UNDERSTANDING INFORMATION SECURITY CULTURE: A CONCEPTUAL FRAMEWORK

Johan van Niekerk[1], Rossouw von Solms[2]

[1,2]Centre for Information Security Studies, Nelson Mandela Metropolitan University, South Africa

[1]johanvn@nmmu.ac.za, +27 41 5043048, PO Box 77000, Port Elizabeth, 6000

[2]rossouw@nmmu.ac.za, +27 41 5043669, PO Box 77000, Port Elizabeth, 6000

ABSTRACT

The importance of establishing an information security culture in an organization has become a well established idea. The aim of such a culture is to address the various human factors that can affect an organization's overall information security efforts. However, *understanding* both the various elements of an information security culture, as well as the relationships between these elements, can still be problematic. Schein's definition of a *corporate* culture is often used to aid understanding of an information security culture. This paper briefly introduces Schein's model. It then incorporates the important role knowledge plays in information security into this definition. Finally, a conceptual framework to aid understanding of the interactions between the various elements of such a culture, is presented. This framework is explained by means of illustrative examples, and it is suggested that this conceptual framework can be a useful aid to understanding information security culture.

KEYWORDS

Information Security, Information Security Culture, Corporate Culture, Organizational Learning, Schein's Model.

UNDERSTANDING INFORMATION SECURITY CULTURE: A CONCEPTUAL FRAMEWORK

1 INTRODUCTION

Today, most organizations need information systems to survive and prosper. Information has become a valuable asset to modern organizations. It is therefore imperative for modern organizations to take the protection of their information resources seriously. This protection of information resources, also known as information security, consist of many processes. Some of these processes are, to a large extent, dependent on human co-operated behavior. Employees, whether intentionally or through negligence, often due to a lack of knowledge, are the *greatest threat* to information security (Mitnick & Simon, 2002, p. 3). Without an adequate level of user **cooperation** and **knowledge**, many security techniques are liable to be misused or misinterpreted by users. This may result in even an adequate security measure becoming inadequate (Siponen, 2001). An organization's information security strategy should thus comprehensively address this "human factor". It is important to note that there are two dimensions to this "human factor" in information security, namely *knowledge*, and cooperation, or *behavior*. These dimensions are to a large extend interrelated to each other.

Organizations cannot protect the integrity, confidentiality, and availability of information in today's highly networked systems environment without ensuring that each person involved shares the security vision of the organization, understands his/her roles and responsibilities, and is adequately trained to perform them (ISO/IEC TR 13335-1, 2004, p. 14). In order to assist in ensuring information security, individual users thus needs **knowledge** regarding their specific role in the security process. This knowledge can be provided via education, training and awareness campaigns.

Once these users have sufficient knowledge about their roles in the security process, there is still no guarantee that they will adhere to their required security roles. It is possible that users understand their roles correctly but still don't adhere to a security policy because it conflicts with their beliefs and values (Schlienger & Teufel, 2003). It is therefore imperative to also ensure that the users have the correct attitude, and thus the desired **behavior**, towards information security. In order to ensure the desired user behavior, it is necessary to cultivate an organizational sub-culture of information security (Von Solms, 2000; Schlienger & Teufel, 2003). Such a culture should support all business activities in such a way that information security becomes a natural aspect in the daily activities of every employee (Schlienger & Teufel, 2003). Education of employees plays a very important role in the establishment of such a culture. It is paramount that the people are educated to *want to be* more secure in their day to day operation (Nosworthy, 2000). Such a change of attitude is of utmost importance, because a change in attitude automatically leads to a subsequent behavioral change (Nosworthy, 2000). Through the establishment of an information security culture, the employees can become a security asset, instead of being a risk (Von Solms, 2000).

Many recent studies have shown that the establishment of an information security culture in the organization is in fact **necessary** for effective information security (Eloff & Von Solms, 2000; Von Solms, 2000). However, such a culture **must** be supported by adequate knowledge regarding information security (Van Niekerk & Von Solms, 2005). Without adequate knowledge, users who want to behave securely, might still apply a security control incorrectly. Conversely, a user who has adequate knowledge, but believes that secure behavior is unnecessary in his/her specific role, might still behave in an insecure way. Due to this co-dependence between the knowledge dimension of the human factor in information security, and the behavioral dimension, it would be beneficial to deal with both these dimensions holistically. It would thus make sense to have a single conceptual framework that can be used to reason about both the knowledge, and the behavioral aspects of this human factor in information security. This paper will briefly adapt the "generic" definition of *corporate* culture to the specific needs of an *information security* culture. This adapted definition will then be used to

provide a conceptual framework for examining the various aspects of the human factors in information security.

