Association for Information Systems
AIS Electronic Library (AISeL)

MCIS 2017 Proceedings

Mediterranean Conference on Information Systems (MCIS)

9-2017

Fostering Information Security Culture In Organizations: A Research Agenda

Maria Karyda
Dept. of Information and Communication Systems Engineering, University of the Aegean, mka@aegean.gr

FOSTERING INFORMATION SECURITY CULTURE IN ORGANISATIONS: A RESEARCH AGENDA

Research full-length paper

Track N° 10

Maria Karyda, University of the Aegean, Greece, mka@aegean.gr

Abstract

Information security is a major challenge for organizations due to the proliferation of digitization and constant connectivity. It is becoming widely accepted that raising an information security culture, meaning instilling security behaviour in people interacting with ICTs, is key to maintaining a healthy security posture. However the academic field of information security culture has been described as immature, lacks empirical validation, while the constituents of the concept as well as methods, tools, frameworks and metrics for fostering and evaluating it within organisations remain elusive. This paper, based on a critical analysis of relevant literature and practice, provides a research agenda of critical issues that need to be addressed so that users, from security's weakest link, become an important actor for proactive information security. These issues include the need for proper and employable definitions of information security culture and the need to explore the existence of security subcultures, the need to develop frameworks, tools and metrics for guiding, evaluating and comparing security culture raising programs, the need to explore the interplay between organisational elements (including organisational structure, type and management practices) and security culture, the need to identify the impact of security culture in issues such as innovation adoption, the need to investigate the influence of national and organisational culture on security culture and so on.

Keywords: information security culture, security behaviour, security compliance.

1 Introduction

Information security is one of the biggest challenges of our time. Governments, enterprises and individuals are increasingly reliant on Information and Communication Technologies (ICTs) as digitalization proliferates fast in both private and public sector. Digitalization and constant connectivity have the potential to create economic growth and welfare for enterprises as well as more efficient public services. However, this potential can be limited by an increased level of information security threats. The impact of information security incidents can be very significant for individuals and organisations, in terms of lost revenue, loss of sensitive data, breach of personal data, damage to equipment that is critical for business functions, denial-of-service attacks, network outages and so on. Cyber security incidents, intentional and accidental ones, are already affecting the global economy and security and privacy concerns remain an obstacle to the digitization of businesses and e-government services.

Most organisations follow security management programs and information security policies (ISP) and employ security measures to protect their information and communication infrastructure. Technological advances on the own, however, do not necessarily produce more secure environments. For information security scholars, users, whether intentionally or through negligence, often due to a lack of knowledge, are considered a major threat to information security (Mitnick and Simon, 2002; Theoharidou et al., 2005). Without an adequate level of end user cooperation and knowledge, security controls are liable to be misused or misinterpreted by users, rendering even adequate security measures ineffective (Siponen, 2001). In this context, information security is people-based and any information security strategy needs to comprehensively address the human factor. Social aspects of information security, broadly discussed in literature as information security culture, have been relatively recently included in the information security research agenda (for example Schlienger and Teufel, 2003; Kolkowska, 2011; Vroom and von Solms, 2004; Da Viega and Eloff, 2010; Furnell, 2007; Connolly, 2000; von Solms, 2000).

Currently, several organisations as well as states, attempt to create the ‘right’ mindset of individuals with regard to information security, raising an information security culture. Overall, an information security culture can be considered as the way individuals act with regard to information security, so as to protect information assets and achieve the desired level of security, together with the underlying security perceptions, attitudes, assumptions, norms and values that guide their behaviour. However, the academic field of information security culture remains immature (Karlsson et al., 2014) and organisations lack guidance in fostering it; several issues concerning the creation, adoption and evaluation of an information security culture, as well as its interplay with organisational culture and impact on organisations remain to be addressed.

This paper analyzes extant literature (in the following section) and current practice (in section 3) on information security culture and describes a research agenda (section 4) on critical issues and challenges that need further research. These issues, include, among others, setting criteria for identifying security subcultures, the need to develop frameworks, tools and metrics for guiding, evaluating and comparing security culture raising programs, exploring the interplay between the organisational structure, type and management practices and security culture, the analysis of the impact of security culture on innovation adoption and the need to investigate the influence of national and organisational culture on security culture. Findings of this analysis provide a roadmap for researchers in the effort to explore the issue and provide frameworks, tools and methods that can facilitate raising and sustaining a security culture in organisations and inform security management on issues to take into consideration when designing and implementing security culture programmes.

