available at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Information security culture: A management perspective

*J.F. Van Niekerk**, *R. Von Solms*

Institute for Information and Communication Technology Advancement, Nelson Mandela Metropolitan University, South Africa

ARTICLE INFO

Article history:
Received 30 October 2008
Received in revised form
19 October 2009
Accepted 20 October 2009

Keywords:
Information security
Information security culture
Corporate culture
Organizational learning
Schein's model

ABSTRACT

Information technology has become an integral part of modern life. Today, the use of information permeates every aspect of both business and private lives. Most organizations need information systems to survive and prosper and thus need to be serious about protecting their information assets. Many of the processes needed to protect these information assets are, to a large extent, dependent on human cooperated behavior. Employees, whether intentionally or through negligence, often due to a lack of knowledge, are the *greatest threat* to information security. It has become widely accepted that the establishment of an organizational sub-culture of information security is *key* to managing the human factors involved in information security. This paper briefly examines the *generic* concept of corporate culture and then borrows from the management and economical sciences to present a conceptual model of information security culture. The presented model incorporates the concept of *elasticity* from the economical sciences in order to show how various variables in an information security culture influence each other. The purpose of the presented model is to facilitate conceptual thinking and argumentation about information security culture.

1. Introduction

Today information can be seen as a basic commodity, similar to electricity, without which many businesses simply **cannot** operate (Carr, 2003). Unfortunately, in the interconnected world we live in, information is a lot more vulnerable than other basic commodities. It is highly unlikely that the actions of a discontent teenager on another continent can affect a company's electricity supply. The same cannot necessarily be said about the availability of information resources. It is thus vital for organizations to ensure their continued access to this commodity by protecting their information assets.

Many organizations will be unable to do business without access to their information resources. However, protecting these information resources often has no direct return on investment. Securing information resources does not as a rule generate income for an organization. Business people are therefore rarely interested in how their information resources are protected. From a business perspective, any solution would be adequate as long as it is cost-effective and takes into account issues such as productivity and ease of use (Wylder, 2004, p. 6). It can thus be argued that the goal of securing information is, to a certain extent, in conflict with the normal business goals of maximizing productivity and minimizing cost. Security is often seen as detrimental to business goals because it makes systems less usable. According to Wood (2005, p. 224) the only absolutely secure system is an unusable one.

This conflict between business and security objectives has become so well recognized, that the ability to resolve such conflicts should be seen as a key performance indicator for information security officers (Wood, 2005, p. 224). It can also be argued that the problem of managing information security, to a certain extent, is nothing more than the management of

* *Corresponding author*. School of ICT, PO Box 77000, Port Elizabeth 6031, South Africa. Tel.: +27 41 5043048; fax: +27 41 5043313.
E-mail addresses: johanvn@nmmu.ac.za (J.F. Van Niekerk), rossouw@nmmu.ac.za (R. Von Solms).
0167-4048/$ – see front matter © 2009 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2009.10.005

many similar conflicts. These "conflicts of interests" are of special importance once one starts dealing with the role(s) humans play in the information security process. Information security consists of many processes. Some of these processes are, to a large extent, dependent on human cooperated behavior. Employees, whether intentionally or through negligence, often due to a lack of knowledge, are the *greatest threat* to information security (Mitnick and 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".

Many recent studies have shown that the establishment of an **information security culture** in the organization is **necessary** for effective information security (Eloff and Von Solms, 2000; Von Solms, 2000). Through the establishment of such a culture, the employees can become a security asset, instead of being a risk (Von Solms, 2000). However, even with such a culture in place there still exist certain "trade offs" and "conflicts of interests" that should be managed. This paper aims to provide a conceptual framework to assist readers in understanding the interactions at various levels of such an information security culture. It is hoped that this framework, which incorporates elements of both managerial and economical science, will promote better understanding of information security culture amongst readers from a managerial background.