In examining this adapted definition, it is important to realize that knowledge, and the underlying educational programs needed to impart such knowledge, is often seen as part of corporate culture. It is not the intent of this paper to dispute this view. In fact, this paper supports the view that knowledge and education will always play a role towards ensuring specific behavior patterns. However, this paper does attempt to highlight the fact that the knowledge ”dimension” is of *particular* importance in an information security culture, and that security knowledge plays a very specific *enabling* role in information security. The additional knowledge ”dimension” this paper will present, represents the knowledge needed to effectively implement, or use, the security measures if the desired attitude can be assumed. The knowledge that form an underlying part of *any* corporate culture is *still* assumed to be present. In *that* respect, an information security culture is assumed to be the same as a ”normal” corporate culture.

2 RESEARCH PARADIGM AND RATIONALE

The work in this paper is based on qualitative, or phenomenological- , research methods, as described in Creswell (1998). This paper should thus be seen as ”an inquiry process of understanding based on distinct methodological traditions of inquiry that explore a social or human problem” (Creswell, 1998, p. 15). The research presented here does not attempt to define *new* knowledge, but rather to provide a more in-depth understanding of the phenomenon described as ”information security culture”. As far as could be determined, the specific conceptual model, as well as the underlying interactions between the various levels of information security culture, as presented in this paper, has never been published before. It is the authors’ belief that the use of this conceptual model could improve the understanding of the concept of information security culture. Since the concept of organizational culture has been largely ”borrowed” by information security researchers from the humanities, it was deemed fitting to also ”borrow” the research paradigm, used in this paper from the humanities.

The model for corporate culture as presented in Schein (1999) has become widely accepted amongst information security researchers (Schlienger & Teufel, 2003). However, this model describes corporate culture in *general*, and not information security culture *specifically*. In order to ensure a rigorous research approach, even concepts with a seemingly obvious meaning will be revisited in this paper. The description of these concepts in the presented information security framework is deemed necessary because there might exist differences between the ontologies commonly adhered to by information security specialists and researchers from the management sciences.

The aim of this paper is thus to present an holistic, conceptual model of information security culture, for information security practitioners and students. This model aims to clarify, at a conceptual level, the interactions between various elements comprising such an information security culture. The model also attempt to clearly define, in an information security context, concepts such as the strength and the stability (or predictability) of an information security culture. The model presented in this paper is intended to clarify, and improve, the understanding of exiting concepts. It is hoped that this model will be of use to other information security researchers when examining the human factors in information security. Before the specific concept of an information security culture is examined, this paper will first explore the existing definition of corporate culture.

3 CORPORATE CULTURE

Every organization has a particular culture, comprising an omnipresent set of assumptions that is often difficult to fathom, and that directs the activities within the organization (Smit & Cronjé, 1992, p. 382). Such a culture could be defined as; the **beliefs** and **values** shared by people in an organization (Smit & Cronjé, 1992, p. 382). Beliefs and values, however, are both concepts that can be difficult to quantify. It is therefor often tempting to think of culture as just ”the way we do things around here”

(Schein, 1999, p. 15), or that ”something” that makes an organization more successful than others (Smit & Cronjé, 1992, p. 383). However, oversimplifying the concept of culture is the biggest danger to understanding it (Schein, 1999, p. 15).

A better way to think about culture is to examine the different ”levels” at which culture exists (Schein, 1999, p. 15). This way of thinking about corporate culture is already widely accepted in information security (Schlienger & Teufel, 2003). In order to clarify these levels of culture, each of the levels will be briefly examined:

- **Level One: Artifacts.** Artifacts are what you can observe, see, hear, and feel, in an organization (Schein, 1999, p. 15). Artifacts would include visible organizational structures and processes. At the level of artifacts, culture is very clear and has an immediate emotional impact, which could be positive or negative, on the observer (Schein, 1999, p. 16). Observing the artifacts alone, however, does not explain **why** the members of the organization behave as they do (Schein, 1999, p. 16). In order to understand the reasons for the behavior patterns of organization members it is necessary to examine ”deeper” levels of culture (Schein, 1999, p. 16), such as the organization’s espoused values.

