MISSTEV: Model for Information Security Shared Tacit Espoused Values

by

Kerry-Lynn Thomson

MISSTEV: Model for Information Security Shared Tacit Espoused Values

by

Kerry-Lynn Thomson

Thesis

submitted in fulfillment of the requirement for the degree

Doctor Technologiae

in

Information Technology

in the

Faculty of Engineering, the Built Environment and Information Technology

of the

Nelson Mandela Metropolitan University

Promoter: **Prof. Rossouw von Solms**
Co-Promoter: **Prof. Lynette Louw**

October 2007

ABSTRACT

One of the most critical assets in most organisations is information. It is often described as the lifeblood of an organisation. For this reason, it is vital that this asset is protected through sound information security practices. However, the incorrect and indifferent behaviour of employees often leads to information assets becoming vulnerable. Incorrect employee behaviour could have an extremely negative impact on the protection of information.

An information security solution should be a fundamental component in most organisations. It is, however, possible for an organisation to have the most comprehensive physical and technical information security controls in place, but the operational controls, and associated employee behaviour, have not received much consideration. Therefore, the issue of employee behaviour must be addressed in an organisation to assist in ensuring the protection of information assets.

The corporate culture of an organisation is largely responsible for the actions and behaviour of employees. Therefore, to address operational information security controls, the corporate culture of an organisation should be considered. To ensure the integration of information security into the corporate culture of an organisation, the protection of information should become part of the way the employees conduct their everyday tasks – from senior management, right throughout the entire organisation. Therefore, information security should become an integral component of the corporate culture of the organisation.

To address the integration of information security into the corporate culture of an organisation, a model was developed which depicted the learning stages and modes of knowledge creation necessary to transform the corporate culture into one that is information security aware.

DECLARATION

I _____ , hereby declare that:

- The work in this thesis is my own work.
- All sources used or referred to have been documented and recognised.
- This thesis has not previously been submitted in full or partial fulfillment of the requirements for an equivalent or higher qualification at any other recognised educational institution.

_____

My sincerest gratitude to the following people:

My promoter, Professor Rossouw von Solms,
and my co-promoter, Professor Lynette Louw,
for their support, patience and guidance.

My family
for their encouragement and belief in me.

And above all,
to my Creator who made it possible.

TABLE OF CONTENTS

LIST OF FIGURES AND TABLES

Figures

Tables

CHAPTER 1

INTRODUCTION

1.1 Prologue

Information is a particularly significant asset to most organisations. It is often described as the core of the emerging electronic economy and is vital for the successful operation of most organisations (Gordon, 2002, online). It is, however, difficult to measure the exact value of the information that an organisation possesses. Nonetheless, it is apparent that any breach in the confidentiality, integrity or availability of information could result in harmful consequences for an organisation (Gordon & Glickson LLC, 2001, online).

Therefore, information security controls, which include physical, technical and operational controls, should be implemented and managed in an organisation to ensure that the information is kept secure (Krige, 1999, p 7). However, there are many challenges facing the implementation of information security practices in to organisations. One of the greatest challenges hindering successful information security practices in an organisation is the human element and the associated operational controls. Employees' behaviour and actions often represent the weakest link in the information security process. Although an organisation may have the best physical and technical controls, employees may, maliciously or unintentionally, circumvent these controls and compromise information assets (Martins & Eloff, 2002, p 203). Therefore, the issue that should be addressed to assist in the successful implementation of information security practices in to an organisation is that of employee behaviour and actions.

A decisive influence on the behaviour and actions of employees in an organisation is the corporate culture. Corporate culture is the outcome of all the collective, taken-for-granted assumptions that a group has learned throughout an organisation's history. Corporate culture is generally defined as values that are shared by everyone in an

organisation, including fundamental beliefs, principles and practices. These collective assumptions and beliefs will influence and determine the actions of employees (Schein, 1999, pp 15-17, 29). Thus, the corporate culture of an organisation largely influences the behaviour and actions of employees, and, as was detailed previously, it is the incorrect behaviour and actions of employees that often impede information security. Therefore, it follows that the corporate culture of an organisation should ideally be shaped and modified to influence the behaviour of employees appropriately towards the effective protection of information assets.

For the purpose of this thesis, the term 'senior management' will be used to include the Board of Directors, the CEO and directors. This term will be used for all occurrences of management, including corporate culture. It is acknowledged, however, that in terms of corporate culture, even though the term 'senior management' is used, corporate culture can be influenced and shaped by all levels of management in an organisation.