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". The work presented in this paper is a continuation, an expansion, of work previously published by the authors (Van Niekerk and Von Solms, 2006). 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 and 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 a 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 attempts 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 existing 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 and Cronjé, 1992, p. 382). Such a culture could be defined as; the **beliefs** and **values** shared by people in an organization (Smit and Cronjé, 1992, p. 382). Beliefs and values, however, are both concepts that can be difficult to quantify. It is therefore 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 and 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 and Teufel, 2003). In order to clarify these levels of culture, each of the levels will be briefly examined:

- **Level One: Artifacts**. Artifacts are what can be observed, seen, heard, and felt, 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 consists 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-day running of the organization depend 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 and 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 consists 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 is generally ignored, because it can be assumed that the average employee would have the required 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 **cannot 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 therefore be seen s a fourth level to an information security culture that will affect each of the other three layers. For example:

4.1. *Artifacts*

Artifacts are *what actually happens* in the organization. Without the necessary skills and proficiencies, it would be impossible to perform information related tasks securely. 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.

4.2. *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.

4.3. *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 and 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 is 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**. Fig. 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 that knowledge, or a lack thereof, would have on the overall information security culture.

In order to ensure an adequate level of information security knowledge, international standards such as ISO/IEC 27002 (International Standards Organization, 2005) recommends the use of an organizational information security awareness campaign. Awareness campaigns address the problems that a lack of knowledge could lead to. These campaigns help to create a culture of information security, by instilling the aspects of information security in every employee as a natural way of performing his or her daily job (Von Solms, 2000). Awareness campaign is **the** key element in ensuring that the knowledge level of an information security culture is of adequate "strength".

Before the interactions between the above levels of an information security culture can be examined in more depth, a final "tool" is needed. The model presented later in this paper also needs to borrow the concept of *elasticity* from the economical sciences.

5. Elasticity in information security culture

Elasticity is a general economic concept that measures the *change in one variable caused by changes in other, related variables* (Acs and Gerlowski, 1996, p. 49). In other words, elasticity measures how *sensitive* a variable is *to change* in another variable. In the presented model, the concept of elasticity will be borrowed, but instead of attempting to **measure** the change the concept will simply be used to explain the fact that change will be inherent in any such system and that the speed at which such change takes place depends on the *degree of elasticity* in the system. In order to provide more clarity of exactly what is meant by elasticity, another basic idea will first be borrowed from the economical sciences. Fig. 2 shows a basic supply and a basic demand curve. According to economic theory (Acs and Gerlowski, 1996, p. 45) the market will be in *equilibrium* if the quantity of goods or services demanded in the market is matched perfectly by the quantity of goods or services supplied in this market. In such a system, assuming all other variables are fixed, the price that could be asked for the goods or services would be perfectly static **and predictable**.

If, however, one of the variables in such a market were to change, for example if an increase in the quantity of goods or services demanded was to occur, the equilibrium would be disturbed. In such a case the other variable, the quantity of goods or services supplied would have to increase to match the increase in demand in order to bring the system back into equilibrium. While this situation of *disequilibrium*, exists, the price that could be asked for the goods or services supplied, would be more dynamic and **difficult to predict**. In Fig. 3, the price could fall anywhere in the shaded area, due to the increase in demand.

The term **elasticity** is used in economics to describe the relationship, shown in the above system, whereby increased demand would **cause** an increase in supply to eventually bring the system back into equilibrium. However, not all systems would have the same inherent *degree of elasticity*. Elasticity could in fact range from systems that are *infinitely elastic* to systems that are completely *inelastic*. In an infinitely elastic system, shown in Fig. 4, an increase in supply would have no effect on either the demand or the price people would be willing to pay. Fig. 4 thus does not even show the supply curve since its position in such a perfectly elastic system is irrelevant in determining the price. On the other hand, in a completely inelastic system, shown in Fig. 5, the variables would be "locked together". The supply and demand would thus always stay in equilibrium (Acs and Gerlowski, 1996, p. x). An example of such an inelastic system would be certain types of life saving medicines. People who need such medicines would be willing to pay **any** price for such medicines. For the purposes of this paper it is also important to note that in such an inelastic system consumers would be willing to pay any