- **Level Two: Espoused Values.** An organization’s *espoused values* are the ”reasons” an organizational insider would give for the observed artifacts (Schein, 1999, p. 17), for example; that the organization believes in team work, that everyone in the organization’s view is important in the decision making process, etc. Espoused values generally consist of the organization’s *official* viewpoints, such as mission- or vision-statements, strategy documents, and any other documents that describe the organization’s values, principles, ethics, and visions (Schein, 1999, p. 17). However, it is possible for two organizations to have very different observable artifacts and yet share very similar espoused values (Schein, 1999, pp. 18-19). This is because there is an even deeper level of thought and perception that drives the overt, or observable, behavior (Schein, 1999, p. 19). The espoused values are values which the organization *wants* to live up to. The interpretation, and application, of these espoused values in the day to running of the organization depends on the shared tacit assumptions between the employees of that organization.

- **Level Three: Shared Tacit Assumptions.** The *shared tacit assumptions* in an organization develop in any successful organization. Often these assumptions are formed in the organization’s early years, *because* certain strategies have proven to be successful (Schein, 1999, p. 19). If strategies based on specific beliefs and values continue to be successful, these beliefs and values gradually come to be shared and taken for granted. The beliefs and values become *tacit assumptions* about the nature of the world and how to succeed in it (Schein, 1999, p. 19). These values, beliefs, and assumptions that have become shared and taken for granted in an organization, form the essence of that organization’s culture. Beliefs, in this sense, refer to a group of people’s convictions about *the world and how it works*, whilst values refer to a community’s basic assumptions about *what ideals are worth pursuing* (Smit & Cronjé, 1992, p. 383). It is important to remember that the shared tacit assumptions resulted from a *joint learning process*.

The corporate *culture* of any organization, is a result of all three the above levels. At its most basic, and most difficult to quantify, level, the members of the organization share certain beliefs and values. These *shared tacit assumptions* act as a kind of ”filter”, which affects how individuals will carry out their normal day-to-day activities. It also influences how these individuals interpret the organization’s policies, and how they implement its procedures. These policies and procedures form part of the organization’s *espoused values*. The espoused values can be seen as the ”visible” contribution of the organization’s management towards the organization’s culture. To a degree, espoused

values provide cultural direction. The interpretation of this ”direction”, however, is extremely dependant on the underlying shared tacit assumptions. These three levels of corporate culture could be seen to correspond closely to the behavioral aspects of the ”human factor” in information security. As mentioned earlier, this ”human factor” in information security consist of two dimensions, namely knowledge and behavior, which are very inter-related. Due to the co-dependency between these two dimensions it is not possible to ignore the impact a lack of information security related knowledge would have on an organizational sub-culture of information security.

4 INFORMATION SECURITY CULTURE

In ”normal” definitions of organizational culture, the relevant job-related knowledge are generally ignored, because it can be assumed that the average employee would have the needed knowledge to do his/her job. In the case of information security, the required knowledge is not necessarily needed to perform the employee's *normal* job functions. Knowledge of information security is generally only needed when it is necessary to perform the *normal* job functions in a way that is consistent with good information security practices. It **can not be assumed** that the average employee has the necessary knowledge to perform his/her job in a secure manner. If an organization is trying to foster a sub-culture of information security, **all activities** would have to be performed in a way that is consistent with good information security practice. Having adequate **knowledge** regarding information security is a prerequisite to performing **any** normal activity in a secure manner. Information security knowledge, or a lack thereof, could therefor be seen as a fourth level to an information security culture that will affect each of the other three layers. For example:

Artifacts: Artifacts are *what actually happens* in the organization. Without the necessary skills and proficiencies, it would be impossible to perform security related tasks correctly. Thus, for the day-to-day task to happen in a secure way, the users would have to have sufficient knowledge of **how** to perform their tasks securely.

Espoused Values: To create the policy document, the person, or team, responsible for the drafting of the policy must know **what** to include in such a policy in order to adequately address the organization's security needs.

Shared Tacit Assumptions: This layer consists of the beliefs and values of employees. If such a belief should conflict with one of the espoused values, knowing **why** a specific control is needed, might play a vital role in ensuring compliance (Schlienger & Teufel, 2003).

