AN HOLISTIC FRAMEWORK FOR THE FOSTERING OF AN INFORMATION SECURITY SUB-CULTURE IN ORGANIZATIONS

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

Modern businesses operates in an emerging global information society. In this information society it is imperative for modern organizations to take the protection of their information resources seriously. This protection of information resources is to a large extent dependent on human co-operated behavior. This *human factor* is the weakest link in information security, and consists of two interrelated dimensions. Firstly, employees must have sufficient knowledge about information security in order to effectively implement, and maintain, the various information security controls. Secondly, the employees must have the correct attitude towards information security. These two dimensions to the human factor in information security are closely related, and to a degree co-dependent upon each other. It would thus make sense to address these dimensions holistically. This paper combines previously proposed principles and methodologies into a single holistic framework that addresses both the dimensions to this *human factor* in information security.

KEYWORDS

Information Security, Information Security Culture, Outcomes Based Education, Awareness, Double-loop Learning, Organizational Learning, Transformative Change Management.

AN HOLISTIC FRAMEWORK FOR THE FOSTERING OF AN INFORMATION SECURITY SUB-CULTURE IN ORGANIZATIONS

1 INTRODUCTION

Modern businesses operates in an emerging global information society. The current global economy is increasingly dependent on the creation, management, and distribution of information resources. Today, many organizations need information systems to survive and prosper. It is therefore imperative for modern organizations to take the protection of their information resources seriously. This protection of information resources is 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 (M. Thomson, 1998, p. 12),(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).

It is important to note that there are two dimensions to this ”human factor” in information security, namely knowledge, and cooperation, or *behavior*. These two dimensions to the human factor are, to a large degree, closely related to each other but will be briefly discussed separately in order to clarify the different emphasis of each.

1.1 Knowledge

Organizations cannot protect the integrity, confidentiality, and availability of information in today’s highly networked systems environment without ensuring that each person involved understands his/her roles and responsibilities and is adequately trained to perform them (NIST 800-16, 1998, p. 3). Thus, an individual user should be made aware of the specific operational controls that are dependant on his/her behavior in order to be effective. In order to ensure this required level of knowledge, extensive awareness, training and educational programs will be needed. The obvious question at this point would be to ask exactly what should users be taught?

ISO/IEC 17799 (2000) states that all employees of the organization and, where relevant, third party users, should receive appropriate training. This training should include security requirements, legal responsibilities and business controls, as well as training in the correct use of information processing facilities before access to information or services is granted (ISO/IEC 17799, 2000, p. 9). This statement, even though it greatly clarifies some issues relating to what should be taught in an information security educational program, raises another question namely, what is appropriate training?

Determining exactly how much knowledge a user requires can be a daunting task. It would make sense for an organization’s security educational program to cover all the controls specified by the specific information security standard used by the organization. However, it is clearly unreasonable to expect each and every end-user to be educated about all the controls specified by a standard such as the ISO/IEC 17799. According to ISO/IEC TR 13335-1 (2004) each employee should know his or her role and responsibility, his or her contribution to IT security, and should share the IT security vision (ISO/IEC TR 13335-1, 2004, p. 14). It is therefore necessary to tailor the educational material used to the needs of the individual user. The educational methodology used, should thus support this requirement. This paper will not deal with all the criteria such a selection process should adhere to. It should however be clear that, due to the important role user education plays in the information security process, it is *vital* to use a pedagogically sound methodology for the creation of such educational programs (Van Niekerk & Von Solms, 2004a). Van Niekerk and Von Solms (2003, 2004a) dealt with information security education and the requirements an educational methodology would have

to meet in order to be suitable for information security education extensively, and also introduced outcomes based education (OBE), as a methodology that could meet these predefined requirements (Van Niekerk & Von Solms, 2003, 2004a). 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. Outcomes based education cannot change corporate culture, since outcomes are not values, beliefs, attitudes, or psychological states of mind (Spady, 1994, p. 2).