2 Information Security Culture Background: Related Research

Raising an information security culture in organisations has been the object of several academic studies in the past years (for example Schlienger and Teufel, 2003; Kolkowska, 2011; Vroom and von

Solms, 2004; Da Veiga and Eloff, 2009; Furnell, 2007, 2008; von Solms, 2000); however the academic field of information security culture has been described as immature (Karlsson et al., 2014). It is mostly dominated by research on the relation of security behaviour and ISP compliance and comprises of theoretical approaches and conceptual frameworks aiming to describe a security culture. On the other hand, the critical role of employee's security behavior for the overall security of organisations has been studied in depth (e.g. Albrechtsen and Hovden, 2010; Bulgurcu et al., 2010; D'Arcy et al., 2009; Herath and Rao, 2009b; Sommestad et al. 2014; Pahnila et al., 2013; Vance, 2012), identifying a wide set of factors that shape employee security behaviour, including attributes of the individuals (e.g. perceptions, values, habits, knowledge, security awareness, etc.), as well as conditions of the organizational environment (e.g. availability of resources, organisational commitment, norms etc.) (Topa and Karyda, 2016).

Research on information security culture draws largely on the concept of *organizational culture* and employs culture-related theories developed in other fields, such as management and industrial psychology. Organization culture has been associated with different groupings of individuals (including nations, cities, organizations, work groups, professions, and so on (Yammarino and Dansereau, 2011) and has been associated with information security culture as it may promote or even 'hinder change' (Nosworthy, 2000). The role, however, of organisational culture in shaping information security culture and the impact of the latter remain unexplored.

Several studies on security culture (including the works of Schlienger and Teufel (2005), Vroom and Von Solms (2004), Zakaria and Gani (2003)) base their conceptualizations on models of organizational culture, and particularly on Shein's (1985, 1992) model. Schein (1992) identifies three distinct levels in organizational cultures, starting from the basic *underlying assumptions* which are unconscious and the ultimate source of values and actions, to *espoused values* and finally *to artifacts and behaviours* which are visible and can part of the organizational structure and processes. Research in information security culture has been largely on the assumption that, if managers can predict or control the information security culture(s) of their organization, they can manage the information security of their organization more efficiently (Da Veiga and Eloff, 2009) and focuses mainly on changing employees' basic assumptions and beliefs to align them with security values implemented in information security policies (Vroom and von Solms 2004). Thus, a broad stream of relative research focuses on information security policy (ISP) compliance within organisations; in this direction a security culture has even been described as the '*ideal state of compliance*' (Furnell and Thomson, 2009).

Other scholars consider a security culture as the outcome of employees' interaction with information security controls (e.g. passwords, anti-virus software etc.). Martins and Eloff (2002) and Da Veiga et al. (2007) define information security culture as the information security perceptions, attitudes and assumptions that are accepted and encouraged in an organisation. Dhillon (1997) defines it as the behaviour, values, and assumptions that contribute to the protection of information. For Helokunnas and Kuusisto (2003) security culture is a system in which attitude, motivation, knowledge, and mental models about information security all interact together. Straub (2002), on the other hand, proposes using the theory of social identity for understanding a security culture, as individuals are influenced by different cultures and are expected to be influenced by ethical values, national legislation and the organization setting.

Van Niekerk and Von Solms (2005) defined an outcomes based theoretical framework for information security culture change, in which the introduction of security culture in an organisation starts with top management commitment, identifies current and desired state, includes employee education and evaluates culture change through a set of culture change metrics, using the organisational culture model of Schein (1985). Chia (2002) proposes a set of dimensions for measuring the efficiency of the information security culture, including (a) a belief in the importance of information security; (b) goals, policies, procedures and continual improvement processes; (c) cooperation and collaboration; and (d) attention to auditing objectives and their fulfillment. This approach has, however, been criticized by

Helokunnas and Kuuisto (2002), who emphasize the human aspects of information security. Vroom and von Solms (2004) suggest the establishment of a training culture and cooperation with employees on the basis of the gradual adoption of the organization's security management, individual values and user behavior. Security culture in organizations is generally treated as monolithic, however it has been suggested that different security cub-cultures can co-exist within organizational boundaries. Kolkowska (2011) pinpoints the existence of different security subcultures within the same organization, stemming from the underlying different and even conflicting values.