1.2 Identification of the Problem Area

As described in the previous section, the successful protection of information assets, through information security practices, is highly dependent on the behaviour and actions of employees in an organisation. Further, the behaviour and actions of employees are largely influenced by the corporate culture of an organisation.

To be successful, information security should become part of the way the employees conduct their everyday tasks, from senior management, right throughout the entire organisation. Therefore, information security should become an integral part of the corporate culture of the organisation. It is possible for the correct information security actions and practices to be enforced in an organisation through rewards and consequences. However, this is not ideal because, without strict enforcement, employees may stray from the correct information security practices. To be truly effective, the correct information security practices should become second-nature to employees and part of the corporate culture. Further, as information security is very much reliant on the

correct behaviour of users, the corporate culture should contribute towards the fact that the *de facto* behaviour of users is indeed what senior management envisaged as acceptable behaviour in terms of information security (Thomson & von Solms, 2004, pp 19-31).

In many organisations, the information security vision or focus of senior management and that of the employees is immensely disparate, resulting in senior management and employees actually working in 'opposing directions', as indicated in Figure 1.1. The consequence of this is that minimal achievement of organisational goals is evident in an organisation and information security is, therefore, not successfully integrated into the organisational corporate culture.

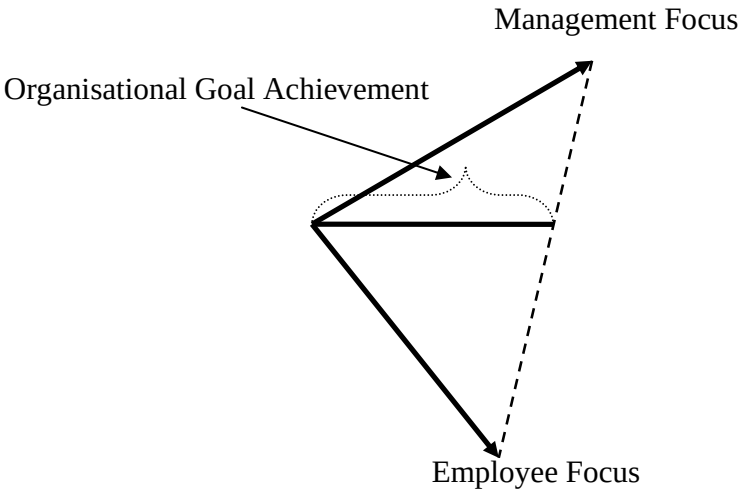

Figure 1.1: Minimal organisational goal achievement
Source: Accel-Team, 2000, online

Employees' lack of understanding and support for the vision of senior management is most often demonstrated in erroneous behaviour and a small degree of goal congruence is evident in many of the information security implementations of organisations. Even though the corporate culture influences the behaviour of employees, it is estimated that only five per cent of organisations have a definable culture, where senior management takes an active role in the shaping of the culture (Atkinson, 1997, p 17). Therefore, only

in a minority of organisations is senior management aware and active in positively influencing the behaviour of employees.

The challenge in most organisations is to ensure that the information security vision or focus of senior management is essentially supported by the employees, primarily through their behaviour. This should result in senior management and employees having the same focus and working towards the same organisational goals. The closer the focus of senior management and employees are aligned, the greater the chance of the achievement of the organisational goals, as indicated in Figure 1.2.

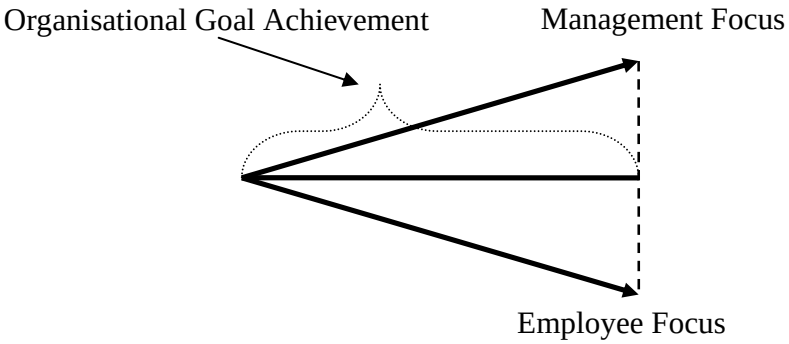

Figure 1.2: Increased organisational goal achievement
Source: Accel-Team, 2000, online

In order to begin the alignment of the focus of management and employees, senior management should ensure that its vision is outlined and communicated to employees. Senior management should preferably detail its information security vision in the Corporate Information Security Policy. The main aim of any policy, including the Corporate Information Security Policy, is to influence and determine the decisions and actions of employees by specifying what behaviour is acceptable and what behaviour is unacceptable within the context of corporate culture (Whitman & Mattord, 2003, p 194). By developing a Corporate Information Security Policy, senior management is exhibiting its vision and commitment to the protection of information assets and detailing what should be expected from employees.