1.2 Behavior

Most current user education programs fail to pay adequate attention to behavioral theories (Siponen, 2001). In order to change a learner's values, beliefs, attitudes, or psychological states of mind, **more** than just education will be required. The "strength" of current beliefs and values will also have a major impact on how easy or difficult it will be to change these beliefs and values. It is therefor important to realize that the learners in a corporate information security education program will, in most cases, be **adults**. Adults have well established values, beliefs, and opinions, as opposed to the formative beliefs, values, and opinions of children. In addition to this, adults may have had differing education, varying years of experience, and a wealth of previously learned information (NIST 800-16, 1998, p. 21). Adults relate new information and knowledge to previously learned information, experiences, and values. This happens both consciously and unconsciously, and could lead to misperception and miscommunication (NIST 800-16, 1998, p. 21).

To counter these risks and thereby address the second dimension to the human factor, 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).

A detailed examination of corporate culture falls outside the scope of this paper, instead the definition of corporate culture as presented by Schein (1999a) will be used. This definition is commonly applied to an information security culture (K. Thomson & Von Solms, 2004; Schlienger & Teufel, 2003). According to Schein (1999a), corporate culture exists at three levels, namely:

- **Artifacts**: The visible and measurable day-to-day behavior in the organization.
- **Espoused Values**: The written documents, such a vision or policy statements, that espouse the organization's *formal* values.
- **Shared Tacit Assumptions**: The underlying beliefs and values of the employees. These are the true drivers of employee behavior and were formed as the result of joint learning experiences based on successful past behavior.

To ensure the successful protection of information assets, a formalized approach towards establishing and maintaining a corporate sub-culture of information security needs to be taken. Since the aim of such a process would be to change employee behavior, it would be sensible to "borrow" the necessary methodologies from the behavioral sciences. Corporate culture, and approaches towards changing such a culture, have been studied in depth in the management sciences. This paper will

”borrow” a transformative change management process for the management of a corporate culture change process, from these sciences. For more detail on the process used, refer to Schein (1999a, 1999b); Woodall (1996).

Due to the interdependence between the two dimensions of the ”human factor” in information security, it is also important to keep in mind that, in the case of an information security sub-culture, the above three levels of a corporate culture will all be underpinned by a requirement for adequate information security knowledge. Thus, an employee who has the desired attitude, but, lacks the necessary knowledge, won't be able to behave securely. Conversely, an employee who has the requisite knowledge, but lacks the desired attitude, might still behave in an insecure manner. It is therefor necessary to address both employee knowledge, and employee behavior, in order to successfully deal with the ”human factor” in information security. According to Eloff and Von Solms (2000) the successful management of IT-resources in any modern organization presupposes the following of a holistic approach towards information security. This need for an holistic approach also holds true for dealing with the ”human factor” in information security. It would therefor make sense to combine the various methodologies and processes used for both employee education, and for the establishment of an information security sub-culture, into a single holistic framework. Such a framework should use educational principles that directly contribute towards the establishment of an information security sub-culture, and that will also produce a high level of user awareness and behavioral discipline. The rest of this paper combines previously proposed principles and methodologies into such an holistic framework.

2 AN HOLISTIC FRAMEWORK

This section will attempt to present a single holistic framework for the introduction of both an organizational information security sub-culture, and an information security education program. In order to facilitate understanding, the teaching of correct password usage and the related fostering of a ”secure password culture” will be used as a continuous example throughout the remainder of this paper. This example should not be viewed as a *complete* solution, since it is intended only to clarify and illustrate the relevant steps. As with most other information security processes, the introduction of a corporate sub-culture of information security has to start with top-management.

2.1 Top Management Commitment

Firstly, top management will have to show its commitment to information security and to the ”new” desired culture. This is done, firstly, by developing visionary statements and/or slogans (Sadri & Lees, 2001). This could be part of the corporate vision statement or an awareness campaign. Top management also has to visibly support the desired culture through its own behavior (Wallace, Hunt, & Richards, 1999), and through a commitment in terms of rewards for desirable behavior and punishment for undesirable behavior (Alpander & Lee, 1995). Rewarding desirable behavior and punishing undesirable behavior are both vital factors in shaping employee compliance in information security (Gonzalez & Sawicka, 2002). Once management has committed to the new culture, the *vision* for this information security culture has to be followed up by a corporate information security policy. This policy will form part of the organization's *espoused values*. The policy, in turn, is followed up by various sub-policies, each dealing with specific aspects of the desired culture.