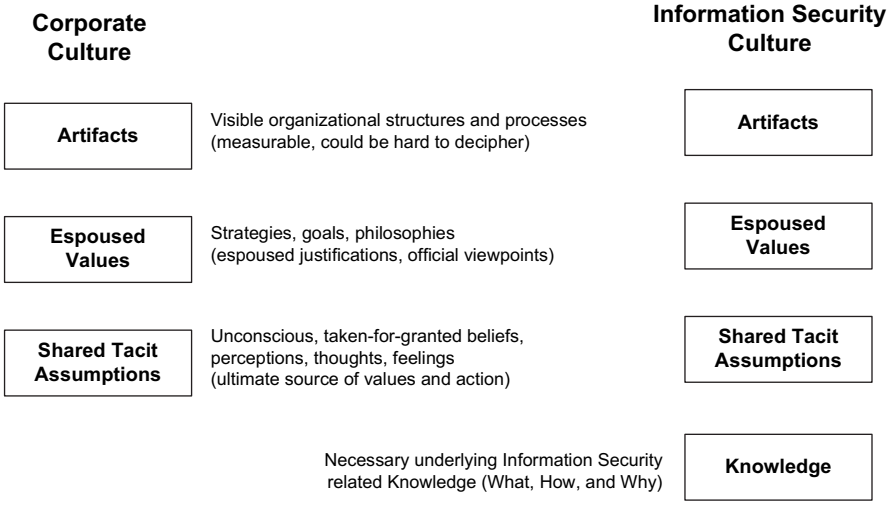

Fig. 1 – Levels of culture. Adapted from Schein (1999, p. 16).

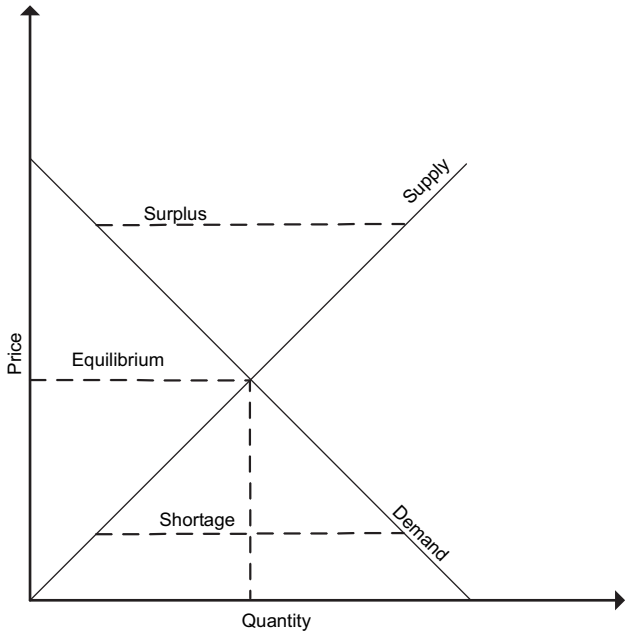

Fig. 2 – Market equilibrium (Acs and Gerlowski, 1996, p. 47).

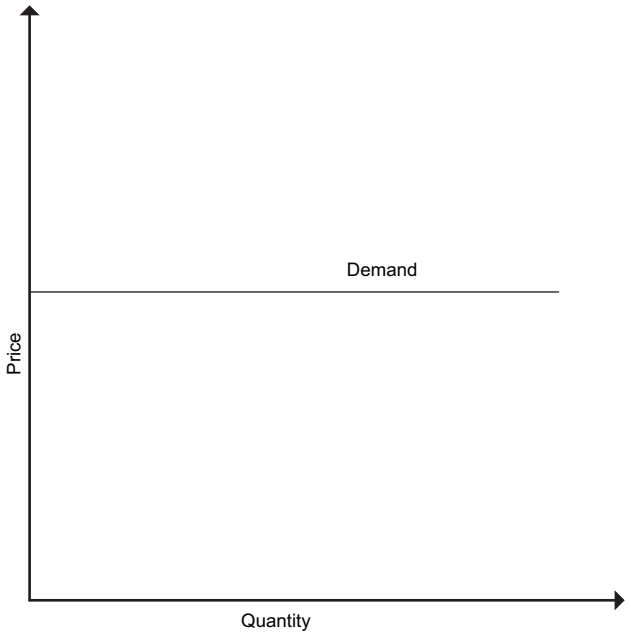

Fig. 4 – Perfectly elastic demand curve (Acs and Gerlowski, 1996, p. 52).

price but can only do so *if they have the necessary means*. Without the necessary means even consumers who are willing to pay any price would still be unable to do so.

