European Journal of Business and Management
ISSN 2222-1905 (Paper) ISSN 2222-2839 (Online)
Vol.6, No.38, 2014
www.iiste.org

# Information Security Subcultures in Information Security Management: A Conceptual Framework

Daniel Muendo
Department of Management Science, University of Nairobi,P.O. Box 30197, Nairobi, Kenya
E-mail: dkmuendo@gmail.com

**Abstract**
The rationale behind an organization's information system is to provide access to its information resources and services anywhere anytime over networks. This need creates issues of security in the management of the information systems. The information system approach is socio-technical by nature, involving people and processes as well as technologies; hence, the culture and characteristics of the organization are factors in effective information security management. This implies that the concept of information management is multi-dimensional and includes the human, organizational and technological dimensions. Stemming from this information security culture is considered as an important factor in the management of information security in an organization by overcoming the problem with employees' lack of compliance with information security management initiatives. However the security culture of an organization is based on the different security subcultures of different sections or subsections that have its basis on the training backgrounds of the individuals and or different tasks performed by each of the groups or a combination of both. This paper addresses information security from the management point of view paying close attention to the information security subculture as seen in the organizations and looks into different methods that the security subcultures can be studied in relation to information security management.
**Keywords:** Information security management system, organizational culture, information security culture, information security subculture.

## 1. Introduction

Organizations today transact in a worldwide setting which enables them to work in partnership and share information resources with one another but conversely exposes them to many threats both within and without the organization, thus the need to secure their information assets. The human element is fundamentally at the center of ensuring the safeguarding of an organization's information resources through their behavior when interacting with information and information systems. Through the establishment of information security policies, management requires employees to act in a secure manner and consequently protect information assets. However, employees are known not to adhere to the security policies, leading to security breaches (Vroom & von Solms, 2004; Kolkowska, 2009). To mitigate the risk posed by the non-adherence of employees to security policies researchers suggest the development of a culture of information security (information security culture) (Thomson,2009), based on information security practices which should be an integral part of every employee's daily work routines and organizational systems (Schlienger & Teufel, 2002).

Martins & Eloff (2002) believe that information security culture is concerned with what is acceptable and what is not acceptable in relation to information security. Thus, the absence of a proper information security culture will increase the inherent risks of inconsistent employee security behavior with regard to the information assets handling activities of organizations. Researchers in organizational culture emphasize that organizational culture may vary across different groups within organizations (Jermier, Slocum et al. 1991). Analogously, the information security culture of an organization may vary across different groups such as managers, IT-professionals, administrators, accountants and any other employees within one organization. Thus, the purpose of this paper is to establish the existence of different information security subcultures in an organization and propose a conceptual framework.

## 2. Literature Review

### *2.1 Information Security Management Practices*

Information security management (ISM) is "a systematic approach to encompassing people, process and information technology systems that safeguards vital systems and information protecting them from internal and external threats" (Barlette & Fomin, 2008). The overall goal of ISM is the prevention of damage to organizational information assets. The management aspect of information security deals with issues of top management's support, addressing the need to support the campaign for certain standards and codes of conduct which are used to apply measures and controls based on the organizational and formal regulations aspect. Moreover, (Chia, Maynard et al. 2002; Ruighaver et al. 2007) also agree that establishing and socializing organizational culture and norms is essential for employees' adaptation to attempts that reinforce controls using informal communication and security awareness among social agents.

 

Emanating from the management wave of information security, information security standards are well represented in the relevant literature (Saint-Germain, 2005; Von Solms, 2005). Their usefulness lies more in their nature of providing guidelines for application. Sometimes conformance to best practices is assumed to give a competitive advantage and some governmental organizations even require it. In general, these standards have been developed through the experiences of leading technological countries. The aim of research on information security management carried out at the micro organizational level (Ruighaver et al., 2007) has been to identify relevant practices of information security management on an organizational basis.