Gaining complete top management commitment for the culture change process will thus be the first component to the integrated framework.

2.2 Define Problem in Business Context

According to Schein (1999a, pp. 86-87), culture change should always be done in a specific business context. Without such a context, culture change has no meaning. In terms of information security this would mean that each specific security need should be addressed individually in order to ensure that

both the dimensions to the human factor are dealt with. Defining the problem in a specific business context would consist of three steps. For each individual business problem:

2.2.1 Assess the Current State

The first step in defining the needed culture change is the assessment of the current state. This should be done at multiple levels. Firstly the current **espoused values**, or policy items and related business procedures, should be assessed. Secondly the current **artifacts** need to be assessed. In other words, measurements should be gathered to determine how well the current espoused values are implemented. Thirdly, the underlying **shared tacit assumptions** need to be assessed. This layer of underlying beliefs and values will generally be the most difficult to quantify. Several techniques, such as interviews and surveys, might contribute towards such an assessment (Martins & Eloff, 2002; Schein, 1999a, pp. 59-87). Lastly, in addition to the cultural layers, it is vital to assess the current underlying information security related **knowledge** of the employees. Several tools could be used to assess current knowledge levels, for example; questionnaires, online tests or interviews. In terms of password usage, it is thus, as an example, necessary to answer the following questions:

1. **Espoused Values**: What current policies and/or procedures exist regarding the authentication of employees?
2. **Artifacts**: How often do employees change their passwords? Do employees share their passwords with others?
3. **Shared Tacit Assumptions**: How serious are employees about keeping their passwords confidential?
4. **Knowledge**: Do all employees know *how* to change their passwords?

Once the current state has been assessed, the ideal future state should be defined in terms of the specific business process.

2.2.2 Define the Ideal State

The ideal future state for the specific business process should also be defined in terms of all three layers of the corporate culture, as well as the required employee knowledge. Such a definition should be specific and in terms of measurable outcomes. Without a clear definition of the behavioral changes that are ultimately needed, it is not possible to test the relevance of culture to the change process (Schein, 1999a, p. 134). For the password example, this definition could include:

- **Espoused Values**: One of the information security policy statements would be: *"All users of information must be authenticated before being allowed to use information resources"*. This policy item, in turn, should be supported by a set of procedures dealing with the specific operational control. Thus, for password usage, one such procedure could be:
  - All users must use passwords that is at least eight characters long and include at least two non-alphabetic characters
- **Artifacts**: In terms of the measurable artifacts clear metrics, supporting the relevant espoused values, need to be defined. For password usage an example would be:
  - Administrative log-files should show that all passwords are changed at least once every two weeks.
- **Shared Tacit Assumptions**: Defining the desired underlying beliefs and values for an ideal future state will require a lot of insight into exactly what beliefs are needed. Basically this

phase of a culture change process should answer the question: ”If you are to solve the business problem or achieve the ideals that are not being met, **what** are the **new ways of thinking** and working that will get you there?” (Schein, 1999a, p. 133). For the password example this could include:

  - Every user must place as much value on the confidentiality of his/her user account's password, as he/she places on his/her personal bank account's pin-number.

- **Knowledge**: The knowledge required by individual employees should be clearly defined. This could be done in terms of the specific outcomes for the related employee education program. For the password example a specific outcomes could be:

  - The learner should be able to demonstrate that he/she is able to successfully change his/her own password

Once the *ideal* future state has been defined in terms of both the corporate information security subculture, and the required employee knowledge, the gap between the current state and the desired state needs to be analyzed for the specific business problem being addressed.

