Journal of Universal Computer Science, vol. 18, no. 12 (2012), 1628-1642
submitted: 15/9/11, accepted: 15/2/12, appeared: 28/6/12 © J.UCS

Information Security Service Culture – Information Security for End-users

Rahul Rastogi
(Nelson Mandela Metropolitan University, Port Elizabeth, South Africa
and Engineers India Limited, New Delhi, India
rahul.rastogi@eil.co.in)

Rossouw von Solms
(Nelson Mandela Metropolitan University, Port Elizabeth, South Africa
rossouw.vonsolms@nmmu.ac.za)

Abstract: Information security culture has been found to have a profound influence on the compliance of end-users to information security policies and controls in their organization. Similarly, a complementary aspect of information security is the culture of information security managers and developers in the organization. This paper calls this is as the 'information security service culture' (ISSC). ISSC shapes and guides the behaviour of information security managers and developers as they formulate information security policies and controls. Thus, ISSC has profound influence on the nature of these policies and controls and thereby on the interaction of end-users with these artefacts. ISSC is useful in transforming information security managers and developers from their present-day technology-focused approach to an end-user centric approach.

Keywords: Information security service culture, ISSC, Information security culture, culture, information security management
Categories: H.3.1, H.3.2, H.3.3, H.3.7, H.5.1

1 Introduction

Information security culture pervading in an organization is recognized as having a profound influence on end-user compliance to information security policies and controls in the organization. According to Von Solms, the idea of information security culture (ISC) emerged in the third wave of information security evolution [Von Solms, 00]. Information security culture can be created in an organization by "instilling the aspects of information security to every employee as a natural way of performing his or her daily job" [Von Solms, 00]. Martins and Eloff define ISC "as the assumption about which type of information security behavior is accepted and encouraged in order to incorporate information security characteristics as the way in which things are done in an organization" [Martins, 02]. Ramachandran et al. state that ISC involves "identifying the security related ideas, beliefs and values of the group, which shape and guide security-related behaviors" [Ramachandran, 08]. The importance of ISC lies in the fact that it fosters an attitude in end-users whereby safe information security behaviors become a way of organizational life for these end-

users [Van Niekerk, 05; Von Solms, 00]. ISC shapes and guides the behavior of end-users in the organization in regard to information security policies and controls.

Just as ISC has influence on the security-related behaviors of end-users, it can be said that a similar cultural force acts on the information security managers and developers in an organization. This paper calls this cultural force as 'information security service culture' (ISSC). ISSC acts as a patterning force; it shapes and guides the actions of information security managers and developers in the organization as they go about their task of developing information security policies and controls. Through this guiding action, ISSC influences the nature of information security policies and controls and the subsequent interaction of end-users with these artefacts. This makes ISSC a worthy topic to study and explore.

The paper is organized as follows. The concept of ISSC is related to the concepts of culture, service culture and information security culture. The paper begins by first examining this relationship. The following section then discusses the dysfunctional elements of present-day ISSC as it exists in the form of assumptions held by managers and developers of information security in today's organizations regarding end-users and their security-related behaviors. This section explores these assumptions and how these assumptions influence the nature of information security policies and controls in the organization. The section demonstrates that negative assumptions of end-users in the perception of information security managers and developers lead to bureaucratic and technology-focused information security polices and controls in the organization. The subsequent section examines different paradigms of information system development in order to identify an alternative approach to information security in the organization. Based on this discussion of paradigms, the paper proceeds to discuss ISSC its constituent elements. The paper discusses the service-oriented nature of ISSC and how it is mapped to Schein's model of culture [Schein, 04]. This section illustrates how information security managers and developers can be migrated towards end-user centric approach to information security in the organization thereby curing them of their "particularly rich tradition of indifference to the user" [Zurko, 96].

A note of caution is provided here. Some of the concepts presented later in the paper come from the streams of information systems and information systems development. These concepts are subsequently applied to information security. It can be said that the streams of information systems or IT and information security are closely related [Albrechtsen, 09; Frangopoulos, 07] and, hence, the concepts or results from the former fields can be validly applied to the latter. Further, it is to be noted that the paper treats the terms 'engineer', 'technologist' and 'developer' as synonyms. In the subsequent discussions, different authors have used one term or the other; this chapter uses the term 'developer' and refers to the role of people who manage and develop the systems (including information systems and information security policies and controls) that underlie the work of other people in the organization.

2 Culture, Service Culture, Information Security Culture and Information Security Service Culture (ISSC)

The concept of information security service culture is closely related to the three concepts of culture, service culture and information security culture. Further, the concepts of service culture and information security culture themselves are related to the concept of culture. This section discusses this relationship. The section also explores the components of culture.