Research has also explored the challenges and difficulties in raising a cyber security culture in small and medium-sized enterprises (SMEs). These difficulties are largely based on the fact that, typically, SMEs lack resources, time and knowledge needed to foster a security culture (Helokunnas and Iivonen, 2003), they usually lack formal assignment of responsibilities of end users and are more susceptible to national influences, such as changes in legislation (Warren, 2003).

Overall, research on information security culture has primarily addressed the issue at an organizational level (e.g., Da Veiga and Eloff (2009), Malcolmson (2009), Schlienger and Teufel (2003)). Research at the individual level includes the works of Hu et al. (2012), Dugo (2007), McCoy et al. (2009), while Herath and Rao (2009) studied security culture with relation to groups. Finally, research on cyber security culture at the national level is scarce (Furnell, 2008) and has been based on the works of G. Hofstede (1983) who developed an empirical model of dimensions of national cultures and defines culture as "*the collective programming of the mind that distinguishes the members of one group or category of people from another*" (Karlsson et al., 2014)

As the academic field of cybersecurity culture is still immature and mostly comprises of descriptive and theoretical or philosophical approaches, lacking empirical validation (Karlsson et al., 2014), it is difficult for managers and organisations to adopt research results. Moreover, scholar research has yet to address issues such as how social and/or organizational processes form individuals' information security behaviour, the influence of national cultures, how organisations can integrate their organisational culture and security culture, and how to evaluate and measure the security culture of organisations.

3 Information security culture in organisations: current practice

The 2005 OECD survey on "The Promotion of a Culture of Security for Information Systems and Networks in OECD Countries" [1] identified two main drivers which support the development of a security culture at the national level: a) E-government applications and services and b) the protection of national critical information infrastructures. Currently, several countries have compiled cyber security strategy plans, making awareness-raising a starting point for their efforts to implement a culture of security.

The International Telecommunication Union (ITU) considers the creation of an information security culture as an essential approach to cyber security. In its 2011 Cybersecurity Strategy Guide[2] to the UN member States, ITU recommends that countries base their security strategies on their national values, because culture and national interests influence the perception of risk and because a strategy

[1] OECD, "The Promotion of a Culture of Security for Information Systems and Networks in OECD Countries", OECD Digital Economy Papers, No. 102,2005, OECD Publishing, Paris., http://dx.doi.org/10.1787/232017148827

[2] ITU National Cybersecurity Strategy Guide, ITU, available at https://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf

rooted in national values is likely to gain support of stakeholders such as the judiciary and private sector. The ITU Strategy provides companies with principles on coordinating, developing and implementing human capacity so as to build a culture of cybersecurity. It also identifies the need for establishing public-private partnerships in order to promote a security culture, behaviour and tools.

The Brussels-based committee of the International Chamber of Commerce (ICC) and the Federation of Enterprises in Belgium (FEB - Fédération des entreprises de Belgique) have issued a Cyber Security Guide[3] which provides guidelines and checklists to companies on how to protect their information assets, advising companies to enhance their culture, so that they become able to respond to the security challenges of their digital environment. Following the Belgian Cyber Security Guide, corporate management needs to be committed to cyber security and to delegate the responsibility to their management teams and external experts to ensure that cyber security remains a regular topic for the board and that the necessary actions are taken. The Guide also underlines the fact that protecting company information should be everyone’s responsibility and suggests to managers that this should be made tangible to employees at all layers of their company by embedding ‘good security principles’ in the day-to-day work. These principles, according to the Guide, should be common-sense and pragmatic in order to sustain their impact and to allow implementation in both big and small companies avoiding a “one size fits all” approach. In this context, creating the ‘right’ (security) culture should a part of security governance that needs to inspire the desired behaviour and mindset by implementing the appropriate security practices, as by creating the right mindset and effective cyber security skills, people can cease to be the weakest link of information security, and transform into being an asset to it.

Finally, the Belgian Cyber Security Guide informs companies that an adequate cyber security culture can also enable a move into new technologies and foster innovation, as risk aversion would be managed and adequate assessment of the threats of new technologies would be balanced against their potential benefits. It also argues that the company culture can be improved by conducting regularly internal and/or independent assessments and audits, such as penetration testing and intrusion detection, as an open approach to security issues and incidents could signify that people are allowed to make mistakes so they are not afraid to report security incidents when they happen.

