ISC) can help in addressing the problem of the “human error” with regards to information security (Kraemer and Carayon 2005; Lim et al. 2009). It is only in recent years that the potential value of ISC within an organization gained recognition by Information Systems (IS) scholars as an important aspect in sustaining a sufficient level of IS security in that organization (da Veiga and Eloff 2010). ISC promotes security-cautious behaviour of employees and therefore can help to avoid human-related security breaches. Hence, organizations are encouraged to build a culture of information security in such a way that information security becomes a natural aspect of the daily activities of all employees. Incidentally, in 2012, about 90% of security breaches started with weak authentication or stolen credentials (QuinStreet Enterprise 2013). This trend will obviously continue because it is one of the easiest ways to breach a system.

Government agencies, businesses, and researchers are paying great attention to the issue of information security. Because of the speed with which the technologies have been adapted, it is not surprising that there is a knowledge and skills gap when it comes to IS security. A considerable amount of research has been undertaken in order to fill this gap, but a number of aspects warrant further investigation because the subject of IS security is far-reaching and highly topical. ISC is one such area which remains largely unexplored and as yet not well understood (Chia et al. 2002; Malcomson 2009; Sasse et al. 2007). Prior research on the topic of ISC has a narrow focus and there are many calls for further investigation within this domain. In particular, Sasse et al. (2007) make the point that further investigation is required on how to develop and

maintain a healthy security culture in an organisation. Malcomson (2009) also calls for a wider approach to carry out a study of ISC, and Lim et al. (2009) argue that research on the topic of ISC is limited and they call for more studies in the area of ISC.

The purpose of our study is to integrate models of national, organizational and security cultures as well as behavioural theory and identify factors that promote security-cautious behaviour of employees within organizational settings. Our intention is to explore how these factors interact and influence employee behaviour by seeking answers to the following questions:

- What are the principal factors that impact upon an employees’ behaviour with regards to information security in organizational settings?
- What are the principal factors that influence the information security culture within organisations?
- How do these factors vary between different national cultures?

A high-level overview of the conceptual framework upon which we base our investigation is presented in Figure 1.

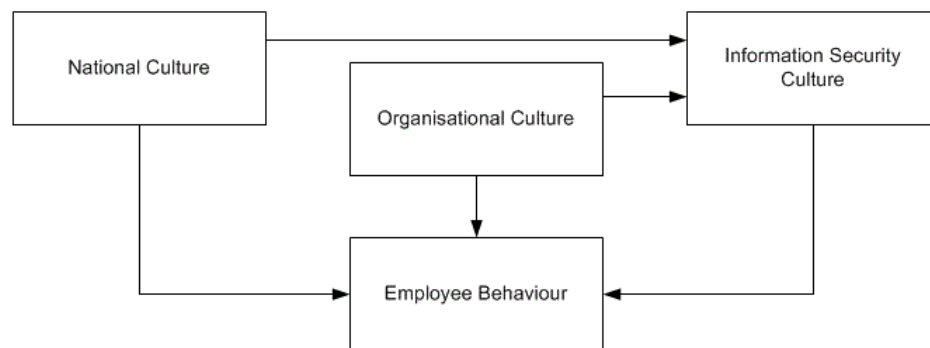


Figure 1. Influence of Culture on Employee Behaviour with regards to Information Security

This paper is organised as follows. It begins with a literature search conducted to shed light on research gaps in the ISC field. Next, a review on ISC is presented including discussion of the relationships between ISC and organizational culture (OC) as well as ISC and national culture (NC). The paper then wraps up by setting forth our main propositions, outlining the planned research approach and future directions, and alluding to some of the limitations and challenges that lie ahead for us.

LITERATURE REVIEW

Literature Search Approach

In order to identify research gaps in the area of ISC, an extensive literature search was carried out. To begin with, suitable publications including journals and conferences were identified. To find appropriate journals, Lamp's Index of Information Systems Journals and various MIS journal ranking indices were consulted. 55 relevant journals were selected, falling into three groups: Top IS journals (e.g. MISQ, EJIS, ISJ), dedicated security journals (e.g. ACM TOIS, J Comp Sec, IEEE Trans IFS), and other respectably ranked journals of relevance to the domain (e.g. IEEE Software, CAIS, CACM, IT&P, I&ST, ACM TOIS). All back issues of these journals were trawled using key search phrases. Additionally, conference paper databases were searched. The Excellence in Research for Australia conference ranking was used to define the quality of a conference; only papers published in A-ranked conferences were considered. Overall, our literature search of relevant journal and conferences identified 105 articles which addressed the topic of information systems security as it relates to OC.