Eloff and Eloff (2003) state that the process of ISMS consists of two phases, namely, planning and then implementing information security management practices for establishing and maintaining information security. According to (Von Solms, 2005), ISMP consists of, obtaining clear direction from guidance available in security standards or codes of practice which include assessment of various potential risks to the information, formulation of a risk management strategy resulting in the identification and implementation of physical, technical and operational security controls, staff training in security practices, testing the security infrastructure, detecting and responding to security incidents, auditing the security function and reporting to the board on its effectiveness, case in point ISO/IEC 27001:2005 (ISO/IEC 27001, 2005) which adopts a process approach for implementing information security management practices in the organization. This process approach consists of the Plan-Do-Check-Act (PDCA) model.

*2.2 Organizational Culture and Subcultures*

This section looks at different aspects of organizational culture including its concepts, definitions, its importance and components, examining the key studies conducted in this area, analyzing the philosophical underpinnings of such studies as well as by discussing the conceptual development of the organizational culture construct. The concept of culture has no two theorists or researchers defining culture in the same way (Denison & Mishra, 2000). Culture is defined differently, measured differently and evaluated differently (Schein, 1985). This lack of agreement on the construct of culture has resulted in a great deal of argument and debate (Mathew, 2007), leading to many different definitions and perspectives on the subject. Following the same some define organizational culture as the observable behavioral rules in human interaction (Van Maanen, 1979); some as the dominant values in an organization (Deal & Kennedy 1982); yet others as a consistent perception within an organization (Robbins, 2001). One of the most common definitions of organizational culture includes shared values, beliefs, or norms (Barney 1986; Kerr 1991; Martin 2002). In other literature it is seen as the personality of the organization (Robbins, 2001). As a summary, Saxena (2000) stated that organizational culture can be defined as 'philosophies and values shared by the members of organizations and their behavioral patterns for translating them into practical actions'. But the most often referred to definition of organizational culture was devised by Schein (1985, 1992), and also which in literature is most widely accepted (Huczynski & Buchanan, 2001).

The strength of an organization's culture is observed through the socialization of new members (Van Mannen & Schein, 1979). Socialization is a process that continues throughout an individual's association with an organization, because as an organization changes and develops, individuals need to adapt to new changes. Individuals are most aware of the socialization process when they first join a company or are shifted to different departments or teams (Feldman & Brett, 1983). In essence, socialization can be viewed as a form of organizational integration (Ivancevich et al., 2000). Organizations with strong cultures are considered to operate under a cohesive set of values and norms (George & Jones, 1996). These values and norms unite team members together and generate a commitment from employees to achieve organizational goals (George & Jones, 1996). In weak cultures, minimal direction and guidance is provided to employees, and in these environments it is the formal organizational structure that guides behavior, rather than values and norms (George & Jones, 1996). Organizational Culture is certainly not a uniform phenomenon and within a culture, subcultures can also exist (Hampden-Turner, 1990). Several writers have emphasized that organizational subcultures may exist independently of organizational culture, and that a small work group may have its own distinct set of values, beliefs and attributes (Brown, 1995; Martin, 1992; Martin and Siehl, 1983; Schneider, 1990; Sackman, 1991; Trice and Beyer, 1993). Brewer (1993) further suggested that if an organizational culture is not articulated strongly enough, the subculture may take precedence over the organizational culture for individual employees and thus gain their commitment.

*2.3 Information Security Culture*

Information security culture in organizations has been explained using theories adapted from various disciplines such as psychology, economics, and management. To this end, possibly the most popular approach in studying the culture of information security within organizations has been to employ various organizational culture theories and models due to the view that a security culture is a part of organizational culture, by and large, Schein's (1985) model of organizational culture being the most common.

 

Information security scholars draw an association between organizational culture and a culture of information security in an organization. For example Peters & Waterman (1982) explain that in organizations with strong cultures, people mostly know what they are supposed to do, and therefore these organizations don't completely rely on policies, procedures and rules. Therefore, strong security culture within an organization would promote security competent behavior of employees without employing radical security compliance measures, such as, for example, punishment. Dhillon (1995) describes information security culture as "the totality of human attributes such as behaviors, attitudes, and values that contribute to the protection of all kinds of information in a given organization" is generally accepted in the field, and is also consistent with the concept of culture, Schlienger & Teufel (2002) emphasize the importance of a strong organizational culture to create a culture of information security in an organization. Yet others intimate that information security culture emerges from the way in which people act towards information and the security thereof (Kraemer & Carayon 2005), Lim et al. (2009) point out that organizational culture shapes and directs employees' attitude and behavior; therefore, an understanding of organizational culture is crucial when studying security culture within an organization.