The Norwegian Centre for Information Security (NorSIS) realized a project on the Norwegian Cyber security culture[4], aiming to explore and measure the cyber security culture on a national level and create a national metric for cyber security culture, so as to develop effective cyber security practices and improve national cyber resilience. Results of the project were also expected to provide indications on what security regulations the Norwegian consider acceptable and how to implement them. The Study on the Norwegian cyber security culture explored eight core issues to evaluate the national cyber security culture: Collectivism, Governance and Control, Trust, Risk perception, Techno-optimism and digitalization, Competence, Interest and Behaviour. Collectivism signified the degree to which individuals considered themselves part of a greater ‘collective’ e.g. a group, organisation or state. Governance and Control evaluated users’ views on regulation, and especially on governance and control of information and communications technology (ICT). Trust was used to identify to the level of trust users have on governments, organisations and so on. Risk perceptions were associated with the likelihood of risk behaviour of individuals and techno-optimism was employed to explore citizens’ attitudes towards digitalization. Competences depicted citizens’ digital skills whereas Interest identified the level of individuals’ interest in ICTs. The study also explored the behavioural patterns of citizens with

[3] Belgian Cyber Security Guide, available at https://www.b-ccentre.be/wp-content/uploads/2014/04/B-CCENTRE-BCSG-EN.pdf

[4] THE NORWEGIAN CYBER SECURITY CULTURE, NorSIS, Norway, 2016, available at https://norsis.no/wp-content/uploads/2016/09/The-Norwegian-Cybersecurity-culture-web.pdf

regard to cyber security as well as the level and sources of cyber security education received by Norwegian citizens.

A major finding of this study is that cyber security education in Norway, fails, in most cases, to teach citizens the complex interaction between cyber security at the individual and the societal and national level. The study concludes that cyber security culture can be shaped early in life, and calls the Norwegian government to increase its effort to educate the young and ensure that the whole population is properly educated in cyber security. It also argues that the focus on compliance to internal security policies in organisations is not likely to enable individuals become more resilient to cyber security threats outside their businesses area of interest.

4 Identifying challenges for raising an information security culture

An information security culture relates to the security behaviour of people while interacting with ICTs, as well to their views, beliefs and values with regard to cyber security. Relative research and practice include mainly theoretical approaches that fail to provide adequate guidance and adopt a partial approach to the issue. Organisations lack appropriate guidance and tools on how to foster and evaluate a cyber security culture. Current approaches mainly include security awareness programs, education and training; however, as the analysis of relevant literature and practice shows, they fail to address the following issues:

- Different levels of analysis for studying and developing security cultures have been identified including individuals, workgroups or teams that interact on a face to face or virtual basis, larger groups like whole organizations and societies or countries, thus the content of information security culture with regard to different levels of analysis needs to be clarified and properly defined. In accordance, security research and practice needs to develop and validate specific guidelines, practices, and tools that guide and facilitate the establishment and proliferation of information security culture in the context of groups, organisations, including small and medium sized ones.
- Within information security literature, security culture is mostly associated with security behaviour, and in its turn, research in security behavior primarily addresses compliance to security rules and policies. When compliance, however, remains the major objective, the comprehensive goal of raising a security culture is not fulfilled, as compliance is focused on specific topics.
- Relevant research has identified several organisational elements that can influence and shape an information security, including the organisational culture and existing subcultures, business type, the size and structure of the organization, existing norms and values and so on. However, their role with regard to raising and shaping a security culture needs further exploration. For instance, exploratory research is needed to identify if/which different levels or types of information security cultures are desirable, e.g. with regard to government institutions, organisations owning/managing infrastructure of critical importance, such as energy, telecommunications etc. Relative research also lacks theoretical frameworks and methodological tools that allow comparing between the effects of different types or instances of information security cultures.
- Another issue that is yet to be addressed concerns the dynamic interplay between organization culture and security. Relative research argues (Nosworthy, 2000) that an organisation's culture has a strong influence on organizational security, as it may 'hinder change' and ascertain appropriate changes according to critical business processes, however fostering a security culture has also an impact on organisational culture.
- Management at all levels, from tactical to senior, plays a critical role for shaping organisational culture and promoting change. However, responsibilities and agenda on fostering an in-

formation security culture are little explored, e.g. with relation to the effectiveness of practices such as lead by example, exhibiting commitment to security goals, allocating appropriate resources and so on.