Information Security Culture

In a general sense, ISC can be defined as the “totality of patterns of behaviour in an organisation that contribute to the protection of information of all kinds” (Dhillon 1997, p.59). Malcomson (2009, p.361) asserts that “security culture is indicated in the assumptions, values, attitudes and beliefs, held by members of an organisation, and behaviours they perform, which could potentially impact on the security of that organisation, and that may, or may not, have an explicit, known, link to that impact”. A more comprehensive definition of ISC is that put forward by Da Veiga and Eloff (2010, p.198) as:

“attitudes, assumptions, beliefs, values and knowledge that employees/stakeholders use to interact with the organisation’s systems and procedures at any point in time. The interaction results in acceptable or unacceptable behaviour (i.e. incidents) evident in artifacts and creations that become part of the way things are done in the organisation to protect its information assets. This information security culture changes over time”.

ISC emerges from the way in which people behave towards information and the security thereof (Kraemer and Carayon 2005). ISC in organisations has been explained using theories adapted from various disciplines such as psychology, economics, and management. This is a conventional trend for an emerging discipline. To this point, perhaps the most popular approach in studying the culture of information security within organisations has been the employment of various OC theories and models. By and large, Schein’s (1985) Model of Organizational Culture dominates this trend of research.

For example, Schlienger and Teufel (2002) offer the Three Layers of Security Culture and Their Interactions Framework that assists management in fostering organizational ISC.

Zakaria's et al. (2003) Conceptual Checklist of Information Security Culture Levels has similar purpose, that is developing ISC in organisations. The Information Security Culture Dimensions Framework by Kraemer and Carayon (2005) is utilised to understand and describe ISC. Other ISC frameworks based on the Schein's Model of Organizational Culture include the Theory of Policy Enforcement (von Solms and von Solms 2004), the Theory of Changing Security Culture (Vroom and von Solms 2004), the Outcomes Based Framework for Culture Change (van Niekerk and von Solms 2005), the Information Security Governance Framework (da Veiga and Eloff 2010), and the Framework of Levels of Security Culture (van Niekerk and von Solms 2010). By and large, these frameworks offer mechanisms to create and maintain ISC in organizational settings.

Relationship between Organizational Culture and Information Security Culture

Schlienger and Teufel (2002), Zakaria and Gani (2003) and Zakaria et al. (2003) view the organizational information security culture as a part of OC and argue that ISC shouldn't be studied in isolation from broader OC. For example, Schlienger and Teufel (2002) criticise the technical focus organisationsemphasise as a means to deal with the issues related to information security. In order to improve the overall level of security within organisations, they introduce a paradigm shift – from a technical approach to a socio-cultural approach – that is a focus on OC to address the problem of the “human factor” in information security. Zakaria and Gani (2003) stress that information security is an issue in the entire organizational context, therefore, they attempt to integrate information security field with OC. Zakaria et al. (2003) regard ISC as a subculture of OC.

Several IS scholars draw a tight link between strong OC and a culture of information security in an organisation. Peters and Waterman (1982) explain that in organisations with strong cultures, people mostly know what they are supposed to do, and therefore these organisations don't completely rely on policies, procedures and rules. Therefore, a strong security culture within an organisation would promote security-adequate behaviour of employees without employing radical security compliance measures, such as, for example, punishment.

Dhillon (1997, p.59) relates vulnerabilities of computer systems to "discordance between the organizational vision, its policy, the formal systems and the technical structures". Chia et al. (2002) stress that a development of security policy must be supported by OC. Lim et al. (2009) point out that OC shapes and directs employees' attitude and behaviour; therefore, an understanding of OC may be useful when studying ISC within an organisation.