[Davis, 85] defines culture as the "pattern of shared values and beliefs that give the members of an organization meaning, and provide them with the rules for behavior in the organization" [Grönroos, 07]. Schein defines culture as "a pattern of shared basic assumptions that was learned by a group as it solved its problems of external adaptation and internal integration that has worked well enough to be considered valid and therefore, to be taught to new members as the correct way to perceive, think and feel in relation to those problems" [Schein, 04]. Thus culture operates in an organization by shaping how people in an organization "do certain things, think in common ways and appreciate similar goals, routines and even jokes" [Grönroos, 07]. Culture acts as a patterning force and always exists. Researchers in the fields of service management and information security have cited the importance of culture to their respective fields.

Culture is critically important for service organizations [Grönroos, 07; Zeithaml, 08]. Zeithaml et al. define service culture as "a culture where an appreciation for good service exists, and where good service to internal as well as ultimate, external customers is considered a natural way of life and one of the most important norms by everyone" [Zeithaml, 08]. Grönroos states that "a functioning service culture requires that providing good service is second nature to everyone within that organization" [Grönroos, 07]. Further, service culture arises when all organizational components such as "organizational routines, directions for action given by policies and management and reward systems" converge together to emphasize good service to customer, whether internal or external. Culture, as the attitude of its employees, is particularly important for service organizations. Because delivering a service involves the coming together of the employees and their customers, employee attitudes and performance are visible to customers. Hence the attitude of employees, a reflection of the service culture in the organization, is critically important.

Information security service culture (ISSC) is based upon the concepts of culture and service culture. ISSC refers to the culture, and hence the patterns of shared values and beliefs, amongst the information security managers and developers in the organization. Just as culture and service culture apply to the employees of the organization, ISSC applies to the employees working in the information security function. ISSC consists of the patterning force of culture that drives the information security managers and developers to deliver "good service" to their customers, viz. the end-users in the organization. ISSC is visible when end-users come in contact with information security managers and developers and the information security policies and controls in the organization. Further, as stated above, ISSC can arise only when all the different organizational components come together to stress "good service" to end-users. ISSC and "good service" to end-users, however, do not imply that the security needs of the organization's information assets are completely

ignored; it only means that while these classical security issues are also important, service to end-users should have a dominant role.

The inter-relationship between culture, service culture, information security culture and ISSC are shown in Figure 1. According to this figure, both concepts of information security service culture and information security culture are based upon the concept of culture; ISSC is also based upon the concept of service culture. ISSC differs from information security culture in that ISSC applies to the employees of the information security function, whereas information security culture applies to the end-users in the organization. Further, while ISSC seeks to promote an end-user centric approach to information security, ISC seeks to promote the compliance of end-users to information security policies and controls in the organization. It is also pertinent to note that both ISSC and ISC contribute to the state of information security in the organization.

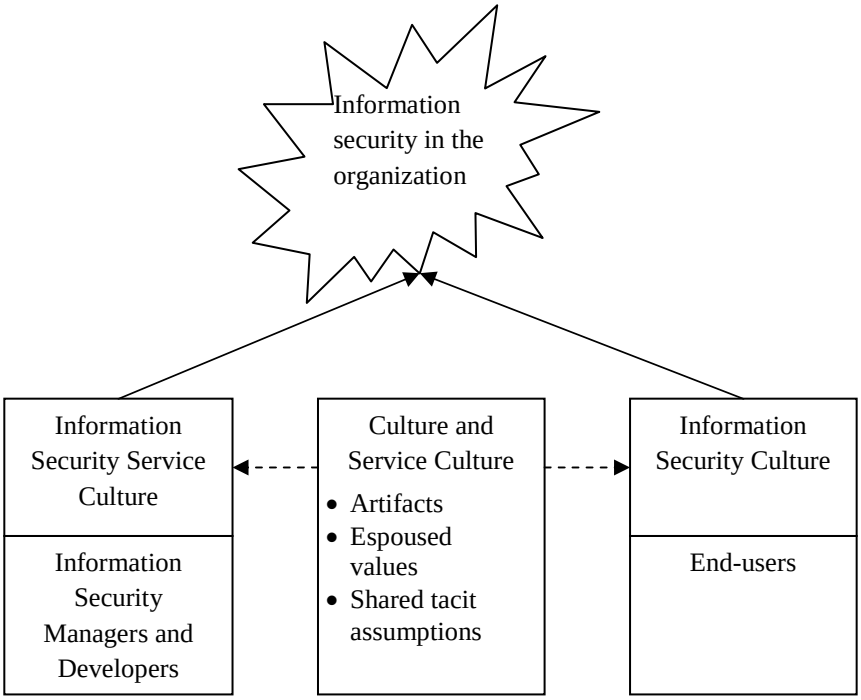

Figure 1: Information security service culture and information security culture leading to effective information security in the organization