2.2.3 Determine the Steps Needed

The steps needed to get from the current state to the desired future state need to be clearly defined. In some cases it might be necessary to go through several intermediate ”states” to eventually attain the desired *ideal* state. Culture is extremely stable and any attempt to change it will thus have to start with a disconfirmation process (Schein, 1999b; Woodall, 1996). Employees will have to realize that the current way of doing things is no longer good enough. Without such an *unfreezing* of current values, employees will resist the change. Human systems tend toward trying to maintain a stable equilibrium. If change is to occur, this equilibrium must be upset by some new force. The recognition and management of these ”change forces” creates the motivation for humans to change (Schein, 1999a, p. 117). The steps needed to get from the current state to the future state should thus cover all the psychodynamic steps of such a transformative change process (Woodall, 1996; Schein, 1999b, 1999a, pp. 116-139), as well as the required, formal, educational programs to impart the needed information security knowledge to employees. For the password example these steps could include:

- **Unfreezing/Disconfirmation**: Regular password audits should be run and disciplinary steps should be taken against employees whose passwords do not conform to the company policies.
- **Learning**: Employees should be taught **what** would constitute a secure password.
- **Internalizing/Refreezing**: The average strength of each department's employees passwords should be included as a key performance indicator for that department's manager..

To a certain extent, a culture change process will always be coercive (Woodall, 1996; Schein, 1999b). Schein (1999b) compares the processes needed for an enforced culture change to ”brainwashing” techniques used in prisoner of war camps. Woodall (1996) argues that such a culture change process can only be considered ethical if there is an equitable balance between the degree of coercion used, and the rewards, and other positive spin-offs, for employees.

The above processes collectively comprise the second major component to the integrated framework this paper is presenting. The second component is thus the defining of the needed culture change in a specific business context. This definition process will repeat for each business process that need to be supported by the new culture. Even though some degree of coercion, and some reward system, will always be needed during a culture change, it is also possible to use education as a source of disconfirmation (Schein, 1999a, pp. 120-121).

2.3 Educate The Employees

According to Schein (1999a, pp. 120-121) employees will often refuse to accept the need for new, responsible behavior patterns until they have been educated to the dangers inherent in environmental events, for example, the dangers inherent in using a weak password. Education is often the only way to convince employees and managers of the need to do things differently (Schein, 1999a, p. 120). For a culture change process it is thus vital to not only teach employees **what** to do, and **how** to do it, but also **why** it should be done. For information security education, outcomes based education (OBE) has been argued to be a suitable methodology (Van Niekerk & Von Solms, 2003, 2004a). An outcomes based curriculum for the password example could be constructed as follows:

2.3.1 Step 1: Defining the outcomes

For the purposes of this example, outcomes will be defined in each of the three critical domains of outcomes, as discussed in (Spady, 1994, pp. 60-61). These outcomes serve as an example only, and should not be considered a comprehensive list.

- **Performance:** These are outcomes relating directly to actual performance, for example:
  - The learner should change his/her password at least once every two weeks.
- **Content**: These are outcomes related to understanding of subject matter.
  - The learner should be able to demonstrate that he/she has the necessary skills to change his/her own password.
- **Literacy**: These are basic literacy skills needed to understand the content level outcomes.
  - The learner should understand what a password is, and what role a password plays in authentication schemes.

Since education could play an important role in the process of disconfirmation, needed for a culture change, care should be taken that the outcomes defined for the educational program address the need for changing. Special care should be taken that all learners understand **why** they should behave in a specific way (Van Niekerk & Von Solms, 2003, 2004a). Once a clear set of outcomes has been defined, the next step in the creation of an OBE program is developing the actual learning opportunities.

2.3.2 Step 2: Develop learning opportunities

The learning opportunities should be developed in line with the basic premises, and principles, of OBE (Van Niekerk & Von Solms, 2003, 2004a), and should also meet the criteria for information security education, as identified in Van Niekerk and Von Solms (2004a). As an example; for password usage, subject matter could be constructed around the following outlines:

- **Classroom training for role-models**: An information security ”role-model” should be identified in each department. These role-models will be sent on a one-day workshop where they will be taught the relative skills to effectively construct and manage secure passwords.
- **A web-based course for end-users**: A web-based course regarding password usage will be created for organizational end-users.
- **A password practice application for end-users**: An application will be developed for employees to test the strength of their own passwords.
- **Secure password usage booklet**: A booklet regarding password usage will be distributed to all staff.