Relationship between National Culture and Information Security Culture

Various scholars demonstrate a connection between NC and employees' compliance with authority and organizational policies and rules (Hofstede 1980; Spector 1982). The original taxonomy of national culture by Hofstede (1980) consists of four dimensions: power distance, uncertainty avoidance, individualism-collectivism and masculinity-femininity. Power distance shows the degree to which status inequality among workers are pronounced in society. Hofstede (2001) argues that there is a correlation between a country's power distance index and the nature of hierarchies in organisations located within that country. Hierarchy is based on power, control and an authoritarian relationship between management and employees. A leader's authority in bureaucratic organisations is highly proclaimed. Quite commonly, fear is used as a motivating factor in such organisations. Therefore, employees don't tend to break rules or disobey orders out

of fear of the consequences. Johnston and Warkentin (2010) reveal that “fear appeals” impact end-user behavioural intentions to comply with recommended individual acts of security. Boss et al. (2009) conclude that a perception of “mandatoriness” is effective in motivating individuals to take security precautions.

Uncertainty avoidance is “related to the level of stress in a society in the face of unknown future” (Hofstede 2001, p.29). Hofstede (2001, p.147) argues that in countries with higher uncertainty avoidance index, organisations tend to have a greater need for rules and employees strongly believe that company’s rules should not be broken even in the company’s best interests. Therefore, organizational security practices are usually documented in the organisation’s policy. On the contrary, in countries with a lower uncertainty avoidance index, organisations tend to have a more relaxed attitude towards rules.

Furthermore, Rotter’s Theory of Locus of Control of Reinforcement has been widely employed in cross-cultural research. This model includes a single dimension of internal locus of control versus external locus of control (Rotter 1966). People who belong to the internal locus of control category believe that they are in control of their fate, while people who relate to the external locus of control category link their life events to the external environment. Spector (1982) relates the Locus of Control variable to employees’ compliance with authority. He notes that externals have a greater compliance and as a result they are easier to supervise. On the other hand, internals tend to be more independent in their work and don’t appreciate intense supervision.

The importance of NC as a determinant of information systems culture is held up by the aforementioned works. However, as yet, very little cross-national research has been conducted within the domain of information systems security. Given trends such as globally-distributed

teams, offshoring, and cloud computing, there is a need for a broader understanding of differences in information systems security behaviour arising from factors inherent within NC. For example, views on privacy and security of individual data are dramatically different in Europe as compared to the United States (Levin and Nicholson 2005; Zafir 2012). These differences may have significant effect on the stringency of organizational security policies and rules and therefore on employees' behaviour with regards to information security (Boss et al. 2009). Therefore, we submit that NC should be also included in the study of ISC.

Relationship between Culture and Employee Behaviour

Previous research shows an association between different layers of culture, including national, organizational and information security, and human behaviour. For example, Ali and Brooks (2008) define national culture as a shared set of core values, norms and practices in a society that shape the behaviour of individuals within society. Hofstede (2001) compares culture with an onion consisting of multiple layers; values are the inner layer of the onion and the core element of culture. They are invisible until they become evident in behaviour. Furthermore, Hall (1976) and Karahanna et al. (2005) also show an association between NC and individuals' behaviour.

OC researchers, such as Baker (1980); Philips (1984); Kilmann (1985) and Schein (1985) also connect OC and human behaviour. For example, Philips (1984) states that culture is a set of tacit assumptions which guide acceptable perceptions, thoughts, feelings, and behaviour among members of the group. Baker (1980) emphasises the importance of OC as a power that can lead an organisation to success or weaken its vitality because OC directly affects employee behaviour.

Kilmann (1985) identifies culture as a separate and hidden force that controls behaviours and attitudes in organisations.

Finally, there is an abundance of IS research acknowledging the relationship between behaviour and ISC (da Veiga and Eloff 2010; Dhillon 1997; Kraemer and Carayon 2005; Lim et al. 2009; Malcomson 2009; Schlienger and Teufel 2002).

RESEARCH METHODOLOGY

We propose to employ Sequential Exploratory Mixed Method research design, in particular the Instrument Development model as shown in Figure 2.