An information security culture needs to be available at different levels in an organization including individual level, group level and organizational level. As indicated in the information security model, each of the three levels incorporates different key issues (Martins, 2008). At organizational level: policy and procedures, benchmarking, risk analysis, and budget are the key issues. At group level management: trust; and at the individual level awareness and ethical conduct are the key issues. In the organizational context, when the three layers are consistent with each other, there is an integrated culture (Martin, 1992). Martin further puts forward that organizations may have differentiated or fragmented cultures. The differentiation or fragmentation may be the result of differences in cultures across groups in an organization. Alternately, there may be discrepancies in the culture reflected in the various layers of Schein's model. Often, espoused culture, i.e., culture as reflected in the stated beliefs of organizational members, may vary from enacted culture, i.e., culture observed in the behaviors of the organizational members. The difference between espoused and enacted cultures is referred as to action inconsistency (Martin, 1992). In summing up, it is clear that researchers in organizational studies have challenged the traditional rigid view of organizational culture as a single monolithic culture and have begun adopting a more relaxed view of organizational culture as a collection of subcultures.

*2.4 Information Security Subcultures*

Information security culture is ideally considered in the singular, but the literature suggests the reality is more complex. It may nest other subcultures, which vary between organizational units. Moreover, not only can security perception vary between these subcultures, but members of the subcultures can affect security controls based on their perception of other subcultures' security perceptions. According to Schlienger & Teufel (2003), information security culture is defined by defining organization culture; organization culture is defined by how an employee sees the organization. It is collection phenomenon that grows and changes over time and, to some extent; it can be influenced by the management. In the same way information security culture has different subcultures based on sub-organizational departments and or functions. Information security subculture is a culture in regard to the organizational information security culture. It should support all activities so that information security becomes a natural aspect in the daily activities of every employee.

Differentiation in cultures across sub-organizational groups has been reported in research (Boisnier & Chatman, 2002). Boisnier & Chatman, (2002) note that the culture consists of a "set of taken-for-granted, emotionally charged beliefs, called ideologies", identified with that particular subgroup. It has values and beliefs that are tacit. In contrast, the explicit and easily observable parts of the subgroup culture are the artifacts, which are mechanisms by which members express and affirm their beliefs. Some of the subgroup artifacts include subgroup-based myths, ceremonies, symbols, languages and gestures, physical artifacts, sagas and legends, rituals, taboos and rites. As individual members of the subgroup express the underlying ideologies through various cultural forms and interact with other members, the ideologies tend to evolve and add new beliefs and values back into the system. Additions of new ideology and cultural forms help in the enrichment and expressiveness of the culture, but also complicate culture by making it fuzzy. Further, the differences in these subcultures are often the potential source of conflicts (Rao & Ramachandran, 2011), and as a result warrant attention in organizations.

There have been few studies focused on the understanding and characterization of information systems subculture. Among these Schein (1985), Bahn (1995) and Iivari & Abrahmsson (2002) limit their focus to only particular subgroups of members in information systems, whereas Guzman and associates have looked at a broader group of information systems experts (Guzman, Stanton, Stam, Vijayasri, Yamodo,Zakaria and Caldera 2008). Schein (1985) briefly points out that data processing group have their own attitudes, beliefs, patterns and vision about the utilization and importance of technology. Rao & Ramachandran (2011) have also reported differences in security cultures of subgroups outside the context of a single organization. Thus, the security subcultures in an organization are likely to be subject to both career and organizational influences among others

 

and have an effect in the overall management of information security in the organization.

**3.0 Theoretical Underpinnings**

This section will review the key theories that that form the foundation of a study of information security subculture starting with Structuration theory, Actor Network Theory and finally Emergence theory. Structuration theory (ST) by Giddens is a general theory of social organization rather than a theory specific to the IS, but it has been used widely in the IS literature to discuss the about the relationship between technology and organization (Orlikowski, 2000).