A very **similar** situation to the one demonstrated above also exists when one looks at the human factors in an organization's information security environment. As discussed earlier, two of the basic ''levels'' of an information security culture would be the company's espoused values and the employees' shared tacit assumptions. To a certain extent, it can be argued that the policies and procedures comprising the espoused values in an information security culture are an indication of how much security management is ''demanding'' from employees. Similarly, the shared tacit assumptions can be seen as a reflection of how much ''compliance'' employees are willing to ''supply''. If one were to model these two ''supply'' and ''demand'' curves, the intersection of these curves would be an indication of the actual amount of effort employees are willing to give. In other words, the ''price'' in this case would be the measurable

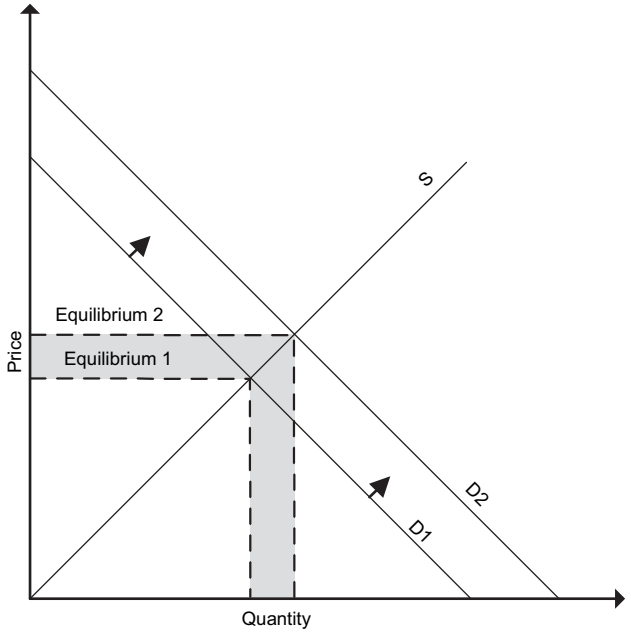

Fig. 3 – Change in equilibrium caused by increased demand. Adapted from Acs and Gerlowski (1996, p. 48).

Fig. 5 – Perfectly inelastic demand curve (Acs and Gerlowski, 1996, p. 52).

employee participation in the organization's security efforts. Similarly, having the requisite knowledge to be able to participate in these security efforts is analogous to having the means to pay the required price. Such a system is modeled in Fig. 6. If the management expectations are in perfect equilibrium with the employees' shared tacit assumptions, the resulting effort employees expended on behalf of the organization's information security would be perfectly predictable (Fig. 6). Should management expect more than employees are willing to provide, it would be less easy to predict the actual amount of effort employees would expend towards the overall security goals (Fig. 7). It should also be clear that employees who are in fact willing to perform their security related roles would only be able to do so if they have the requisite knowledge.

In an information security culture there exists a causal relationship between the artifact level and the other three levels. In other words: the visible artifacts or, "how the employees *actually* behave towards information security", is caused by the combined effects of the espoused values, the shared tacit assumptions and the underlying information security knowledge. In Fig. 6 the artifact level is represented by the intersection of the lines. In Fig. 7 the artifact level is represented by the shaded area between the two possible intersection points. This reflects the fact that it would be difficult to predict how employees will actually behave (artifacts) in a scenario where management demands (espoused values) and the effort employees are willing (shared tacit assumptions), or able (knowledge), to supply are not in equilibrium. In such a causal relationship elasticity plays an important role. More "demanding" espoused values will have an elastic effect on the artifacts, and will require a matching increase in the shared tacit assumptions and/or the knowledge level(s). Thus, if an organization's management increases the "strength" of the organization's security related policies and procedures,

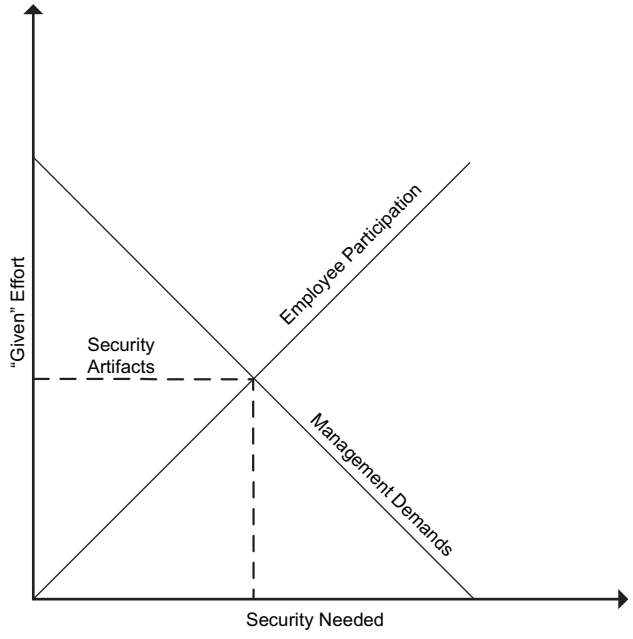

Fig. 6 – Management expectations in equilibrium with employee's security contribution. Adapted from Acs and Gerlowski (1996, p. 47).