Having discussed the meaning and role of various types of cultures, it is important to understand the constituent parts of culture. According to Schein, culture exists at three levels – 'artifacts', 'espoused values and beliefs' and 'underlying assumptions' (Figure 2) [Schein, 04]. The topmost level is that of artifacts. Artifacts are the observable phenomena that reflect a particular culture. In the context of a group, artifacts are the visible behavior of the group. In an organization, artifacts refer to the organizational processes and structural elements that lead to the behavior of the

constituent groups. Espoused values and beliefs are psychological or attitudinal in nature, and exist at the conscious level. They reflect the strategies, goals and philosophies of the group. Whereas artifacts are the visible manifestations of behavior, espoused values and beliefs are the invisible determinants of behavior. Below the beliefs and values at the conscious level, lie the shared tacit assumptions. Shared tacit assumptions operate at the unconscious level and are deeply ingrained. These assumptions are 'taken-for-granted' and are strongly held in a group.

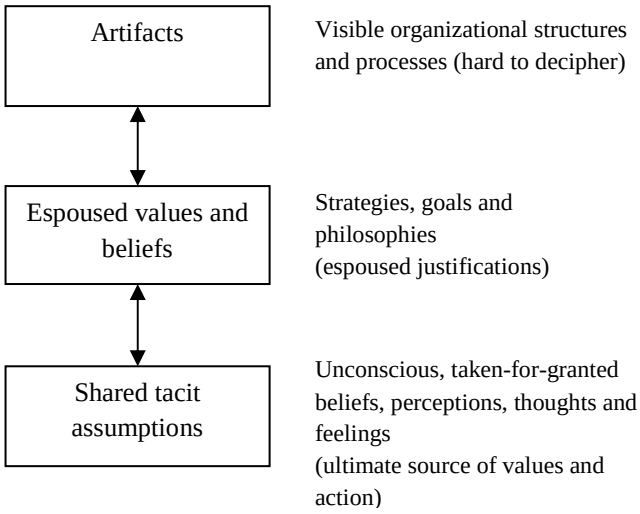

Figure 2: Levels of culture (from [Schein, 04])

The role of culture as a patterning force is extremely important for organizations, particularly in a service context. The above discussion has provided an overview of the related concepts of culture, service culture, information security culture and information security service culture. ISSC differs from information security culture in that ISSC applies to the employees of the information security function whereas information security culture applies to the end-users in the organization. The next section discusses in greater detail the influence of ISSC over information security managers and developers who formulate information security policies and controls in the organization.

3 The assumptions of information security managers and developers regarding end-users

As stated earlier, information security managers and developers hold shared assumptions regarding end-users. These assumptions lead to the creation of an image of end-users in the perception of information security managers and developers. Various researchers have explored the link between developers' assumptions and perceptions of end-users and the nature of systems that result from these perceptions.

This section discusses this link in an attempt to understand the image of end-users in the perception of information security managers and developers and how this image influences the nature of information security policies and controls in the organization. The section goes on to discuss the resultant bureaucratic nature of present-day information security management.

3.1 The role of assumptions

The developers in the organization have an implicit perception regarding the end-users in the organization. As these developers develop systems for the use of end-users, their perceptions of end-users have an impact on the nature and the success or failure of the developed systems [Bostrom, 77; Orlikowski, 94]. In the field of information systems development (ISD), Bostrom and Heinen [Bostrom, 77] and Orlikowski and Gash [Orlikowski, 94] have adopted a similar approach to understand the interaction between developers of information systems and their end-users in the organization.

According to Bostrom and Heinen, the development of information systems is impacted significantly by the view that system designers and developers hold regarding the organization, end-users and the function of the information system within the organization [Bostrom, 77]. The knowledge, skills and values of the designers and the assumptions they hold about the organization and end-users influence their design of information systems. These factors act as "frames of reference" and "perceptual filters" that act to guide the designers and developers. Bostrom and Heinen [Bostrom, 77] further state that these frames of reference act at the sub-conscious level and designers and developers may not always be aware of the content of their frame of reference.

Orlikowski and Gash use the concept of "technological frames", or "technology frames", to understand the development and use of information systems in organizations [Orlikowski, 94]. Technological frames, or technology frames concern the "assumptions, expectations and knowledge" that people in an organization hold regarding technology in the organization [Orlikowski, 94]. According to Orlikowski and Gash, technological frames have powerful effects as they influence the design and use of technologies in the organization [Orlikowski, 94]. In this way, information systems reflect the "objectives, values, interests and knowledge" of the designers and developers of the system. These assumptions are implicit and the group often may not be aware of them.