- Whereas relevant research adopts theoretical approaches to raising an information security culture, it is necessary to develop tools and metrics for evaluating it. To this direction, in depth surveys and case studies could provide insights with regard to how we can describe, "measure" and evaluate an information security culture.
- The effects of raising an information security culture have not been studied; however, practice suggests that organisations could benefit from it in multiple ways. For instance, the adoption of innovations and new technologies could be facilitated, as a security culture would allow a balanced evaluation of possible threats against anticipated benefits and could mitigate individuals' risk aversion. In this way, organisations could benefit with regard to the adoption of innovations and new technologies; however more research is needed on the issue. Furthermore, there are reasons to believe that people in organisations would report security issues and incidents more openly and voluntarily, which is of critical importance in the advent of regulations such as the European General Data Protection Regulation (GDPR) that comes into force in 2018 and mandates, among others, data breach notification under certain provisions.
- The process of raising a cyber security culture could, if properly managed, function as a self-learning process for organisations, producing valuable insights with regard to organisational values, norms etc. Further research on the topic is needed, as organisations and countries (e.g Uber[5], Cisco[6], Norway, Belgium etc.) are beginning to employ programs on raising a security culture.
- Although security culture in organisations is largely treated in research and practice as 'monolithic' it has been pointed out (Kolkowska, 2011) that different security subcultures can co-exist within the same organisational setting. Thus, we need criteria for identifying and describing them, as well as guidelines on how to raise different security cultures if/when there is a need for it (for instance employees in different departments etc). Although security is everyone's job and it is important that all employees can use their judgment when faced with risk decisions, most organizations do not have one single security culture. It is therefore critical to identify specific roles and responsibilities as well as agendas of issues related to different departments and managerial levels. For instance, the role of middle managers is critical for security, as they often make decisions weighing security risk against potential business gains; on the other hand organisations need to need to support their IT personnel take a more proactive role in security protection. Senior management needs to establish the importance of security and incorporate security to company's vision and mission so as to diffuse the security culture. At the operational level people need to understand the necessity of the change and the importance of cyber security; they also need to be motivated to embrace this change and act towards security goals. All this however, needs to be explored and justified by research, so as to facilitate organisations adopt a security culture that can be sustained.
- Research has identified the role of different Internet cultures (also called cyber cultures[7]) in shaping users' security behaviour. Their impact however, on information security culture, as

[5] https://medium.com/uber-security-privacy/from-the-ground-up-building-product-security-at-uber-59c824eab41c

[6] http://www.cisco.com/c/en/us/about/security-center/establishing-security-culture.html

[7] for instance in UK a recent report has identified that most users in Britain can be grouped into five distinct clusters, or cultures (Cultures of the Internet: The Internet in Britain, Oxford Internet Survey 2013 Report, available at http://oxis.oii.ox.ac.uk/wp-content/uploads/2014/11/OxIS-2013.pdf)

users' attitudes, habits and values with regard to the Internet is related to their cyber security behaviour, has not yet been investigated.

- Another issue that totally lacks research is how current management practices such as outsourcing (e.g. through ASPs etc.) and bring-your-own-device, affect and/or affected by the security culture of an organization. There is no research on the issue, however there are reasons to believe that outsourcing, though a cost effective solution, especially for SMEs, might deprive companies from information technology expertise that would be essential for fostering a security culture. At the same time, employees using their own devices for work and personal purposes would need to align their security behaviour with that of their company.
- Finally, there is little research on the effect of national cultures on information security culture (Furnell, 2008). As individual values and organisational norms are influenced by national cultures, we need to further explore how national characteristics can affect the security behaviour of individuals. There are indications, for instance, that in collectivistic societies, employees are more influenced by the expectations of their peers and superiors, whereas in individualistic ones, they tend to act according to their own interests. In the case of South Korea, for example, employees were found to be motivated to use protective technologies under the influence of their peers and superiors (Herath et al., 2014) while in Ireland employees were reported to tend to break rules in a collective manner (Connolly et al., 2015).