Information security management having both social-technical dimensions, ST attempts to offer a middle way between the two competing positions. On one hand, functionalism dictates that objective external social structures act on passive human agents. On the other, interpretive tradition sees society as an effect of human agency. In ST, there is a view of social structure being produced by and acting back on the agents who are the subjects of that structure which they instantiate through their establishment of it (Jones et al. 2004). Both in information security management and organizational culture ST has been used to integrate the two traditional research approaches. It bridges the gap between the quantitative and qualitative studies through the conceptualization of structure the rules and resources used by people in their interaction. Thus, ST is not used as an alternative approach, but a sort of conciliatory approach which reconciles the two conflicting traditional perspectives. Accordingly it does not substitute the old perspectives, instead it helps to acknowledge and connect them at a higher level of abstraction. Other authors share the same view. Martin (1992, 2008).

The key benefit derived from the use of this theory is that it attempts to offer a middle way between two competing positions in social theory in the case of information security management the social and the technical aspects of information security, thus can be referred to as meta-theory. Nevertheless, what is missing from structuration theory are concepts that allow the interrogation of the relationship between individuals and technology. It appears that such concepts can be found within actor network theory (ANT). ANT is largely concerned with the interactions between technology and individuals. According to some of the most prominent interpretive researchers in IS, ANT contains a wealth of concepts for understanding the relationship between technology and individuals, such as actors, networks, the process of inscription, and reconfiguration (Monteiro, 2000). They maintain that addition of these concepts will allow for the further theoretical development for the interplay between technology and the social.

ANT offers a language of analysis that sensitizes us to new ways of understanding. The difference in opinion between the social and the technical is solved by the perception that both are intertwined. Moreover, ANT does not reduce a priori information security implementation to simplistic factors, but it is able to analyze it in all its complexity. It cuts across economic, political, strategic, social and technical issues related to information security implementation and allows for making sense of the unfolding implementation process (Monteiro, 2000). Though still a growing theory in IS research compared with ST, ANT has already demonstrated huge potential in information systems research and thus could be applied in ISM.

In comparing these two theories, some researchers have argued that the different and incompatible treatment of agency is irreconcilable (Rose et al., 2005). They argue that neither ST nor ANT offers a particularly convincing account of the interaction of humans and technology, and that their different accounts of agency make them hard to integrate in any meaningful way. Some researchers suggest that ST exaggerates the role of human agency in creating and producing its context. Proponents of ANT perceive the context to be both social and material, which is a hybrid of both human and non-human actors. Advocates of ST argue that human and non-human agency cannot be labeled as equivalent. However, despite the issue of agency, Walsham (2002) made a valuable contribution by combining these two theories in the same case, using ST to guide broader social analysis, and ANT to describe the detailed socio-technical processes that took place. ANT not only provides theoretical concepts as ways of viewing elements in the real world, it also suggests that it is exactly these elements which need to be traced in empirical work. (Walsham 1997). ANT provides a study of social constructivism by attending to power strategies and networks of human and non-human actors. The glue that holds the actor network of IS together is the power to have strategic control of the IS processes by professionals and the way technological solutions inscribe organizational behavior. Unfortunately the socio-material approach implemented by both ST and ANT does not deal with the complexities created by the interaction between information security and subculture, since the emergent information security subculture is a new entity.

*3.1 Emergence Theory*

Critical realism has become an important perspective in modern philosophy and social science (Robson 2002), but critical realism has to a large extent been absent in IS research. Information systems research based on the principles and philosophy of critical realism overcomes some of the problems associated with “traditional” information systems research approaches. Critical realism’s statement of belief is to identify the reality of the natural order and the events and discourses of the social world. It holds that “we will only be able to understand

 

and so change the social world if we identify the structures at work that generate those events and dialogues. These structures are not spontaneously obvious in the observable pattern of events; they can only be identified through the practical and theoretical work of the social sciences." (Bhaskar, 1989).