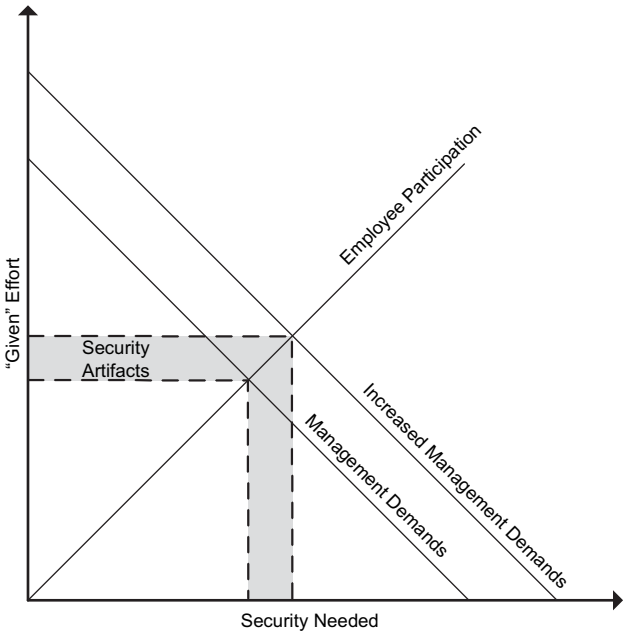

Fig. 7 – Increased management expectations require increased employee participation. Adapted from Acs and Gerlowski (1996, p. 48).

the "demand" (security needed) will increase in Figs. 6 and 7. Such an increase will in turn require an increase in how much "security effort" employees are willing to give, or an increase in the security related knowledge of employees, or an increase in both. Without such matching increases in the other levels of the security culture, the culture will not be in equilibrium and it would thus become more difficult to predict the resulting employee behavior (artifacts).

In order to simplify the representation of the elasticity concept, it should be noted that the dynamic system represented in Figs. 6 and 7 currently does not explicitly show the knowledge level. The knowledge level should, however, be assumed present in all cases. As mentioned above, this level can be seen as representing the ability to "pay" the demanded "price", and as such will have an equally important effect on the resulting employee behavior (artifacts) as the other two levels. The conceptual framework presented in the rest of this paper will attempt to clarify this causal relationship between the artifact level and the other three levels of an information security culture.

6. 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 information security culture. In order to clearly demonstrate the interactions between these four levels, and their effects on the overall security efforts, it is necessary to first provide a basic reference framework.

6.1. *Basic elements and terminology of the conceptual framework*

The basic elements of this framework are depicted in Fig. 8. The representation in this and subsequent figures was chosen over the basic curves used in Figs. 2 and 3, because it is easier to model all the interactions in this way, rather than adding an additional dimension to the model used to examine the concept of elasticity. The elements in Fig. 8 can be described as follows:

- BL: Minimum Acceptable Baseline – 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.

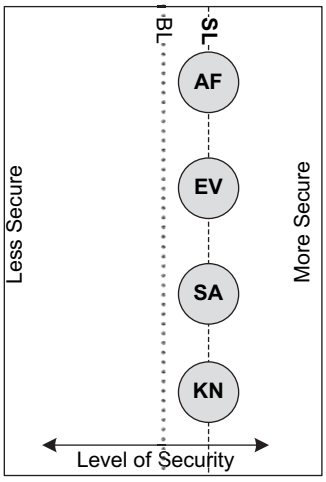

Fig. 8 – Basic elements of the conceptual framework. (BL = minimum acceptable baseline, SL = nett security level, AF = artifacts, EV = espoused values, SA = shared tacit assumptions, KN = knowledge.)