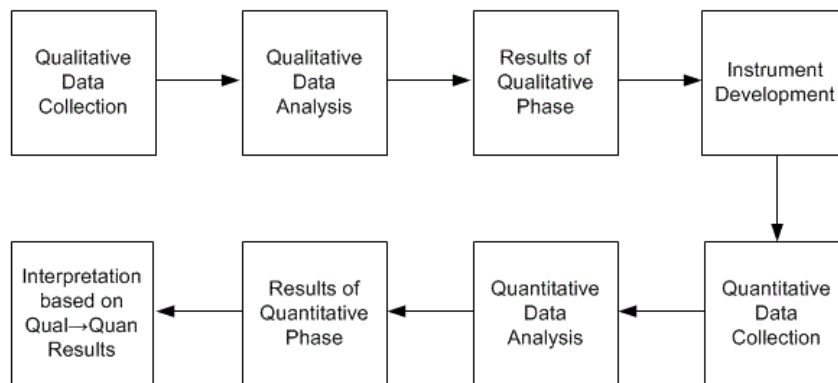


Figure 2. Exploratory Design: Instrument Development Model (Source: Creswell and Clark 2006, p.76)

The intent of this approach is that the results of the first method (qualitative) can help develop the second method (quantitative). This design is particularly useful when a researcher needs to develop and test an instrument because one is not available (Creswell and Clark 2006). Since much of the earlier work in the area of ISC is of a purely theoretical or hypothetical nature as opposed to being based on empirical evidence, survey instruments for the type of study we intend to conduct are not readily available. Therefore, we consider the Exploratory Design,

Instrument Development Model as the most suitable research method. Where applicable, elements of research instruments used in previous studies, such as those based on Hofstede's national culture model, will be adapted.

Our research approach consists of two phases. In the first phase, we will qualitatively explore the research topic through interviews. As is clear from the results of a systematic literature search conducted for this study, research on ISC is still in its infancy. Therefore there is a need to investigate the concept of ISC in depth. Additionally, the qualitative findings then will guide the development of items and scales for a quantitative survey instrument, e.g. a questionnaire.

At this point in time, twenty interviews have been carried out in Irish and US organisations – ten in each country. Data analysis on interviews conducted in the US has begun in June, 2013. The methodology adapted by this study is based on the constant comparative method. The purpose of this approach is to continually compare specific incidents of data in order to develop concepts and integrate them into a coherent explanatory model. The data analysis comprises of nine phases. Phase 1 (Open Coding) involved broad participant-driven open coding of the transcripts from their original chronology into an initial set of codes (32 codes were identified). Phase 2 (Categorisation of Codes) included re-ordering themes identified and coded in phase 1 into categories of themes by grouping related themes under these categories and organising them into a framework that makes sense to further the analysis of the data. The following four broad categories have been identified: culture, employee, factors that influence employee behaviour with regards to information security, and factors that influence information security rules and practices in organizational settings. Phase 3 (Coding on) is currently underway. The agenda of this stage is to break down the categories from phase 2 into sub-

categories to offer clearer insights into the meanings embedded therein. In phase 4 we intend to generate memos against each significant code (or groups of codes) in order to synthesise their content into manageable proportions to facilitate an initial empirical findings report on the data collected. Next, phases 1-4 will be repeated for interviews conducted in Ireland. The subsequent analysis will include phase 5 (Creating Common Framework), phase 6 (Data Reduction), phase 6 (Validation of Analytical Memos), phase 7 (Writing Analytical Memos), phase 8 (Data Validation), and finally, phase 9 (Synthesising Analytical Memos).

Our rationale for choosing Ireland and the US as the two countries for a cross-national comparative study was partly based on convenience, but is also guided by the aforementioned observation that there are significant differences in regulatory environments and approaches towards data protection between the US and Europe. Because many multinational corporations based their European headquarters in Ireland, especially within the ICT sector, the choice of Ireland as a proxy for Europe makes it interesting to compare with the US. This of course is an oversimplification and we intend to expand the study to further include other regions of the US and Europe. We are also considering the possibility of replicating the study in other jurisdictions through links with colleagues in Australia and South Africa.

CONCLUSION AND FUTURE WORK

In the literature, the “human error” factor has been recognized as a root cause of as many as 39% of security breaches in organizations. ISC has been viewed as a means to control “human error”. This research-in-progress is an effort to integrate models of national, organizational and information security cultures, and behavioural theory in order to investigate how organizational and national cultures affect ISC. Additionally, this study aims to build a deeper and richer

understanding of the various factors that influence employee behaviour with regard to IS Security. Since the internationalization of the IT market, the concept of national culture has become a particularly important factor in examining security problems associated with organizational information assets. However, the notion of cross-cultural research has been largely ignored by IS security scholars. Therefore, this study has potential to make a valuable contribution for IS security researchers and practitioners in understanding the nature of organizational security values and behaviours within two heterogeneous cultures. We believe that this is the first study to examine the relationships between ISC, OC, and employee behaviour in two different cultural environments.