5 Conclusions

Despite the different definitions and approaches used, there is a common understanding that information security culture is related to a shared pattern of values, mental models and activities among users or employees. A security culture it can be studied at different levels of analysis, from the individual to a country. Several studies discuss the issue of information security culture; however the academic field of security culture is still far from mature, as existing research is, to a large extent, mostly descriptive and theoretical or philosophical and lacks empirical validation (Karlsson et al., 2014).

The current challenge is to foster an information security culture that integrates with the organisational culture, so that users' behavior contributes towards the protection of the digital infrastructure and digital risk management and information security becomes a part of their daily activities. However, related research still needs to tackle several aspects of fostering an information security culture, including the influence of organisational culture, structure, size, type and management practices on security culture, the existence of different types of security cultures and subcultures, the role of different managerial levels on raising a security culture, the impact of national cultures, the effects of developing a security culture on organisations, with regard to, for example, adoption of innovations and exploitation of digitization and so on.

Overall, extant literature has yet to address the issue of can organisations integrate organisational culture and organizational behaviour and establish an information security culture that addresses security threats and contributes to the protection of information assets.

Finally, through the analysis of relevant research and practice, this study has also identified that, an information security culture can also affect the merits of digitization, as perceptions of cyber risks and attitudes and knowledge on how to protect the digital environment can facilitate or limit digitalization. This could lead to users and organisations more willing to embrace the possibilities that the technology represents, and, at the same time, limit the deployment of inappropriate or excessive security measures out of fear unnecessary, or out of ignorance. Thus, one of the bigger challenges of implementing an information security strategy is to turn individuals, from security's weakest link, as considered by security researchers and practitioners, to an important actor and ally for proactive cyber security. To this end, this paper has proposed a research roadmap that could lead to an organized and systematic body of knowledge on information security culture in organisations, to be used by organisations to design, implement and evaluate their own security culture programmes.

References

Albrechtsen, E. & Hovden, J.: Improving information security awareness and behavior through dialogue, participation and collective reflection. An invention study. Computers & Security 29(4) (2010) 432-445

Bulgurcu, B., Cavusoglu, H. & Benbasat, I.: Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Quar-terly 34(3) (2010) 523-548

Chia, P., Maynard, S., Ruighaver, A., Exploring organisational security culture: Developing a comprehensive research model. In Proceedings of the IS ONE World Conference, Las Vegas, NV, USA, 4–5 April 2002.

Da Veiga A., Martins N., Eloff J., Information security culture – validation of an assessment instrument, Southern African Business Review, 11(1):146–66, 2007.

Da Veiga, A., Eloff, J.: A framework and assessment instrument for information security culture Computers and Security, 29, 196–207, 2009.

D'Arcy, J., Hovav, A. & Galletta, D.: User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. Information Systems Research 20(1) (2009) 79-98

Dhillon G., Managing information system security, London: Macmillan, 1997.

Dugo, T.M., The insider threat to organizational information security: a structural model and empirical test, http://etd.auburn.edu/etd/handle/10415/1345, 2007.

Furnell S., IFIP workshop – information security culture, Computers and Security, (26):35, 2007.

Furnell, S., Thomson, K., From culture to disobedience: Recognizing the varying user acceptance of IT security, Computer Fraud and Security, 5–10, 2009.

Furnell, S.: End-user security culture: A lesson that will never be learnt?, Computer Fraud and Security, 6–9, 2008.

Furnell, S., Clarke, N., Organisational security culture: Embedding security awareness, education and training. In Proceedings of the 4th World Conference on Information Security Education (WISE 2005), Moscow, Russia, 18–20 May 2005.

Helokunnas, T., Iivonen, L., Information security culture in small and medium size enterprises, in e-Business Research Forum—eBRF 2003; Tampere University of Technology: Tampere, Finland, 2003.

Helokunnas, T., Kuusisto, R., Information security culture in a value net, in Proceedings of the 2003 IEEE International Engineering Management Conference (IEMC 2003), Albany, NY, USA, 2–4 November 2003.

Herath, T., Rao, H., Protection motivation and deterrence: A framework for security policy compliance in organisations. European Journal of Information Systems,18, 106–125, 2009a

Herath, T., & Rao, H.R.: Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decision Support Systems 47(2), 154-165, 2009b

Hofstede, G.,.National cultures in four dimensions: A research-based theory of cultural differences among nations, International Studies of Management & Organization, 13(1-2), pp.46-74, 1983.