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 Fig. 8 should thus, firstly, be interpreted as a *strong*, or secure culture. All four levels in Fig. 8 have 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. One could also say that this would be perfect cultural *equilibrium*. The culture depicted in Fig. 8 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 conducive 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.

6.2. *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 ''elasticity 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. In cases where the various levels are not in equilibrium this artifact level becomes more difficult to predict. In such cases the degree of elasticity in the specific system would determine how long it would take before the system ''settles'' into equilibrium. In infinitely elastic systems this equilibrium might never be attained, whilst completely inelastic systems would always be in equilibrium. In terms of the degree of elasticity in a security culture, the knowledge level also plays a very specific role in that it can act as an ''inhibitor'' of the elastic effect. A lack of knowledge can prevent employees who want to act securely from doing so. For the specific areas where the necessary security knowledge is lacking, this lack results in an infinite degree of elasticity in the security culture. The visible behavior (artifact level) cannot move towards equilibrium because the employees lack the means to provide the desired behavior.

Figs. 9–13 show 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 Figs. 9–13 assume 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 five examples can be interpreted as follows:

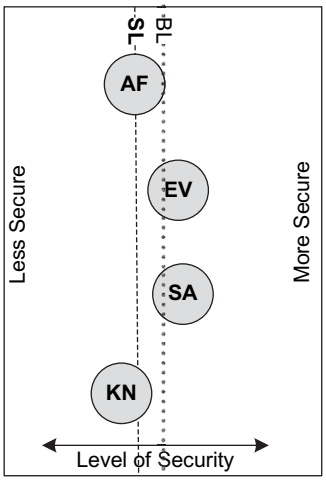

Fig. 10 – Insecure and ''Mostly Stable'' Culture. (BL = minimum acceptable baseline, SL = nett security level, AF = artifacts, EV = espoused values, SA = shared tacit assumptions, KN = knowledge.)

''Neutral'' and Stable (Fig. 9). The desirability of the various levels of culture is ''neutral'', or average. In other words the *strength* of each level neither exceeds, nor falls short, of the minimum acceptable baseline standards. The Nett Security Level (SL) perfectly overlaps the Baseline (BL). 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.

Insecure and ''Mostly Stable'' (Fig. 10). 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

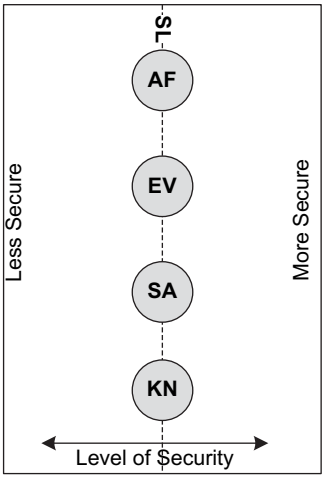

Fig. 9 – ''Neutral'' and stable culture. (BL = minimum acceptable baseline, SL = nett security level, AF = artifacts, EV = espoused values, SA = shared tacit assumptions, KN = knowledge.)

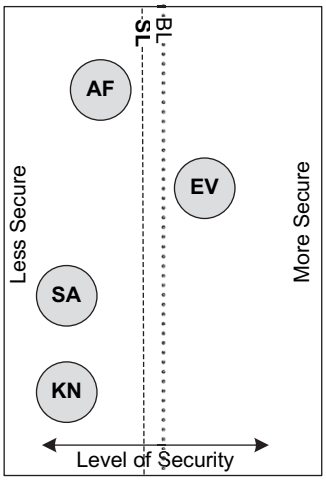

Fig. 11 – Insecure and unstable culture. (BL = minimum acceptable baseline, SL = nett security level, AF = artifacts, EV = espoused values, SA = shared tacit assumptions, KN = knowledge.)