Smith (2010) notes that emergence points to the process of constituting a new entity with its own characteristics through the interactive permutation of other, different entities that are essential to create the new entity but that do not contain the characteristics present in the new entity. Emergence involves the following: First, two or more entities that exist at a "lower" level interact or combine. Second, that interaction serves as the basis of some new, real entity that has existence at a "higher" level. Third, the existence of the new higher-level entity is fully dependent upon the two or more lower-level entities interacting, as they could not exist without doing so. Fourth, the new, higher-level entity nevertheless possesses characteristic qualities that cannot be reduced to those of the lower-level entities that gave rise to the new entity possessing them. When these four things happen, emergence has occurred and the new whole entity is more than the sum of its constituents.

Elder–Vass (2010) introduced the relational emergence theory based on the philosophy of critical realism. He provides a general ontological framework to discuss the social structures and human individuals as entities with emergent properties which determine the social events. An entity is a 'whole', which consists of parts structured by means of the relations among each-other. Emergent entities possess some properties produced by mechanisms which depend on the properties of individual parts and the way the parts are structured in order to form the entity (whole). The properties which derive from the entity are not possessed by its individual parts. The way the parts are related at a certain point in time will depict the joint effect they will have. Therefore the relation between the entity and its parts is not of causation, but of composition (Elder-Vass 2010).

The importance of the interactions between the parts is expressed by Holland (1998) as: Emergence is above all a product of coupled, context-dependent interactions. Technically these interactions, and the resulting system, are nonlinear: The behavior of the overall system cannot be obtained by summing the behaviors of its constituent part, the whole is indeed more than the sum of its parts. However, we can reduce the behavior of the whole to the lawful behavior of its parts, if we take the nonlinear interactions into account. There are some elements which an emergent entity should have (Elder-Vass, 2010). First of all, the different parts which an emergent entity consists of should be recognized. The relationships between the parts which cause this type of entity should be identified. Based on the emergence theory an emerging entity will arise which will be a combination of information security, and organizational subculture are part of the constitution of the new entity. Information security management should thus embrace a holistic perspective considering information security subculture as one entity. Thus emergence theory would be a better lens into looking into the concept of information security subculture since in its constitution, all it parts are considered as whole parts themselves but also emergence theory allows the new entity to exist on its own as a whole, more than just a summation of its constituent parts. Its applicability for situations like an emerging information security subculture the relevance is clear, as it would be able to work through the complexities.

## 4.0 Methodology

In order to accomplish the purpose of study of identifying a conceptual framework to investigate the effect of information security subcultures on information security management, a comprehensive literature review was carried out and it was mainly based on academic journals under both information security management and culture literature. According to Hopayian (2001) and Ngai et al.(2009), a systematic review approach and content analysis are strongly recommended for writing concept or review papers. Therefore, a systematic searching approach was followed and finally, a content analysis was performed to identify the theoretical concepts and supported empirical findings in achieving the purpose of the study.

## 5.0 Proposed Conceptual Framework

The conceptual framework presented is developed from the literature review and it depicts how the study has been developed. The framework contains the conceptual model which schematically shows the expected relationships between the different constructs as found in literature. Based on the emergence theory (Eldar-Vass, 2010) which describes the constitution of new entities based on interactions of entities at different levels. At the lowest level, there is interaction between organizational culture and information security measures to form information security culture. Level two interaction is between organizational subculture and information security culture. The resultant entity information security subculture, a new entity with its own characteristics. As an entity information security subculture is fully dependent on lower level entities, it possess characteristic qualities that cannot be reduced to those of the lower level entities that gave rise to the new entity; information security subculture is a whole entity on its own more than the sum of its constituents. The relationship between these entities and the effectiveness of information security management will be evaluated using this conceptual framework.

 