- **Awareness**: A password awareness campaign will be launched.

When creating the above ”courses”, care should be taken that all the previously identified outcomes are addressed. Once a comprehensive set of learning opportunities has been created, a set of assessment criteria for the various outcomes needs to be defined.

2.3.3 Step 3: Assessment and Feedback

For each defined outcome a corresponding assessment standard should be defined. These assessment standards are necessary in order to provide feedback to the learners. The importance of feedback in both OBE and information security education has been argued extensively in Van Niekerk and Von Solms (2003, 2004a). Without assessment and feedback, learning cannot take place. The feedback system must emphasize **applied** learning in **relevant**, life-role contexts. In the case of the password example, this would mean that assessment criteria would have to be defined for all outcomes across each of the three critical domains in which outcomes have been defined. For example:

- **Performance**: A password strength metric will be calculated and stored every time an employee changes his/her password.
- **Content**: The learner should be able to demonstrate that he/she has the necessary skills to change his/her own password.
- **Literacy**: The learner should be able to score 80% or more on a basic computer literacy test.

For the purposes of testing **knowledge**, assessment of the content level outcomes is the most important. However, in a culture change process the performance level outcomes will play a much larger role, since the metrics of these outcomes will also measure the cultural artifacts. Once the required assessments criteria have been defined, the final part of creating an outcomes based educational program is to ensure all the necessary components for the effective administration of such a program are in place.

2.3.4 Administration

The educational process in general can be viewed as a system of teaching and learning activities that are tied together via various feedback loops. It also includes other functions such as assessment, admission, quality assurance, direction and support (Tait, 1997). All of these components can, and should, play a role in the creation of an effective Information Security education program. The education of employees forms the third major component in the framework this paper is presenting. Once employees have been educated, the next step in a culture change process, would be to define ”cultural metrics” to measure the actual culture change.

2.4 Define Culture Change Metrics

Metrics play a vital role in both information security (Von Solms, 2000), and in any culture change process (Schein, 1999b). Without accurate measurements it is very difficult to know the current status of the culture, or to quantify the desired status of the culture. It is vital to remember that shared tacit assumptions are formed as the result of continuously **successful** past behavior (Schein, 1999a, p. 19). In the case of information security, it will be very difficult for employees to know that their new behavior patterns are successful, because successful information security is mostly tacit, and difficult to quantify. It is therefor vital to implement security metrics and to use these metrics to continuously provide feedback to employees. The **performance** level outcomes in an OBE program, can be translated directly to the relevant cultural artifacts the organization desires. The assessment metrics for these outcomes can thus be used as the cultural metrics. The definition of culture change metrics, comprises the fourth component of the framework this paper is presenting. These metrics should be used to provide continuous feedback to both the employees, and management.

2.5 Feedback, Rewards and Punishments

Feedback plays a vital role in a culture change process. The visionary statements, provided by top-management, *must* be **positively reinforced** through management behavior. Even though middle managers do not initialize the cultural change, ultimately it is their actions that produce the desired change (Brubakk & Wilkinson, 1996). Middle management behavior is vital in a culture change process, since middle management will be the ones providing feedback to the employees. If the behavior of a *learner* fits the expectations of important others, i.e. managers and colleagues, in the learner's work and social environment, that behavior will become a stable part of the person, and eventually of the group (Schein, 1999a, p. 129). By providing the "correct" feedback, management is ultimately responsible for the internalization of the new values by employees.

Feedback provided by management can take many forms. On the one hand, employees can be rewarded/punished based on performance level metrics defined for the culture change process. Secondly, feedback relating to actual security incidents taking place need to be given to both employees and management. According to Gonzalez and Sawicka (2002), risk **perception** is vital for human compliance in information security. Employees *must* perceive the risk, through their own, or reported, experiences, if they are expected to comply with secure practices (Gonzalez & Sawicka, 2002).