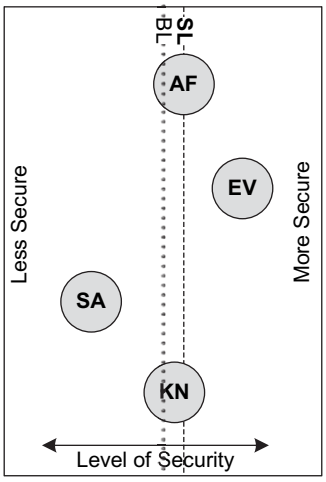

Fig. 12 – Secure and unstable culture. (BL = minimum acceptable baseline, SL = nett security level, AF = artifacts, EV = espoused values, SA = shared tacit assumptions, KN = knowledge.)

policy dealing with a specific control might be lacking because the person(s) responsible for creating the policy lacks the necessary knowledge, or the knowledge needed to implement this control in day-to-day operations might be lacking 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 that the culture will be mostly predictable, hence stable, because the lack of knowledge would probably not apply equally to all controls. This culture would also have an almost infinite degree of elasticity and the artifacts would thus never perfectly align with the espoused values and shared tacit assumptions. This is due to the lack of supporting information security knowledge. The lack of knowledge acts as an

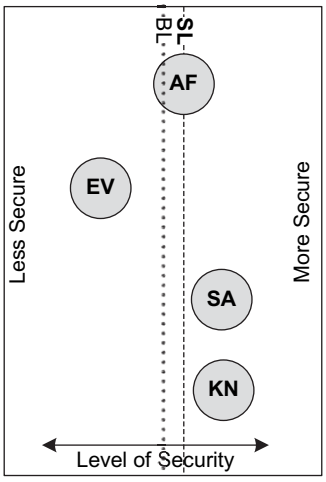

Fig. 13 – Secure and unstable culture. (BL = minimum acceptable baseline, SL = nett security level, AF = artifacts, EV = espoused values, SA = shared tacit assumptions, KN = knowledge.)

"anchor" and prevents the artifacts from aligning with the other layers. By addressing the lack of knowledge the degree of elasticity inherent in this culture could be reduced. This would increase the rate at which a more desirable state is reached where the artifacts align with the shared tacit assumptions and espoused values.

Insecure and Unstable (Fig. 11). 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. In order to make this culture more desirable it would be necessary to address both the lack of knowledge and the underlying shared tacit assumptions of the employees. Once these aspects have been addressed the various levels of the culture will re-align to become more "stable". The rate at which this re-alignment will take place would be dependent on the degree of elasticity present in the system.

Secure and Unstable (Fig. 12). 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 and Teufel, 2003). In this culture the knowledge level is already sufficient to enable employees to behave securely. However, there is still a gap between the knowledge level and the espoused values. This gap will have to be addressed before the culture could possibly align with the espoused values. The degree of elasticity in this culture could be reduced by addressing the shared tacit assumptions of employees. If employees can be convinced of the importance of their respective roles and responsibilities towards the organization's information security the culture *should* start to align itself.

Secure and Unstable (Fig. 13). As in Fig. 12 the various levels contributing to the culture are not aligned. In this case the figure models the scenario where the organization is small and all staff are skilled IT professionals who have both the requisite knowledge levels and the personal belief systems that enable secure behavior. In such a case it is quite likely to have a secure artifact level **despite** the fact that there are little or no espoused values. This is still not a desirable culture. Without adequate security policies (espoused values) in place, there can be no guarantees of desirable behavior. The appointment of additional staff members who might lack the

underlying security knowledge can easily move the observable artifacts in this model back towards the less secure side. Unless the organization actively addresses the lack of espoused values this culture will have an infinite degree of elasticity. The espoused values will never align themselves without active intervention.

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. In the cultures represented by Figs. 12 and 13 the culture can probably be ''improved'' by involving employees in the process of creating the espoused values. In both these cultures involving the employees in a ''negotiation'' process when creating espoused values could reduce the ''gap'' between the espoused values and shared tacit assumption layers. In both cases this would make the culture more predictable, and thus more desirable. In all cases insight into the degree of elasticity inherent in the culture can help guide decisions as to what course would be most appropriate to help manage the culture. If a system has infinite elasticity it will never align itself unless the underlying cause for this infinite elasticity is addressed. If management wants to see faster changes at the artifacts layer, i.e. how people behave on a day-to-day basis, steps should be taken to decrease the degree of elasticity. From a management perspective, the ''perfect security culture'' would be one that is completely inelastic. Such a culture will always instantly reflect changes in the espoused values of the organization.

7. 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 (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 extent 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 Fig. 8 would be such an *ideal* culture.