It should be clear that in an information security culture, knowledge **underpins** and **supports** all three the ”normal” levels of corporate culture. Without adequate knowledge, information security cannot be ensured. The co-dependency between the three ”normal” levels of an organization's information security culture, and knowledge, the ”fourth level”, implies that each of these four levels will have an impact on how ”secure”, or desirable, the overall information security culture will be. The first part of the model presented in this paper is thus an adaptation of Schein's model. This adaptation incorporates the underlying need for information security related knowledge into Schein's model. Knowledge are added as a fourth level of culture that is specific to an information security culture. This adaptation is necessary because in an information security culture the requisite knowledge cannot be assumed to be present. Figure 1, provides a graphical exposition of this adaptation. In this presented conceptual model, knowledge is dealt with as an additional level to culture, as opposed to viewing knowledge as a sub-component of each of the original three levels. This is done solely because modeling knowledge as an additional level makes it easier to clearly show the effect knowledge, or a lack thereof, would have on the overall information security culture.

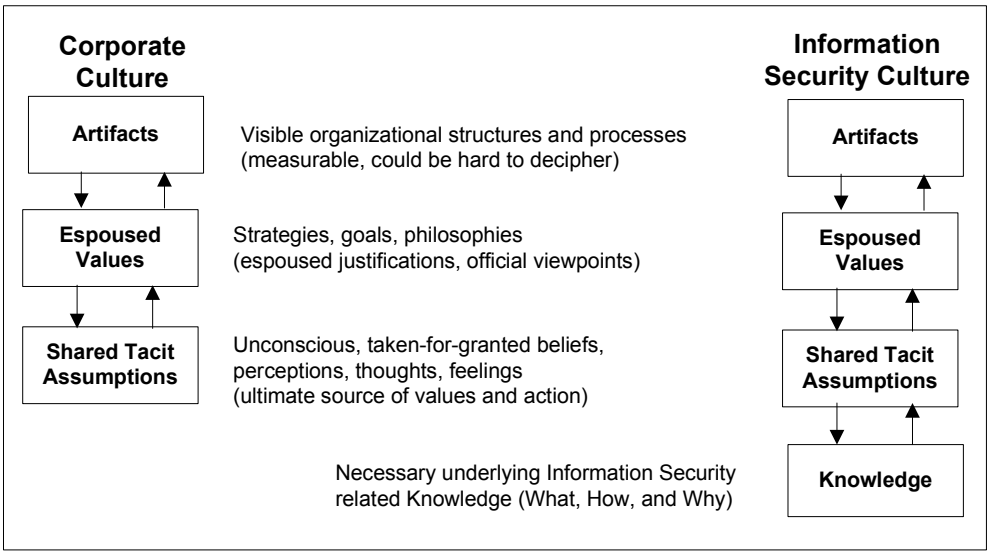

Figure 1: Levels of Culture (adapted from Schein, 1999, p. 16)

5 INFORMATION SECURITY CULTURE: A CONCEPTUAL FRAMEWORK

The overall effect of an organization's information security culture can be seen as an accumulation of the effects of each of the culture's underlying levels. Each of these levels can either positively or negatively influence the overall information security culture. In order to clearly demonstrate the

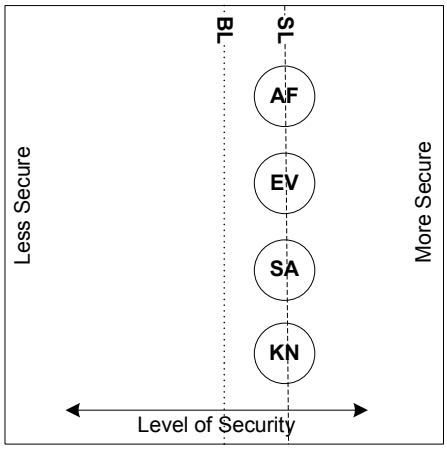

Figure 2: Basic Elements of the Conceptual Framework. *(BL = Minimum Acceptable Baseline, SL = Nett Security Level, AF= Artifacts, EV = Espoused Values, SA= Shared Tacit Assumptions, KN= Knowledge)*

interactions between these four levels, and their effects on the overall security efforts, it is necessary to first provide a basic reference framework.