Lastly, it should be remembered that employees could be coerced into behaving in a specific way, **but** such a behavior change will be superficial and unstable (Schein, 1999a, p. 115). A reward system based on "impartial" metrics, in combination with a degree of coercion is likely to be more successful. In terms of password usage, the following system of feedback, rewards and penalties could, for example, be implemented:

- A personal page on the organization's information security portal, which allows each employee to view his/her personal password metrics.
- A departmental summary page on the organization's information security portal, accessible by the department's manager andhis/her superiors.
- An organizational summary page on the organization's information security portal. This page could be used by the person, or team, responsible for the culture change to manage overall progress.
- A summary of recent security incidents in the organization, as well as explanations of possible consequences had any of these attacks succeeded.

It should be remembered that a change in beliefs and values results from joint learning processes based on *successful* behavior. Feedback, rewards, and penalties, are the mechanisms management should use to ensure that employees understand *what* behavior would be considered successful. The system of feedback, reward, and punishment mechanisms, comprises the fifth component of the framework this paper is presenting. Without sufficient feedback, it will be very difficult for employees to learn new behavior patterns. If unwanted behavior patterns persist, even though management is actively trying to discourage them, it might be necessary to review the desired changes.

2.6 Review and Refinement

A basic principle of organizational change is the fact that governing variables might sometimes need to be adjusted (Van Niekerk & Von Solms, 2004b). Sometimes the changes required from employees are not feasible in practice, or employees might disagree with a policy and thus disregard the policy (Schlienger & Teufel, 2003). In a case where employees refuse to cooperate, due to a fundamental disagreement with the espoused values, management can either try to "bribe", or coerce, employees to comply through rewards, or punishments, **or** management can **negotiate** a more acceptable policy.

In other words, instead of using rewards or punishments to change the shared tacit assumptions, the culture could be ”strengthened” by bringing the espoused values more in line with existing shared tacit assumptions. According to Woodall (1996), equitable involvement of employees in a culture change process is the only way such a process could be considered ethical. The process of constantly reviewing and refining the culture change process comprises the sixth, and final, component of the framework presented in this paper.

3 FRAMEWORK OVERVIEW

In the previous section an integrated, holistic framework was presented for the fostering of an organizational sub-culture of information security. This framework ”borrows” elements from several fields of study in the behavioral sciences, including; outcomes based education, organizational learning theory, and transformative change management. Figure 1 presents a graphical exposition of this framework. The following is a brief overview of this framework:

1. Attain top management commitment.
2. For each business problem, define the culture change in the context of the specific business problem. This step consist of the following sub-steps:
   (a) Assess the current state of the culture in terms of the specific business problem.
   (b) Define the *ideal* future state of the culture in terms of the specific business problem.
   (c) Analyze the gap between the current state and the desired future state and determine the *steps* needed to get *from* the current state *to* the ideal future state.
3. Educate the employees. For this step in the culture change process outcomes based education should be used. An outcomes based program will consist of the following cycle of steps that should be supported by a sound administrative process:
   (a) Define the desired outcomes.
   (b) Define assessment metrics for each outcome.
   (c) Create learning experiences that will enable learners to attain the desired outcomes.
   (d) Expose the learners to the learning experiences. (Educate)
   (e) Provide feedback to learners based on the defined assessment metrics.
   (f) Constantly review the learning experiences, and where necessary revise them.
4. Define culture change metrics. These could be based on the performance level metrics defined for the educational component.
5. Provide feedback to the employees. This feedback should be *backed* by both rewards and punishments, where necessary. Ideally, most feedback should come from middle management, since ultimately it is the consistent actions of middle management that will drive the culture change. The culture change metrics should also feed back into the educational process, which should be a continuous process that reinforces the *new way* of doing things. These metrics should also feed into a review process.
6. Review and refine the culture change process. Where needed, re-examine the governing variables (espoused values), in order to strengthen the culture and assist with the internalization of the new culture.