The model also attempted to show that management demands and employees' participation are strongly interrelated. In an information security culture the visible artifacts are thus dependent on both the supporting knowledge as well as this relationship between espoused values (management demands) and shared tacit assumptions (employees' underlying beliefs and values). In any information security culture a certain degree of elasticity will be present. This elasticity will determine whether or not the shared tacit assumptions will over time align itself to the espoused values of the organization. It will also determine how fast changes will occur if the system is not infinitely elastic. The lower the degree of elasticity in the system, the faster it would take for a possible re-alignment to happen. From a management perspective it would thus be highly desirable to reduce the degree of elasticity in such a culture as much as possible.

In its current form, the model's primary contribution is at a *conceptual* level where it aids in the understanding of information security culture. The current model has limited ''hands-on'' use. In a scenario where an organization's measurable artifacts are undesirable, a manager who is sure that the organization's espoused values is of adequate strength and who is also certain his/her staff members have adequate knowledge, might infer that the employees' beliefs and values are not in line with the espoused values. Based on the presented model, such a manager will also be able to deduce that he/she can make the artifacts easier to predict by addressing the shared tacit assumptions, for example by trying to convince the employees to buy into the espoused values. Through campaigns aimed at improving the employees' attitude towards security management can reduce the degree of elasticity inherent in the culture and thus speed up the pace at which the measurable artifacts become more in line with the espoused values. Alternatively the espoused values could be ''relaxed'' to be more in line with the shared tacit assumptions, similar to the idea of adjusting the governing variables in a double-loop learning system (Smith, 2001). This might result in a culture that is slightly less secure but more predictable.

In either of the above mentioned approaches, use of the current model would only provide very vague guidance to someone wanting to manage an information security culture. In order for this model to become useful as a ''hands-on'' cultural management tool additional research would be required. If one could accurately quantify and normalize the various levels at play in this conceptual model it should be possible to use the model to manage specific aspects of an information security culture more precisely. The assumption made when presenting the example, namely that the desirability of the various levels can in fact 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. For example; a metric that

quantifies the actual degree of elasticity in an information security culture would be a very useful tool to have. This type of usage for the presented model could possibly be addressed by 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.

Appendix. Supplementary data

Supplementary data associated with this article can be found in the online version at doi:10.1016/j.cose.2009.10.005.

REFERENCES

Acs ZJ, Gerlowski DA. Manegerial economics and organization. Prentice Hall; 1996.

Carr NG. It doesn't matter. Harvard Business Review 2003:41–9.

Creswell JW. Qualitative inquiry and research design: choosing among five traditions. Thousand Oaks, CA: Sage; 1998.

Eloff MM, Von Solms SH. Information security management: an approach to combine process certification and product evaluation. Computers & Security 2000;19(8):698–709.

International Standards Organization. ISO/IEC 27002: code of practice for information security management; 2005.

Mitnick KD, Simon WL. The art of deception: controlling the human element of security. Wiley Publishing; 2002.

Schein EH. The corporate culture survival guide. Jossey-Bass Inc.; 1999.

Schlienger T, Teufel S. Information security culture – from analysis to change. Johannesburg, South Africa: Information Security South Africa (ISSA); 2003.

Siponen MT. Five dimensions of information security awareness. Computers and Society 2001:24–9.

Smith MK. Chris Argyris: theories of action, double-loop learning and organizational learning [WWW document]. URL, http://www.infed.org/thinkers/argyris.htm; 2001. Sited 4 March 2004.

Smit PJ, Cronjé GJde J. Management principles: a contemporary South African edition. JUTA; 1992.

Van Niekerk J, Von Solms R. Understanding information security culture: a conceptual framework. Johannesburg, South Africa: Information Security South Africa (ISSA); 2006.

Von Solms B. Information security – the third wave? Computers & Security 2000;19(7):615–20.

Wood CC. Information security roles & responsibilities made easy. Information Shield. 2nd ed.; 2005.

Wylder J. Strategic information security. CRC Press; 2004.

Johan van Niekerk is a senior lecturer in the Department of Information Systems at the Nelson Mandela Metropolitan University. He has been in the employ of the NMMU for the past 13 years and has been a full-time academic for the past 9 years. He is currently working towards a PhD as part of the research efforts at the Institute for Information and Communication Technology Advancement. His research focuses on the human factors in information security.

Prof. Rossouw von Solms is a well know researcher in information security. He has had many previous publications in this field and is employed as a full-time researcher in the Institute for Information and Communication Technology Advancement at the Nelson Mandela Metropolitan University.