Furthermore, this research sets the ground work for a larger scale project where other environments can be considered, including important IT countries in regions such as East Asia, the Indian subcontinent, the Nordic countries, the former Eastern Bloc and so forth. This work may allow us to better model the notion of adversarial behavior in different regions. Thus, from the standpoint of information security, this research has potential to make a crucial contribution to theory and practice.

In terms of shortcomings and limitations, studies that involve culture tend to be rather complex. As Straub et al. (2002) put it, “culture has always been a thorny concept and an even thornier research construct”. Furthermore, studies that include several cultural aspects tend to be even more complex. In particular, it may be hard to separate effects of national and organizational cultures in organizational settings due to similar characteristics. For example, hierarchy in an organization can be a result of a bureaucratic culture of this organization or a societal norm of the country where this organization is located. Quantifying the concept of culture is another challenge that is anticipated in this project. In order to measure culture in a

meaningful way, a value-based approach will be employed. Additionally, a selected research method presents a few challenges; for once it is time consuming. Taking in consideration the aforementioned complexities, we would therefore welcome feedback and suggestions from other researchers who may have encountered this same difficulty or are contemplating similar avenues of enquiry.

REFERENCES

- Ali, M., and Brooks, L. 2008. "Culture and IS: National Cultural Dimensions within IS Discipline," in Proceedings of the 13th Annual Conference of the UK Academy for Information Systems, Bournemouth, United Kingdom, 10-11 April 2008, pp. 1-14.
- Baker, E.L. 1980. "Managing Organizational Culture," *Management Review*, (69:7), July, pp. 8-13.
- Boss, S.R., Kirsch, L.J., Angermeier, I., Shingler, R.A., and Boss, R.W. 2009. "If Someone is Watching, I'll Do What I'm Asked: Mandatoriness, Control, and Information Security," *European Journal of Information Systems* (18), March, pp.151-164.
- Chia, A., Ruighaver, B., and Maynard, B. 2002. "Understanding Organisational Security Culture", in Proceedings of the 6th Pacific Asia Conference on Information Systems, Tokyo, Japan, 2-4 September 2002, pp.1-23.
- Creswell, J.W., and Clark, V.L.P. 2006. *Designing and Conducting Mixed Methods Research*, Thousand Oaks, CA: Sage Publications.
- Da Veiga, A., and Eloff, J.H.P. 2010. "A Framework and Assessment Instrument for Information Security Culture", *Computers & Security* (29:2), March, pp. 196-207.
- Dhillon, G. 1997. *Managing Information System Security*, London, United Kingdom: MacMillan Press Ltd.
- Hall, E.T. 1976. *Beyond Culture.*, Garden City, NY: Anchor Press/Doubleday.
- Hofstede, G. 1980. *Culture's Consequences: International Differences in Work-related Values*, Thousand Oaks, CA: Sage Publications.
- Hofstede, G. 2001. *Culture's Consequences. Comparing Values, Behaviors, Institutions, and Organizations Across Nations*, 3rd ed., Thousand Oaks, CA: Sage Publications.
- Karahanna, E., Evaristo, J.R., and Srite, M. 2005. "Levels of Culture and Individual Behavior: An Integrative Perspective," *Journal of Global Information Management* (13:2), pp. 1-20.
- Kilmann, R.H. 1985. "Managing Your Organization's Culture," *Nonprofit World Report* (3:2), March-April, pp.12-15.
- Kraemer, S., and Carayon, P. 2005. "Computer and Information Security Culture: Findings from Two Studies", in Proceedings of the Human Factors and Ergonomics Society 49th Annual Meeting. Orlando, FL, September 26-30 2005, pp. 1483-7.
- Levin, A., and Nicholson, M.J. 2005. "Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground," *University of Ottawa Law & Technology Journal* (2:2), pp. 357-395.