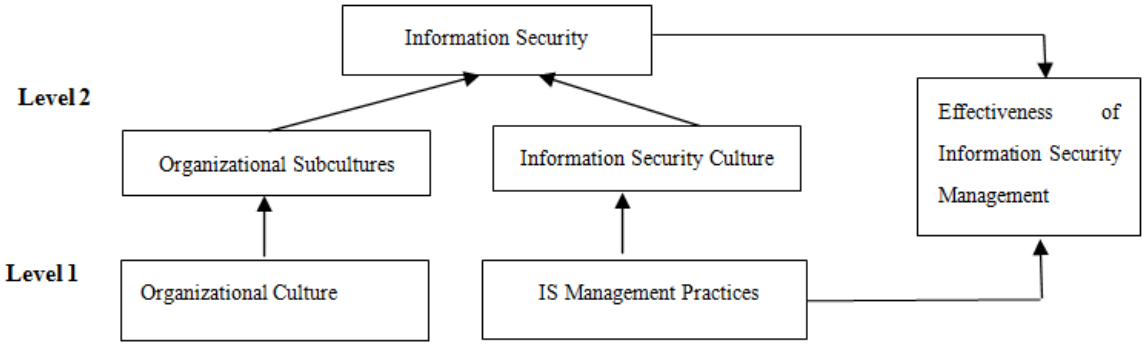


Figure 1: Conceptual Framework

## 6.0 Conclusion

The objective of this study was to identify information security subculture as a basic non-technical factor in information security management and propose a framework for its study. According to data presented by review of current approaches in regards to information security management, and by putting together the literature on information security management in organizations, differences in subcultures across organizations have been reported in the organizational culture literature. An understanding of these differences is important to understand the effects of subcultures. This argument can be extended to the area of information security, the argument that it is necessary to examine the information security subcultures in various organizations to identify differences that might exist, so that they may be taken into consideration in formulating initiatives to enhance information security management. Having established information security subcultures in literature, the researcher generated the above conceptual framework that will assist in empirically establishing the role that is played by information security subcultures in the management of information security in organizations.

## References

Barlett, Y. & Fomin, V.V. (2008). "Exploring the Suitability of IS Security Management Standards for SMEs", in *Proceedings of 2008 Hawaii International Conference on System Sciences,* Hawaii, USA.

Bhaskar, R. (1989) *Reclaiming Reality,* Verso, London.

Birch, D. & McEvoy, N. (1992), Risk Analysis for Information Systems, *Journal of Information Technology*, 7, pp. 44-53.

BIS (2012). 2012 *Information Security Breaches*, Department of Business, Innovation and Skills, UK.

Boisnier, A. & Chatman, J.A.(2002) Cultures and Subcultures in Dynamic Organizations, in: *The Dynamic Organization,* R. Peterson, and Mannix, E. (2ed.), Lawrence Erlbaum Associates,Mahwah, NJ, pp. 87-114.

Brown, A, (1995), Organisational culture, *Pitman*, London.

Burrell, G. & Morgan, G. (1979*), Sociological Paradigms and Organizational Analysis*, London: Heinman.

Chia, P. A., S. B. Maynard, et al. (2002). Exploring Organizational Security Culture.*6th Pacific Asia Conference on Information Systems*, Tokyo, Japan, 2-3 September 2002

Deal, T. & Kennedy, A. (1982). *The New Corporate Cultures – Revitalizing the Workplace after Downsizing, Mergers and Re-engineering*. London: Texere Publishing Ltd.

Denison, D. R. & Mishra, A. K. (2000). Towards a theory of organizational culture and effectiveness. *Organization Science* 6(2), pp. 204-215.

Dhillon, G. (1995). *Interpreting the Management of Information Systems Security.* London: London School of Economics and Political Science.

Dhillon, G. & Backhouse, J. (2001). Current directions in IS security research: towards socio-organizational perspectives. *Information Systems Journal,* 11(2):127-153.

Dhillon, G., Tejay, G., & Hong, W. (2007). Identifying governance dimensions to evaluate information systems security in organizations. *Proceedings of the 40th Annual Hawaii International Conference on System Sciences (HICSS'07), comuter security, IEEE.*

Dhillon, G. & Backhouse, J. (2001), Current directions in IS security research: towards socio -organizational perspectives, *Information Systems Journal*, 11, pp. 127-153.

Elder-Vass D. (2010) *The Causal Power of Social Structures: Emergence, Structure and Agency*, Cambridge University Press, New York.

Feldman, D.C. & Brett, J.M. (1983). Coping with new jobs: A comparative study of new hires and job changers. *Academy of Management Journal*, *26(2)*, 258-272.

George, J.M. & Jones, G.R. (1996). *Understanding and Managing Organizational Behavior*. Reading, MA: Addison-Wesley Publishing Company.