3.2 The assumptions regarding end-users

Ashenden [Ashenden, 08] and Albrechtsen and Hovden [Albrechtsen, 09] have discussed the difficulties arising from the mismatch between the highly technical information security managers and developers and the technically naive end-users. This section is based on these two papers and discusses the assumptions that present-day information security managers and developers hold about end-users in the organization.

According to Ashenden [Ashenden, 08], in most organizations, information security is still a purely technical subject and best managed by technical staff. Information security managers and developers approach their subject in a "command

and control" manner and remain isolated and disengaged from the end-users of their creation. The managers and developers do not make any attempts to understand or negotiate with their end-users and continue to rely on "how they think end-users see information security" [Ashenden, 08].

Albrechtsen and Hovden [Albrechtsen, 09] state that a divide exists between end-users and information security managers with respect to skills, knowledge and responsibilities. This situation leads to information security policies and controls being designed with a duty-oriented or "policing" approach. In this approach, the policies and controls focus on allowing or disallowing end-users from performing specific activities. There is also an emphasis on surveillance and monitoring. Albrechtsen and Hovden [Albrechtsen, 09] further state that information security managers regard end-users both as a resource and as a problem. Managers feel that end-users lack motivation, knowledge and skills required for safe and secure behavior and hence cause adverse incidents. Managers also have negative assessments of end-users. Consequently, information security policies and controls rely on "technological tools that seek to control and monitor user behavior" because "technology is also believed to be more sound and reliable than users". Though user participation and involvement is rated highly, most information security managers remain aloof and distant from end-users while formulating information security policies and controls. Information security managers typically do not have detailed information regarding the information security behaviors of end-users – they continue to design information security policies and controls based on their perceptions of end-users. There is a trust deficit wherein information security managers do not trust end-users. It can be said that the relationship of information security managers and developers with their end-users is marred by incorrect perceptions, distrust and antagonism.

3.3 The resultant approach to information security management

The preceding discussion in this section has presented the link between the assumptions that information security managers and developers hold about end-users and the nature of information systems developed in the organization. The discussion has also covered the negative assumptions of information security managers and developers regarding end-users in the organization. This following discussion covers how these negative assumptions influence the nature of information security policies and controls in the organization.

According to Frangopoulos, present-day information security management is bureaucratic in nature and while it is "complete from a technical viewpoint", it falls short on the treatment of the "idiosyncratic nature of the human element, especially within a social context" [Frangopoulos, 07]. Frangopoulos further states that present-day information security management ignores the inherent variability of humans and their impact on the information security in the organization [Frangopoulos, 07]. Echoing Frangopoulos [Frangopoulos, 07]; Albrechtsen too states that present-day information security management represents a paradox in that it attempts to manage the security of modern and dynamic IT through traditionally structured approaches and perspectives [Albrechtsen, 08].

It can now be said that end-users and information security managers and developers are linked by two factors. Firstly, information security managers and developers formulate information security policies and controls based on

technological considerations only and ignore the needs of end-users. The assumption underlying this approach is that end-users are rational actors who will readily comply with information security policies and controls. This assumption ignores the inherent variability of end-users and is thus flawed. Secondly, as end-users exhibit resistance and rejection of information security policies and controls built upon a flawed assumption, information security managers and developers come to have an antagonistic view towards the end-users in the organization. These two factors conspire to ensure information security managers and developers in the organization continue to neglect the principle of psychological acceptability and the ease of use of information security policies and controls. It can be said that this inadequacy of present day information security policies and controls results from the unrealistic models and expectations of the developers regarding the end-users of these policies and controls. The unrealistic models and expectations, in turn, arise from the lack of knowledge regarding the everyday work and information security behaviors of end-users.

This section has established the importance of assumptions that information security managers and developers hold about end-users. These assumptions determine the nature of information security management and policies and control in the organization. In the present-day, information security managers and developers hold negative assumptions about end-users and this leads to bureaucratic, technology-focused information security policies and controls in the organization; such an environment, in turn, leads to end-user resistance and non-compliance. The next section discusses a possible approach to resolve this imbroglio.

4 A suitable paradigm for the development of end-user centric information security in the organization

This section briefly discusses the various paradigms that are adopted in the development of information systems in organizations. Each paradigm has its own set of assumptions regarding end-users and leads to systems of different natures. The section concludes by identifying a paradigm suitable to the development of information security policies and controls in the organization. The choice of a suitable paradigm is significant as it will determine the kind of assumptions and culture that are required to be inculcated amongst the information security managers and developers in order to ensure an end-user centric approach to information security policies and controls.