- Lim, J.S., Chang, S., Maynard, S., and Ahmad, A. 2009. "Exploring the Relationship between Organizational Culture and Information Systems Security Culture", in Proceedings of the 7th Australian Information Security Management Conference, Perth, Australia, 1-3 December 2009, pp. 87-97.
- Malcomson, J. 2009. "What is security culture? Does it differ in content from general organisational culture?", 43rd Annual International Carnahan Conference on Security Technology, Zurich, Switzerland, October 5-8 2009, pp. 361-366.
- Peters, T., and Waterman Jr, R.H. 1982. *In Search for Excellence. Lessons from America's Best-run Companies*, Glasgow, United Kingdom: Caledonian International Book Manufacturing Ltd.
- Phillips, M.E. 1994. "Industry Mindsets: Exploring the Cultures of Two Macro-organizational Setting," *Organization Science* (5:3), August, pp. 363-383.
- Ponemon Institute 2012. *2012 Cost of Cyber Crime Study: United States*. Traverse City, MI: Ponemon Institute. Available online at: http://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FIN_AL6%20.pdf [Accessed 11 January 2013].
- QuinStreet Enterprise 2013. *Targeted Attacks, Weak Passwords Top IT Security Risks in 2013*, QuinStreet Enterprise. Available online at: <http://www.eweek.com/security/targeted-attacks-weak-passwords-top-it-security-risks-in-2013/> [Accessed 12 February 2013].
- Rotter, J.B. 1966. "Generalized Expectations for Internal Versus External Control of Reinforcement," *Psychological Monographs: General and Applied* (80:1): pp.1-27.
- Sasse, M.A., Ashenden, D., Lawrence, D., Coles-Kemp, L., Flechais, I., and Kearney, P. 2007. *Human Vulnerabilities in Security Systems*, White Paper. Cyber Security Knowledge Transfer Networks, Farnborough, United Kingdom: QinetiQ.
- Schein, E. H. 1985. *Organizational Culture and Leadership: The Dynamic View*, San Francisco, CA: Jossey-Bass.
- Schlienger, T., and Teufel, S. 2002. "Information Security Culture: The Socio-cultural Dimension in Information Security Management," in Proceedings of IFIP TC11 17th International Conference on Information Security, Cairo, Egypt, 7-9 May 2002, pp. 191-202. A., Ghonaimy, M.T., El-Hadidi, and H.K., Aslan (eds.). Deventer, Netherlands Kluwer Academic Publishers.
- Spector, P.E. 1982. "Behavior in Organizations as a Function of Employee's Locus of Control," *Psychological Bulletin* (91:3), May, pp.482-497.
- Straub, D., Loch, K., Evaristo, R., Karahanna, E., and Strite, M. 2002. "Toward a Theory-based Measurement of Culture," *Journal of Global Information Management* (10:1), pp. 13-23.
- Van Niekerk, J.F., and von Solms, R. 2005. "An Holistic Framework for the Fostering of an Information Security Sub-culture in Organizations," in Proceedings of the 5th Annual Information Security South Africa Conference, Johannesburg, South Africa, June 29 - July 1, 2005. Available online at: http://icsa.cs.up.ac.za/issa/2005/Proceedings/Full/041_Article.pdf [Accessed 20 June 2012].
- Van Niekerk, J.F., and von Solms, R. 2010. "Information Security Culture: A Management Perspective," *Computers & Security* (29:4), June, pp.476-486.
- Von Solms, R., and von Solms, B. 2004. "From Policies to Culture," *Computers & Security* (23:4), June, pp.275-279.

- Vroom, C., and von Solms, R. 2004. "Towards Information Security Behavioural Compliance," *Computers & Security* (23:3), May, pp. 191-198.
- Zakaria, O., and Gani, A. 2003. "A Conceptual Checklist of Information Security Culture", in *Proceeding of the 2nd European Conference on Information Warfare and Security*, Reading, United Kingdom, June 30 - July 01, 2003, pp. 365-371.
- Zakaria, O., Jarupunphol, P., and Gani, A. 2003. "Paradigm Mapping for Information Security Culture Approach, in *Proceedings of the 4th Australian Conference on Information Warfare and IT Security*, Adelaide, Australia, November 20-21 2003, pp. 417-426.
- Zanfir, G. 2012. "EU and US Data Protection Reforms: A Comparative View", in *Proceedings of the 7th Annual International Conference on European Integration - Realities and Perspectives*, Saint-Etienne, France, May 18-19 2012, pp. 217-223.