 

Guzman, I. R., K.R. Stam, & J.M. Stanton (2008) "The Occupational Culture of IS/IT Personnel within Organizations," *The DATA BASE for Advances in Information Systems*, 39(1),pp. 33.
Hampden-Turner, C. (1990). *Corporate Cultures: From vicious to virtuous circles.* London: Random House.
Hirschheim, R., & Klein, H.K. (1989), Four Paradigms of Information Systems *Development, Communications of the ACM*, 32(10), pp. 1199-1215.
Holland J.H. (1998) *Emergence: From chaos to order*, Oxford: Oxford University Press.
Hopayian, K. (2001). The need for caution in interpreting high quality systematic reviews. Education and debate, 323, 681-684.
Ivancevich, J., Olekalns, M. & Matterson, M. (2000). *Organisational Behaviour and Management.* Sydney: McGraw Hill.
Iivari, N.& Abrahamsson, P. The Interaction Between Organizational Subcultures and User Centered Design – A Case Study of an Implementation Effort, *Proceedings of the 35th Hawaii International Conference on Systems Sciences,* Hawaii, 2002.
Jermier, J. M., J. J. W. Slocum, et al. (1991). Organizational Subcultures in a soft Bureaucracy: Resistance Behind the Myth and Facade of an Official Culture. *Organization Science*, 2(2), 170-194.
Jones, M., W. J. Orlikowski, & K. Munir (2004) Structuration Theory and Information Systems: *A Critical Reappraisal, in J. Mingers and L. Willcocks (Eds.) Social Theory and Philosophy for Information Systems,* Chichester, UK: John Wiley & Sons, Ltd, pp. 297-328.
Kolkowska, E. (2009). A Value Perspective on Information System Security - Exploring IS security objectives, problems and value conflicts, Orebro University, Orebro, lic thesis.
Kraemer, S. & Carayon, P. (2005) Computer and Information Security Culture: Findings from Two Studies. *Proceedings of the Human Factor and Ergonomics Society 49th Annual Meeting.*
Lim, J. S., Chang, S., Maynard, S. B., & Ahmad, A. (2009). *Exploring the Relationship between Organizational Culture and Information Security Culture.* In 7th Australian Information Security Management Conference, SECAU Security Congress 2009, Perth, Western Australia.
Martin, J. 2002. *Organisational Culture: Mapping the Terrain*. Thousand Oaks, CA: Sage.
Martins, A. and Eloff, J.H.P. 2002. "Information Security Culture" in *Proceedings of the International Conference on Information Security*, Cairo, Egypt.
Martins, A. (2008). Information security culture; DigiSpace at the University of Pretoria: University of South Africa.
Mathew, J. (2007). The relationship of organizational culture with productivity and quality: a study of Indian software organizations. *Employee Relations* 29(6), pp.677-695.
Mishra, S. & G. Dhillon (2006). Information systems security governance research: a behavioral perspective. *9th annual NYS cyber security conference*, New York, USA.
Monteiro, E. (2000). Actor-Network Theory and Information Infrastructure. *In From Control to Drift.* Chiborra, C.U. (Ed.), pp 71-83, Oxford University Press, Oxford.
Monteiro, E., & Hanseth, O. (1995). Social shaping of information infrastructure: On being specific about the technology. *In Orlikowski, W. J., Walsham, G., Jones, M. R., & DeGross, J. I. (Eds.). Information technology and changes in organisational work* (pp. 325-343). London: Chapman and Hall.
Orlikowski, W. J. (2000), 'Using technology and constructing structures: *a practice Lens for Studying technology in Organizations'*, Organization Science, vol. 11 no. 4, pp. 404-428
Orlikowski, W.J. & Iacono, C.Z. (2001). Desperately seeking the 'IT' in IT research – a call to theorizing the IT artifact. *Information Systems Research* 12(2):121−134.
Ngai, E. W. T., Xiu, L., & Chau, .C. (2009). Application of data mining techniques in customer relationship management: A literature review and classification. Expert Systems with Applications, 36(2), 2592–2602.
PWC (2013). Security Breaches Survey 2013. Enterprise and Regulatory Reform (BERR), *PricewaterhouseCoopers on behalf of the UK Department of Business*.
Peters, T.J. & Waterman, R.H. (1982). *In Search of Excellence: Lessons from America's Best-Run Companies.* New York: Harper & Row.
Rao, V. Srinivasan and S. Ramachandran (2011) "Occupational Cultures of Information Systems Personnel and Managerial Personnel: Potential Conflicts," *Communications of the Association of Information Systems,* 29, Article 21.
Robbins, S. P. (2001). *Theory Z: Organisation from a power-perspective*. California Management Review XXV (2), pp. 67-75.
Robson, C. (2002) *Real World Research*, Second edition, Blackwell, Oxford.
Rose, J., Jones, M. & Truex, D. (2005) Socio-Theoretic Accounts of IS: The Problem of Agency, *Scandinavian Journal of Information Systems*, 17, 1, 133-152.
Ruighaver, B., Maynard, B., and Chang, S. (2007). Organisational security culture: Extending the end-user perspective. *Computers & Security,* 26(1):56-62.