Hirschheim and Klein [Hirschheim, 89] define a paradigm as consisting of "assumptions about knowledge and how to acquire it, and about the physical and social world". According to Hirschheim and Klein [Hirschheim, 89], in a professional community, all members typically follow a common paradigm and hence share both perceptions and practices. As already discussed earlier, these perceptions and practices are particularly important in the context of system development. The perceptions and practices of developers have a significant impact on the nature of system development, the nature of the system that is developed and the nature of the use of the system. In their work, Hirschheim and Klein [Hirschheim, 89] present four paradigms of information systems development, viz. "functionalism", "social

relativism", "radical structuralism" and "neohumanism". These paradigms are based on the four paradigms proposed by Burrell and Morgan [Burrell, 79]. Various authors have applied the four paradigms of Burrell and Morgan [Burrell, 79] and Hirshheim and Klein [Hirschheim, 89] to the study of information security [Clarke, 03; Dhillon, 95; Dhillon, 01; McFadzean, 06; White, 05].

Dhillon [Dhillon, 95] and Dhillon and Backhouse [Dhillon, 01] have applied the four paradigms to information security. Dhillon [Dhillon, 95] observes that information systems researchers and developers have begun to move away from a purely technical approach to systems development; the researchers and developers consider the act of systems development as a social act. Unfortunately, information security researchers and developers have remained locked in their "psychic prison" [Bolman, 03] of a "mechanistic, technical vision" [Dhillon, 95]. A similar view is echoed by Frangopoulos [Frangopoulos, 07], Ashenden [Ashenden, 08] and Albrechtsen and Hovden [Albrechtsen, 09]. The present-day approach to the development of information security policies and controls lies in the functionalist paradigm. White and Dhillon [White, 05] have proposed using the "interpretivist" or "social relativist" paradigm for resolving the crisis of information security. This shift from functionalism to interpretivism is necessitated by the fact that information security relies heavily upon end-user interpretation and participation in compliance with information security policies and controls in the organization. In view of these facts, the further discussion in this section considers only the functionalist and interpretivist approaches to information security as outlined by White and Dhillon [White, 05]. The discussion is based on the description of these two paradigms by Hussain and Taylor [Hussain, 07].

In the present-day, functionalist approach to information security in the organization, the information security developer acts as an expert. The developer is focused on technology, tools and methods for controlling the access of end-users to information assets. The developer is unconcerned with the impact on end-users, their working practices, their needs and requirements. The end-users are expected to act mechanistically and according to the needs of the system. This approach satisfies the "system ideal" and leads to a "technology trap" wherein technology is considered to provide the complete solution to a problem. According to Schlienger and Teufel, in this approach, the users are seen as a threat; there is distrust between the developers and end-users and there is no inclination to discuss the human aspect of information security [Schlienger, 02].

The interpretivist approach to information security lies in stark contrast to the functionalist approach. The interpretivist approach is a holistic approach and is based upon understanding how end-users interpret and comply with information security policies and controls in the organization. The information security developer acts as a catalyst or facilitator that seeks to understand the working practices and needs and requirements of end-users. The emphasis is to ensure that end-users will be willing to learn, adapt and accept the information security policies and controls. This approach satisfies the "contextualist ideal" wherein the emphasis is on the social context and processes. In this approach, the end-user is no longer the enemy; rather, the end-user is treated as a "security asset" [Schlienger, 02] and information security becomes a discipline with a "a socio-cultural, human centric approach that is based on trust and partnership, accompanied by appropriate security technology" [Schlienger, 02].

A comparison of the functionalist and interpretivist approaches is shown in Table 1.

Functionalist approach	Interpretivist appraoch
• The information security developer acts as an expert. • The developer is focused on technology, tools and methods for controlling the access of end-users to information assets. • The developer is unconcerned with the impact on end-users, their working practices, their needs and requirements. • The end-users are expected to act mechanistically and according to the needs of the system. • This approach satisfies the "system ideal" and leads to a "technology trap" wherein technology is considered to provide the complete solution to a problem.	• The information security developer acts as a catalyst or facilitator. • The developer seeks to understand the working practices and needs and requirements of end-users. • The emphasis is to ensure that end-users will be willing to learn, adapt and accept the information security policies and controls. • This approach satisfies the "contextualist ideal" wherein the emphasis is on the social context and processes.

Table 1: A comparison of the Functionalist and Interpretivist approaches

Given the importance of end-user behavior to the success of information security in the organization, it is to be expected that an end-user centric approach to information security is required. The present-day approach to information security is functionalistic and is therefore inappropriate. The way out, as suggested by White and Dhillon [White, 05], is to use an interpretivist approach. Such an approach emphasizes the "contextualist ideal" and requires the study of the "social context and associated processes" of end-users, their work in the organization and their information security behaviors. The change from a functionalist to an interpretivist approach requires an antecedent change - that of changing the mind-set of the information security developers towards recognizing and accepting a far more substantive and richer role for end-users. In the context of information security in the organization, this change can be brought through information security service culture (ISSC). The next section presents a discussion of the concept of ISSC.