5.1 Basic Elements and Terminology of the Conceptual Framework

The basic elements of this framework are depicted in Figure 2. The elements in Figure 2 can be described as follows:

- BL: Minimum Acceptable Base Line - This line indicates what would be an acceptable minimum security baseline. In other words, a culture whose net effect would meet the minimum requirements for some industry standard.
- SL: Nett Security Level - This line indicates the actual nett effect of the culture on the overall

security effort. This line can be seen as the cumulative effect of the four underlying levels of the culture. The nett security level (SL) can either be more secure (to the right), less secure (to the left), or just as secure (overlapping) as the minimum acceptable baseline (BL).

- AF: Artifacts - This node represents the relative *strength* of the artifact level (AF) of the culture. If this node is to the left of the minimum acceptable baseline (BL), it indicates that the measurable artifacts are not as secure as they should be. A node to the right of the baseline (BL) would indicate artifacts that are even more secure than the acceptable minimum. A node exactly on the baseline (BL) would indicate artifacts that are just as secure as required by this baseline.

- EV: Espoused Values - This node represents the relative *strength* of the organization's espoused value level (EV). The various policies and procedures comprising this level could be more, less, or just as comprehensive than those recommended as the minimum acceptable baseline.

- SA: Shared Tacit Assumptions - This node represents the relative *strength* of the organization's shared tacit assumption level (SA). The underlying beliefs or values of the employees could be either more, less, or just as in favor of good secure practices as required by the minimum acceptable baseline.

- KN: Knowledge - This node represents how much knowledge the organization's employees have regarding information security. Employees can be more knowledgeable than a certain minimum level needed to perform their jobs securely, they could be less knowledgeable, or they could have exactly the minimum requisite level of knowledge.

As mentioned above, the horizontal alignment of the nodes representing the various cultural levels, AF, EV, SA and KN, in comparison to the minimum acceptable baseline, should be interpreted as an indication of the relative *strength* of each level. In a similar fashion, the horizontal alignment of the nodes in comparison to the same horizontal alignment of the **other** levels should be interpreted as an indication of how *stable*, or predictable, the culture is. The nett security level line (SL) is an indication of the average strength of the culture, or the nett combined effect of all four the levels. The culture depicted in Figure 2 should thus, firstly, be interpreted as a *strong*, or secure culture. All four levels in Figure 2 has a strength greater than the baseline, which also results in a nett security level that is positive, or greater than the baseline. Secondly, all four levels are perfectly aligned with each other. This results in a culture that should be completely *stable*, or predictable. The culture depicted in Figure 2 could thus be said to be the *ideal* culture in terms of information security since it is both *strong* and *stable*.

The terms *strong*, and *stable*, as used above, should not be confused as being indicative of how pervasive or resistent to change the culture might be. According to Schein (1999, pp. 25-26), corporate culture is always strong in the sense of affecting every single aspect of daily life in an organization at a more than superficial level. Culture is also always stable, in the sense that it resists attempts at changing it. In that sense, culture is one of the most stable facets in an organization (Schein, 1999, p. 26). When referring to an **information security culture**, the term *strong*, as used in this paper, should be interpreted as a **desirable** culture that is conductive to information security. The term *stable*, as used in the same context, should be interpreted as an indication of how **predictable** the resulting artifacts, or nett security level of the culture would be for any specific scenario.

All of the factors mentioned above would contribute to the overall desirability of an information security culture. How *strong*, and *stable* an organization's information security culture is, would depend on the interaction between the various levels of culture.