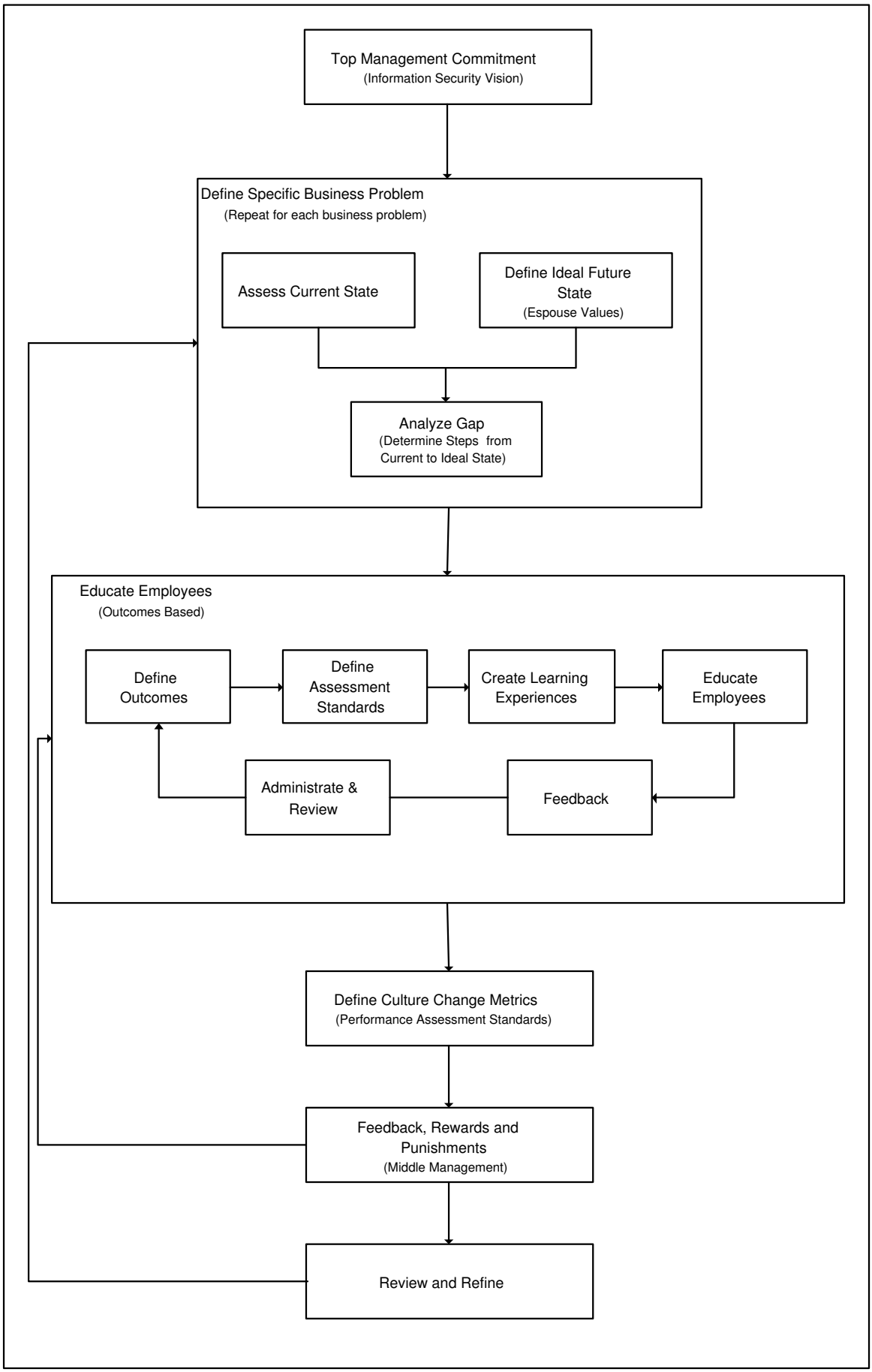

Figure 1: An Outcomes Based Framework for Culture Change

4 CONCLUSION

This paper introduced an holistic framework for the introduction of a corporate sub-culture of information security. The framework combines elements from outcomes based education, organizational learning, and corporate culture, in order to address the two dimensions to the human factor in information security in a holistic fashion. The purpose of the presented framework is to demonstrate how the two dimensions to the human factor in information security, namely knowledge and attitude, *could* be addressed holistically.