5 Information security service culture (ISSC)

The previous sections have highlighted the crucial role of the attitude of the developers of systems towards the end-users of those systems. This attitude plays an important role in shaping how the system is developed, how the developers incorporate human issues and, finally, how the system is accepted and used by end-users. These attitudes have been variously called as the "engineering culture" [Schein,

96; Schein, 04], "frames of reference" [Bostrom, 77], "technology frames" [Orlikowski, 94] and "paradigms" [Burrell, 79; Hirshheim, 89]. These concepts are also applicable in the development of information security policies and controls in the organization [Clarke, 03; Dhillon, 95; Dhillon, 01; McFadzean, 06; White, 05]. As discussed earlier, the traditional approach to information security has been technology oriented, or functionalist, and therefore has failed to garner support from end-users; the way out of this imbroglio is to use an interpretivist approach to information security [White, 05]. This section proposes and discusses information security service culture (ISSC) as a means to migrate developers of information security policies and controls from the functionalist to the interpretivist paradigm.

A key aspect of Schein's model of culture, discussed in the previous section, is the disconnect that can occur between the three levels of culture in a group or organization. Espoused beliefs and values at the conscious level can be said to predict behaviors at the artifacts level. However, if the beliefs and values are incongruent with the assumptions at the unconscious level, then there can be a misalignment between what people 'say' they will do in a situation and what they actually 'do'. Thus as Schein [Schein, 04] says, "a company may say that it values people and that it has high quality standards for its products, but its record in that regard may contradict what it says". If the espoused beliefs and values are congruent with the underlying assumptions, then there is alignment between what people 'say' and 'do'. In the context of information security, it can be said that information security developers and managers suffer from an incongruence between their underlying assumptions and their espoused beliefs and behaviors – there is misalignment between what they say and do in respect of end-users – they profess the importance of end-users to information security and yet, continue to formulate information security policies and controls with scant regard for the needs and requirements of end-users.

Information security service culture is an attempt at aligning what information security developers and mangers say with what they do, that is the espoused and the enacted. In terms of information security, this means that developers and managers adopt the interpretivist paradigm and that the organization provides them with the encouragement and resources to enable them to formulate end-user centric information policies and controls. The three levels of culture can thus be mapped as follows:

- **Shared tacit assumptions**

At the unconscious level, developers and managers of information security should hold the beliefs that end-users are not their "enemy", rather the end-users are an "asset". They should also believe that end-users want to comply with information security policies and controls; and that there often is not any malicious intent behind non-compliance. End-users want to work in the interest of their organization. Any non-compliance is largely a result of the cognitive limitations of end-users or because the information security policies and controls are incompatible with their work practices. The information security developers and managers should also believe that end-users are their customers and that they are there for providing the information security service to the end-users. In this frame of mind, the end-users become the most important entity for the information security managers and developers.

- **Espoused values and beliefs**

This is the conscious level at which the strategies, goals and philosophies exist. At this level, the information security developers and managers should utilize technologies, tools and methods that lead to end-user centric information security policies and controls in the organization. End-user acceptance and ease of use of policies and controls should be important determinants of the security measures. Further, formulation of information security policies and controls must not happen in isolation from end-users; rather, in keeping with the interpretivist paradigm, policies and controls must be formulated with the active involvement of end-users. ISO/IEC 9241-210:2010 is an international standard titled "Human-centred design for interactive systems" [ISO, 10]. Information security policies and controls are "interactive systems" and this standard, with its focus on designing human-centred interactive systems, can provide useful guidance for their formulation. According to this standard, formulation of end-user centric information security policies and controls would require "an approach to interactive systems development that aims to make systems usable and useful by focusing on the users, their needs and requirements, and by applying human factors / ergonomics and usability knowledge and techniques" [ISO, 10]. This standard will enable information security developers and managers to "design and redesign processes to identify and plan effective and timely human-centre design activities". According to ISO/IEC 9241-210:2010 [ISO, 10], the principles of human-centred design are:

a) The design is based upon an explicit understanding of users, tasks and environments.
b) Users are involved throughout design and development.
c) The design is driven and refined by user-centred evaluation.
d) The process is iterative.
e) The design addresses the whole user experience.
f) The design team includes multidisciplinary skills and perspectives.