 

Saint-Germain, R. (2005). Information Security Management Best Practice Based on ISO/IEC 17799. *Information Management Journal,* 39(4):60-66.
Schein, E. H. (1985). *Organizational Culture and Leadership.* San Francisco: Jossey-Bass.
Schein, E.: The corporate culture survival guide. Jossey-Bass Publishers, San Francisco (1999)
Schein, E. H. (2004). *Organizational Culture and Leadership.* Hoboken: John Wiley & Sons, Inc.
Schlienger, T. & Teufel, S. (2002.). Information security culturethe socio-cultural dimension in information security management. *FIP TC11 International Conference on Information Security, Cairo, Egypt; 7-9 May 2002.*
Saxena, I. (2000). Corporate culture and organizational performance: A comparative study of manufacturing organisations. *Management Review* (March 2000): Indian Institute of Management, Bangalore.
Smith, C. (2010) *What is a Person? Rethinking Humanity, Social Life, and the Moral Good from the Person up*, University Of Chicago Press, Chicago.
Trice, H. M & Beyer, J. M. 1993. *The Culture of Work Organizations*. Englewood Cliffs, NJ: Prentice Hall.
Thomson, K. L. (2009). Information Security Conscience: a precondition to an Information Security Culture. 8th Annual Security Conference Las Vegas, NV, USA April 15-16.
Van Maanen, J. & Schein, E.H. (1979). Towards a theory of organizational socialization. *Research in Organizational Behavior Vol. 1*, JAI Press, Greenwich, CT.
Vroom, C. & von Solms, R. (2004). Towards information security behavioral compliance. *Computers 4 Security,* 23(3):191-198.
Walsham, G. (1997) In Information systems and qualitative research (Eds, Lee, A. S., Liebenau, J. and DeGross, J. I.) Chapman and Hall, London, pp. 466-480.
Walsham, G. (2002). Cross-cultural software production and use: A structurational analysis. *MIS Quarterly,,* 26(4):359-380.
Whitman M.E. & Mattord H. J. (2012). *Principles of Information Security* (4th ed.), Course Technology, Cengage Learning.

The IISTE is a pioneer in the Open-Access hosting service and academic event management. The aim of the firm is Accelerating Global Knowledge Sharing.

More information about the firm can be found on the homepage:
http://www.iiste.org

## CALL FOR JOURNAL PAPERS

There are more than 30 peer-reviewed academic journals hosted under the hosting platform.

**Prospective authors of journals can find the submission instruction on the following page:** http://www.iiste.org/journals/ All the journals articles are available online to the readers all over the world without financial, legal, or technical barriers other than those inseparable from gaining access to the internet itself. Paper version of the journals is also available upon request of readers and authors.

## MORE RESOURCES

Book publication information: http://www.iiste.org/book/

Academic conference: http://www.iiste.org/conference/upcoming-conferences-call-for-paper/

## IISTE Knowledge Sharing Partners

EBSCO, Index Copernicus, Ulrich's Periodicals Directory, JournalTOCS, PKP Open Archives Harvester, Bielefeld Academic Search Engine, Elektronische Zeitschriftenbibliothek EZB, Open J-Gate, OCLC WorldCat, Universe Digtial Library , NewJour, Google Scholar