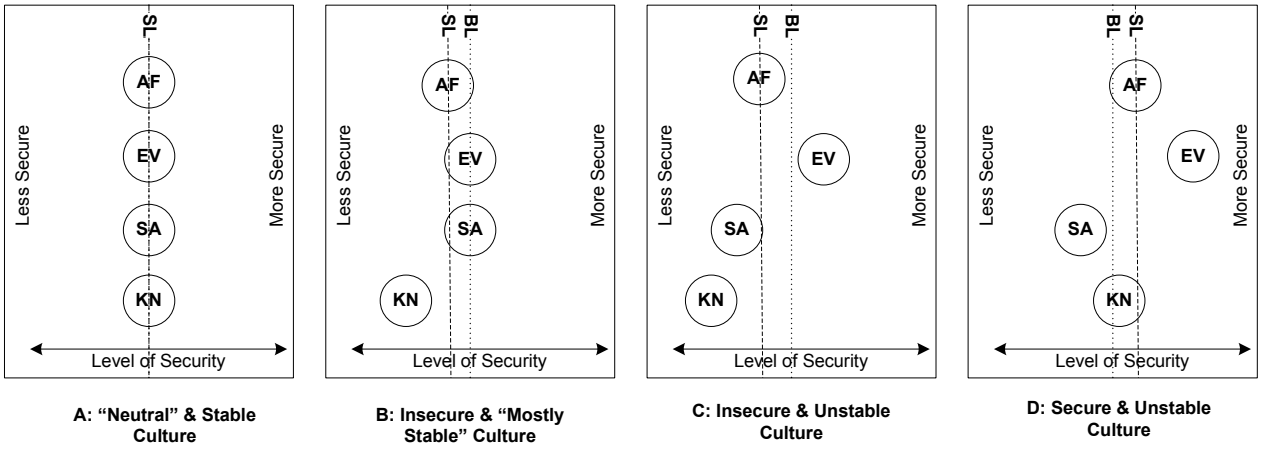

Figure 3: Possible interactions between the various levels of an Information Security Culture. *(BL = Minimum Acceptable Baseline, SL = Nett Security Level, AF= Artifacts, EV = Espoused Values, SA= Shared Tacit Assumptions, KN= Knowledge)*

5.2 Interpreting the Conceptual Framework

Each of the underlying cultural levels will contribute towards the overall strength and stability of such a culture. For example, if an organization has espoused values that are in line with recommended best practices for security, this would make the overall security better. Conversely, should the espoused values fail to address all relevant security related issues, the overall security would be weaker.

The combination of the espoused values, and the ”filtering effect” of the shared tacit assumptions and the user knowledge, on these espoused values, results in the visible, and measurable *artifacts*. From a security viewpoint, the artifact level is a very good indication of the overall security of the organization's information, since this level reflects what *actually happens* in the day to day operations. Fig. 3 shows a few possible effects interactions between the various levels of culture could have on the overall state of the organization's information security.

The examples in Fig. 3 assumes that the desirability of the various levels can be quantified and normalized to the same scale. In other words, it is assumed that, for example, the desirability of the relevant espoused values can be measured and expressed as a value that indicates the contribution of this level towards the overall security. It is also assumed that the other levels can be expressed in the same way, and that the scale of such measurements can be normalized in such a way that these values will indicate the relative desirability of that level when compared to the other levels. The line marked **SL**(*Security Level*) represents the nett effect of the interactions between various levels of the culture. The four examples in Fig. 3 can be interpreted as follows:

- **A:”Neutral” and Stable**. The desirability of the various levels of culture are ”neutral”, or average. In other words the *strength* of each level neither exceeds, nor falls short, of the minimum acceptable baseline standards. Since all the levels have the same level of desirability, the various levels will neither negate nor reinforce the effects of other levels on the overall security. The effects of such a culture would thus be predictable and stable.

- **B:Insecure and ”Mostly Stable”**. Both the espoused values and the shared tacit assumptions in this culture are of sufficient *strength* to meet the minimum acceptable baseline standard. However, in this culture, the employees do not have the requisite level of information security related knowledge. It is thus possible for the measurable artifacts to fall short of the minimum acceptable baseline. For example, either the policy dealing with a specific control might be lacking because the person(s) responsible for creating the policy lack the necessary knowledge, or the knowledge needed to implement this control in day-to-day operations might be lack-

ing amongst the responsible employees. In both such cases, the resulting artifacts *might* be weaker than expected. This misalignment between the various levels also means that it would be difficult to predict the exact relative strength of the overall security level. In this case one could probably assume the culture will be mostly predictable, hence stable, because the lack of knowledge would probably not apply equally to all controls.

- **C:Insecure and Unstable**. The various levels contributing to the culture are not aligned. This would mean that the nett effects of the culture might be unpredictable, due to the opposing forces at play in this culture. The espoused values are very desirable, but the users lack the requisite knowledge and do not have the desired beliefs and values, resulting in a measurable artifact level that is not secure. For any specific security control, a user may, or may not, have the requisite knowledge to fulfill his/her role in the implementation of that specific control. That same user could also agree with the relevant espoused value, or could have beliefs that are contrary to that espoused value. It would thus be very difficult to predict the nett security level of this culture. Such a culture would not be a desirable culture.