- **Artifacts**

The artifacts level is populated by organizational processes and structures and the behaviors of information security developers and manager. The artifacts level is also populated by the end-user centric information security policies and controls. These end-user centric policies and controls will be acceptable to end-users, be usable by them and will earn the commitment of end-users to information security. ISO/IEC 9241-210:2010 [ISO, 10] provides guidance on the activites that need to be performed for the development of human-centred interactive systems. These activities are:

a) Understanding and specifying the context of use.
b) Specifying the user requirements.
c) Producing design solutions.
d) Evaluating the design.

The artifacts level is also populated by the behaviors of business managers and IT managers – their behaviors create an end-user centric environment for the day-to-day work that promotes safe information security behaviors of end-users. Adequate encouragement, knowledge and resources must be provided to information security managers and developers to enable them to undertake the formulation of end-user centric information security policies and controls in the organization. Leadership is a key aspect of building a service culture [Bartley, 07; Grönroos, 07; Mather, 08]. The

behavior of managers in supporting the developers in their end-user centric endevaours removes any incongruence between what is said and what is actually done. According to Grönroos [Grönroos, 07], any incongruity in the stance of managers will be detrimental to establishing the information security service culture – if managers do not walk their talk, then developers too will be unable to deliver end-user centricity.

The three levels of the information security service culture are shown in Figure 3.

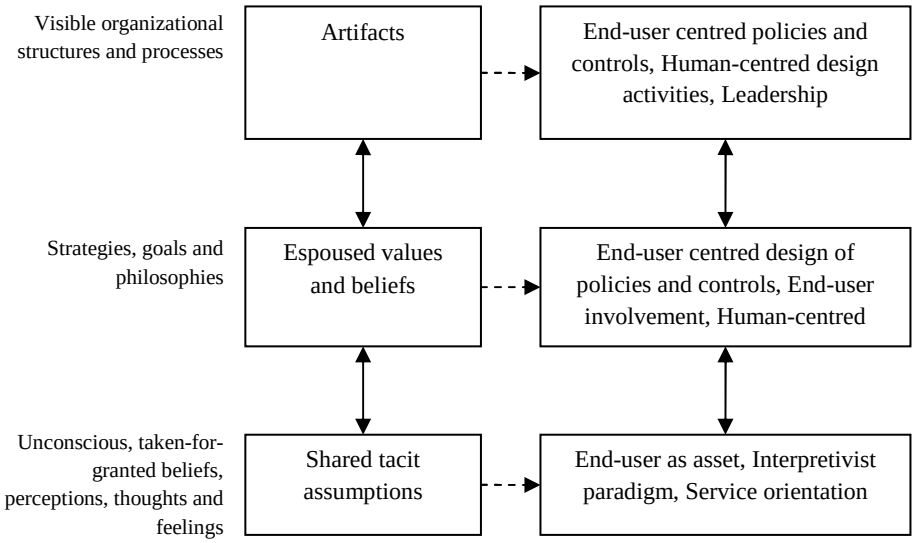

Figure 3: The three levels of information security service culture (ISSC)

6 Conclusion

This paper began with an elaboration of the importance accorded to information security culture in the organization. The paper subsequently identified information security service culture (ISSC) as an equally important concept. ISSC is based upon the concepts of culture and service culture. Further, based upon the works of various researchers, the paper identified the interpretive paradigm as suitable for information security in the organization. The paper then proceeded to delineate ISSC as embodying these concepts and paradigm. The constituent elements of ISSC were mapped to Schein's model of culture. Future work is needed for taking ISSC from the present basic structure to a more detailed methodology for development and management.

References

[Albrechtsen, 08] Albrechtsen, E.: Friend or foe? Information security management of employees. Doctoral Thesis, Norwegian University of Science and Technology, Faculty of

Social Sciences and Technology Management, Department of Industrial Economics and Technology Management, 2008. Retrieved June 20, 2010, from http://ntnu.diva-portal.org/smash/record.jsf?searchId=1&pid=diva2:231438.

[Albrechtsen , 09] Albrechtsen, E., Hovden, J.: The information security digital divide between information security managers and users. Computers & Security, 2009, 6:476-490.

[Ashenden , 08] Ashenden, D.: Information security management: A human challenge? Information Security Technical Report, 2008, 4:195-201.

[Bartley, 07] Bartley, B., Gomibuchi, S., Mann, R.: Best practices in achieving a customer-focused culture. Benchmarking: An International Journal, 2007, 14(4), 482-496.

[Bolman, 03] Bolman, L. G., Deal, T. E.: Reframing organizations. San Francisco: Jossey-Bass, 2003.

[Bostrom, 77] Bostrom, R. P., Heinen, J. S.: MIS Problems and Failures: A Socio-Technical Perspective. Part I: The Causes. MIS Quarterly, 1977, 3:17-32.