Information security depends on both human knowledge, **and** human cooperation. A lack of knowledge can generally be addressed through education, whilst a lack of cooperation can be addressed through the fostering of an organizational sub-culture of information security in the organization. However, if employees have adequate knowledge, but lack the required attitude they will not necessarily behave securely. Conversely, employees who have the correct attitude, but do not have the necessary knowledge, will not be *able* to behave securely. This co-dependency between knowledge and attitude would mean that neither of these factors should be addressed in isolation. The framework presented in this paper incorporates the educational components needed to impart information security knowledge to the employees, into the general culture change process, as presented in (Schein, 1999a). Outcomes based education was used as an educational methodology, since this methodology was shown to be very well suited to information security education (Van Niekerk & Von Solms, 2003, 2004a). Furthermore, the assessment metrics which should be defined for performance level outcomes in outcomes based courses, were incorporated into the culture change process as metrics that could be used to gauge the effects of the change process.

5 REFERENCES

Alpander, G. G., & Lee, C. R. (1995). Culture, strategy and teamwork: The keys to organizational change. *Journal of Management Development, 14*(8), 4–18.

Brubakk, B., & Wilkinson, A. (1996). Agents of change? Bank branch managers and the management of corporate culture change. *International Journal of Service Industry Management*, *7*(2), 21–43.

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.

Gonzalez, J. J., & Sawicka, A. (2002). A framework for Human Factors in Information Security. *Presented at the 2002 WSEAS International Conference on Information Security, Rio de Janeiro, 2002.*

ISO/IEC 17799: Code of Practice for Information Security Management. (2000).

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. (2004).

Martins, A., & Eloff, J. (2002). Assessing information security culture. *Information Security South Africa (ISSA), Johannesburg, South Africa, 2002*.

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

NIST 800-16: Information Technology Security Training Requirements: A Role- and Performance-Based Model. NIST Special Publication 800-16, National Institute of Standards and Technology. (1998).

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

Sadri, G., & Lees, B. (2001). Developing corporate culture as a competitive advantage. *Journal of Management Development*, *20*(10), 853–859.

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

Schein, E. H. (1999b). Empowerment, coercive persuasion and organizational learning: do they connect? *The Learning Organization*, *6*(4), 163–172.

Schlienger, T., & Teufel, S. (2003). Information security culture - from analysis to change. *Proceedings of the 3rd Annual Information Security South Africa Conference, Information Security South Africa (ISSA), Johannesburg, South Africa, 2003*, 183–196.

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

Spady, W. G. (1994). *Outcomes-based education: Critical issues and answers*. USA: American Association of School Administrators.

Tait, B. (1997). Object orientation in educational software. *Innovations in Education and Training International*, *34*(3), 167–173.

Thomson, K., & Von Solms, R. (2004). Towards corporate information security obedience. *10th IFIP WG11.1 Annual Working Conference on Information Security Management, World Computer Congress (WCC), Toulouse, France*.

Thomson, M. (1998). *The development of an effective information security awareness program for use in an organization.* Unpublished master's thesis, Port Elizabeth Technikon.

Van Niekerk, J., & Von Solms, R. (2003). Establishing an information security culture in organisations: An outcomes based education approach. *Information Security South Africa (ISSA), Johannesburg, South Africa*.

Van Niekerk, J., & Von Solms, R. (2004a). Corporate information security education: Is outcomes based education the solution? *10th IFIP WG11.1 Annual Working Conference on Information Security Management, World Computer Congress (WCC), Toulouse, France.*

Van Niekerk, J., & Von Solms, R. (2004b). Organizational learning models for information security. *Information Security South Africa (ISSA), Johannesburg, South Africa*.

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

Wallace, J., Hunt, J., & Richards, C. (1999). The relationship between organisational culture, organisational climate and managerial values. *The International Journal of Public Sector Management*, *12*(7), 548–564.

Woodall, J. (1996). Managing culture change: can it ever be ethical? *Personnel Review*, *25*(6), 26–40.

6 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.