- **D:Secure and Unstable**. The various levels contributing to the culture are not aligned. The espoused values are desirable, and the users have adequate knowledge. The high level of user knowledge in this case somewhat negates the fact that the users do not have the desired beliefs and values, resulting in an overall culture that is more secure than the minimum acceptable baseline. However, this culture should be considered not desirable, because its effects cannot always be predicted. It might be possible for the users to behave insecurely with regards to a specific security control because the specific control conflicts with their beliefs (Schlienger & Teufel, 2003).

The above examples only reflect a few possible scenarios. It should however be clear that the nett effect of any information security culture can be influenced, either positively, or negatively, by how ”secure” the underlying levels of such a culture is. In such a model it might also be possible to deduce the relative state of one or more of the cultural levels. For example, if the organization has *good* espoused values, but the measurable artifacts indicate *bad* security, it might be inferred that the employees lack either the required knowledge or the desired attitude.

6 CONCLUSION

This paper suggested that, for an effective information security culture, the requisite information security knowledge amongst an organization’s users could be seen as a fourth layer to Schein’s (Schein, 1999) model for corporate culture. The various interactions between the layers of such an information security culture were then presented conceptually.

The conceptual model presented showed that the nett overall effect that an information security culture would have on the organization’s information security efforts would depend on the relative desirability, or *strength*, of each underlying level in such a culture. Furthermore, the alignment of the strengths of the individual underlying culture levels relative to the other levels, would to a large extend determine how predictable, hence *stable*, the effects of such a culture would be. The ideal culture would thus be one where all four underlying levels are stronger than the minimum acceptable baseline, and are also perfectly aligned relative to each other. The example in Figure 2 would be such an *ideal* culture.

The assumption made when presenting the example, namely that the desirability of the various levels can be quantified and normalized to the same scale, should by no means be taken as an assertion made by this paper. The aim of the paper was not to present such metrics and normalization processes but rather to show, at a certain level of abstraction, how this conceptual model could be used to reason about information security culture. It should, however, be possible to quantify and normalize the

various factors for certain subsets of controls. For example, it might be possible to turn the presented conceptual model into a working model for a smaller sub-problem such as mapping the relationships between the four levels for password usage. If the required processes and metrics are developed, the conceptual framework might also play a valuable role in the management of an information security culture. This type of usage for the presented model could possible be included in future research efforts. For the present, the contention of this paper is simply that the conceptual model presented, could assist in improving the understanding of an information security culture. The work in this paper should thus be seen as an attempt to lay a solid foundation on which future research could be built.

7 REFERENCES

Creswell, J. W. (1998). *Qualitative inquiry and research design: Choosing among five traditions. thousand oaks, ca: Sage, 1998*. Thousand Oaks, CA: Sage.

Eloff, M. M., & Von Solms, S. H. (2000). Information security management: An approach to combine process certification and product evaluation. *Computers & Security*, *19*(8), 698–709.

International Standards Organization. (2004). *ISO/IEC TR 13335-1:2004 Guidelines to the Management of Information Technology Security (GMITS). Part1: Concepts and models for IT security. ISO/IEC, JTC 1, SC27, WG 1*.

Mitnick, K., & Simon, W. (2002). *The art of deception: Controlling the human element of security*. Wiley Publishing.

Nosworthy, J. D. (2000). Implementing information security in the 21st century - do you have the balancing factors? *Computers & Security*, *19*(4), 337–347.

Schein, E. H. (1999). *The corporate culture survival guide*. Jossey-Bass Inc.

Schlienger, T., & Teufel, S. (2003). Information security culture - from analysis to change. *Information Security South Africa (ISSA), Johannesburg, South Africa*.

Siponen, M. (2001). Five dimensions of information security awareness. *Computers and Society, June 2001*, 24-29.

Smit, P. J., & Cronjé, G. J. d. J. (1992). *Management Principles: A Contemporary South African Edition*. JUTA.

Van Niekerk, J., & Von Solms, R. (2005). An holistic framework for the fostering of an information security sub-culture in organizations. *Information Security South Africa (ISSA), Johannesburg, South Africa*.

Von Solms, B. (2000). Information security - the third wave? *Computers & Security*, *19*(7), 615–620.

8 ACKNOWLEDGEMENTS

The financial assistance of National Research Foundation (NRF) towards this research is hereby acknowledged. Opinions expressed and conclusions arrived at, are those of the author and are not necessarily to be attributed to the National Research Foundation.