[Burrell, 79] Burrell, G, Morgan, G (1979): Sociological paradigms and organisational analysis. London: Heinemann Educational Books Ltd., 1979.

[Clarke, 03] Clarke, S., Drake, P.: A social perspective on information security: theoretically grounding the domain. In S. Clarke, E. Coakes, M. G. Hunter & A. Wenn (Eds.), Socio-Technical and Human Cognition Elements of Information Systems (pp. 249-265). London: Information Science Publishing, 2003.

[Davis, 85] Davis, S. M.: Managing Corporate Culture. Cambridge, MA: Ballinger, 1985.

[Dhillon, 95] Dhillon, G.: Interpreting the management of information systems security. Doctoral Thesis, Information Systems Group, London School of Economics, 1995. Retrieved June 20, 2010, from http://www.lse.ac.uk/collections/informationSystems/pdf/theses/dhillon.pdf.

[Dhillon, 01] Dhillon, G., Backhouse, J.: Current directions in IS security research: Toward socio-organizational perspectives. Information Systems Journal, 2001, 2:127-153.

[Frangopoulos, 07] Frangopoulos, E.: Social engineering and the ISO/IEC 17799:2005 security standard: a study on effectiveness. Master of Science Thesis, School of Computing, University of South Africa, 2007. Retrieved June 20, 2010, from http://uir.unisa.ac.za/bitstream/10500/2142/1/dissertation.pdf.

[Grönroos, 07] Grönroos, C.: Service management and Marketing: Customer management in service competition (3rd ed.). Delhi, India: John Wiley & Sons Ltd., 2007.

[Hirschheim, 89] Hirschheim, R., Klein, H.: Four Paradigms of Information Systems Development. Communications of the ACM, 1989, 32:1199-1216.

[Hussain, 07] Hussain, Z., Taylor, W. A.: Evaluating the behaviour of information systems developers: The relevance and utility of paradigms. Behaviour and Information Technology, 2007, 3:221-236.

[ISO, 10] ISO/IEC 9241-210 (2010). Ergonomics of human-system interaction - Part 210: Human-centred design for interactive systems. ISO/IEC 9241-210:2010, International Organization for Standardization and International Electrotechnical Commission.

[Martins, 02] Martins, A., Eloff, J. P. H.: Promoting information security culture through an information security culture model. In Proceedings of ISSA2002, Johannesburg, South Africa, 2002.

[Mather, 08] Mather, J.: Creating the service culture. Human Resources, 2008,18-19.

[McFadzean, 06] McFadzean, E., Ezingeard, J.-N., & Birchall, D.: Anchoring information security governance research: Sociological groundings and future directions. Journal of Information Systems Security, 2006, 3:3-48.

[Orlikowski, 94] Orlikowski, W. J., Gash, D. C.: Technological frames: Making sense of information technology in organizations. ACM Transactions on Information Systems, 1994, 2:174–207.

[Ramachandran, 08] Ramachandran, S., Rao, S. V., Goles, T.: Information security cultures of four professions: A comparative study. In Proceedings of the 41st Annual Hawaii International Conference on System Sciences, 2008. ISBN: 978-0-7695-3075-8.

[Schein, 96] Schein, E. H.: Three cultures of management: The key to organizational learning. Sloan Management Review, 1996, 1:9-20.

[Schein, 04] Schein, E. H.: Organizational culture and leadership (3rd Ed.). San Francisco: Jossey-Bass, 2004.

[Schlienger, 02] Schlienger, T., Teufel, S.: Information security culture - The socio-cultural dimension in information security management. In Proceedings of IFIP TC11 International Conference on Information Security (Sec2002): Security in the information society: visions and perspectives, 2002.

[Van Niekerk, 05] Van Niekerk, J., von Solms, R.: An holistic framework for the fostering of an information security sub-culture in organizations. Information Security South Africa (ISSA), 2005, Johannesburg, South Africa.

[Von Solms, 00] Von Solms, B.: Information security – the third wave? Computers & Security, 2000, 7:615-620.

[White, 05] White, E. F. R., Dhillon, G.: Synthesizing information system design ideals to overcome developmental duality in securing information systems. In Proceedings of the 38th Annual Hawaii International Conference on System Sciences (HICSS'05) - Track 7, 2005. ISBN: 0-7695-2268-8.

[Zeithaml, 08] Zeithaml, V. A., Bitner, M. J., Gremler, D. D., Pandit, A.: Service marketing – integrating customer focus across the firm (4th ed.). Delhi, India: Tata McGraw-Hill Publishing Company Ltd., 2008.

[Zurko, 96] Zurko, M. E., & Simon, R. T.: User-centered security. New Security Paradigms Workshop, 1996.