Hofstede, G.: Dimensionalizing cultures: The Hofstede model in context, Online Readings in Psychology and Culture, 2(1). http://dx.doi.org/10.9707/2307-0919.1014, 2011

Hu, Q., Dinev, T., Hart, P., Cooke, D.: Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture, Decision Science, 43, 615–660, 2012.

Karlsson, F., Åström, J., Karlsson, M.: Information security culture: State-of-the-art review between 2000 and 2013, Information and Computer Security, 2014.

Kolkowska, E. Security Subcultures in an Organization - Exploring Value Conflicts, ECIS 2011 Proceedings. 237, http://aisel.aisnet.org/ecis2011/237, 2011.

Malcolmson, J.: What is security culture? Does it differ in content from general organisational culture?, 43rd Annual 2009 International Carnahan Conference on Security Technology. pp. 361–366. IEEE, 2009

Martins, A., Eloff, J., Information Security Culture. In Proceedings of the IFIP TC11 17th International Conference on Information Security (SEC2002), Cairo, Egypt, 7–9 May 2002.

McCoy, B., Stephens, G., Stevens, K.: An Investigation of the Impact of Corporate Culture on Employee Information Systems Security Behaviour, in Proceedings of ACIS, 2009.

Mitnick K. and Simon W., The art of deception: controlling the human element of security, Wiley Publishing, 2002.

Nosworthy, J. Implementing Information Security in the 21st Century – Do You Have the Balancing Factors? Computers and Security 19(4): 337-347, 2000.

Pahnila, S., Karjalainen, M. and Siponen, M.: Information Security Behavior: Towards Multi-Stage Models. PACIS, 2013.

Schein E., Organizational Culture and Leadership (2nd ed., San Francisco: JosseyBass, 1992.

Schein E., Organizational culture and leadership. San Francisco: Jossey-Bass, 1985.

Schein, E.: Coming to a new awareness of organizational culture, Sloan Management Review, 25, 1984.

Schlienger T., Teufel S. Tool supported management of information security culture, in Proceedings of the 20th IFIP international information security conference, Japan, 2005.

Schlienger, T., Teufel, S., Information security culture—From analysis to change, in Proceedings of the 3rd Annual IS South Africa Conference, Johannesburg, South Africa, 9–11 July 2003.

Siponen M., Five dimensions of information security awareness, Computers and Society, 24–9, 2001.

Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J.: Variables influencing information security policy compliance: a systematic review of quantitative studies. Information Management & Computer Security 22(1), 42-75, 2014.

Straub, D., Loch, K., Toward a theory-based measurement of culture, Journal of Global Information Management, 10, 13–23, 2002.

Theoharidou M., Kokolakis S., Karyda M. and Kiountouzis E., "The insider threat to Information Systems and the effectiveness of ISO 17799", Computers and Security Journal, Vol. 24, No 6, pp. 472-484, Elsevier, 2005.

Topa, I., Karyda, M., Analyzing Security Behaviour Determinants for Enhancing ISP Compliance and Security Management, 13th European, Mediterranean and Middle Eastern Conference on Information Systems (EMCIS), Krakow, Poland, 2016.

Van Niekerk J., Von Solms R. A holistic framework for the fostering of an information security subculture in organizations, in Proceedings of ISSA 2005, 4th Annual Information Security South Africa Conference, 2005.

Van Niekerk, J.C.; Von Solms, R., Establishing an information security culture in organisations: An outcomes-based education approach, in Proceedings of the ISSA 2003:3rd Annual IS South Africa Conference, Johannesburg, South Africa, 9–11 July 2003.

Vance, A., Siponen, M. & Pahnila, S.: Motivating IS security compliance: insights from habit and protection motivation theory. Information & Management 49(3), 190-198, 2012.

Vroom C., Von Solms R., Towards information security behavioural compliance, Computers and Security, 23(3):191–8, 2004.

Warren, M., Australia’s agenda for E-security education and research, in Proceedings of the TC11/WG11.8 Third Annual World Conference on Information Security Education (WISE3), Naval Post Graduate School, Monterey, CA, USA, 26–28 June 2003.

Zakaria, O., Gani, A., A conceptual checklist of information security culture. In Proceedings of the 2nd European Conference on Information Warfare and Security, University of Reading, Reading, UK, 30 June–1 July 2003.