Equally as important as the development of the Corporate Information Security Policy is the communication of that policy to employees. Further, if it is communicated in the correct manner, the Corporate Information Security Policy should play a vital role in changing the corporate culture. Employees should be made aware of the role they ought to be playing in the protection of information assets. Further to this, employees must be trained in information security practices and educated to gain a deeper understanding of the importance of information assets.

However, senior management is frequently unsuccessful in the communication of the information security vision to its employees and ineffective in aligning management and employee information security goals. Employees are, therefore, often apathetic and nonchalant towards the information security goals of senior management. Only once management and employee goals are aligned and, consequently, everyone in the organisation is working towards the same vision, will an information security conscious corporate culture begin to emerge.

1.3 Problem Statement

Effective information security calls for extensive human interaction which involves all employees in the organisation. As part of its corporate governance duties, it is vital for senior management to provide guidance and direction towards the protection of information assets. However, the necessary leadership from senior management, in most cases, is lacking and the goals and direction of senior management is not communicated properly to employees. Employees, therefore, often do not have an accurate understanding of their role in information security. The fundamental beliefs and values of employees regarding information security, shaped by the corporate culture of the organisation, are not necessarily aligned with the wishes and information security vision of senior management.

Employees fail to get the necessary guidance from senior management to integrate information security procedures and practices into the corporate culture of their

organisation. As a result, one of the principal problems facing the successful implementation of information security practices in to organisations is the apathy and incorrect actions and behaviour of employees exacerbated by the lack of leadership from senior management.

Employees often do not understand the importance of, and the role they should play in, the protection of information assets in an organisation. This is as a result of the fact that the goals of employees in an organisation are often not aligned with the goals of management. As a result, employees' behaviour and actions with regard to information assets frequently reflects the apathy they feel and results in inadequate information security practices in an organisation.

1.4 Objectives

The primary objective of this research study is to develop a model that will assist in the integration of information security practices into an organisation. To achieve this primary objective, a number of secondary objectives are defined.

These secondary objectives include:

- an investigation into the role that management should play in the integration of information security into an organisation
- an examination of the impact that employee behaviour could have on the successful implementation of information security practices in to an organisation
- a study of the theories and concepts underlying corporate culture and determining how corporate culture could influence the employees in an organisation
- an investigation into management's role in corporate culture and the influence of management policies in shaping the corporate culture
- determining the role of the Corporate Information Security Policy in aligning management's information security vision with the behaviour of employees
- a study of the knowledge creation process in an organisation and the learning process of employees

- ❖ an investigation into the relationship that should exist between information security, corporate culture and corporate governance

The integration of the aspects addressed in the secondary objectives should contribute towards the successful development and motivation of the eventual model.

1.5 Research Paradigms and Methodology

Paradigms are generally defined as "universally recognised scientific achievements that for a time provide model problems and solutions to a community of practitioners". They offer a structure of accepted sets of theories, methods and ways of defining data (Collis & Hussey, 2003, pp 46-47).

There are two main research paradigms or philosophies, which are classified as *phenomenological* and *positivist*. The *phenomenological* and *positivistic* paradigms are on either ends of the gamut and very little research is conducted within their pure forms (Collis & Hussey, 2003, pp 47, 51). Therefore, most research cannot be termed entirely *phenomenological* or *positivistic,* but some combination of the two. So, too, does this thesis utilise aspects of both the *phenomenological* and *positivist* paradigms, as will be detailed later in this section.

The *phenomenological* paradigm is concerned with the comprehension of human behaviour from an individual's own frame of reference. This approach stresses the subjective aspects of human behaviour by focusing on the meaning and implication, rather than the measurement, of social phenomena. The *phenomenological* paradigm is, therefore, often referred to as *qualitative* (Collis & Hussey, 2003, pp 47, 53).

The *positivistic* paradigm seeks the causes of social phenomena, with little regard to the subjective state of the individual. Thus, logical reasoning is applied to the research so that precision and objectivity replace hunches and intuition as the means of exploring research problems. *Positivism* is based on the belief that the study of human behaviour

should be conducted in the same way as studies conducted in the natural sciences. The *positivist* paradigm is, therefore, often referred to as *quantitative* (Collis & Hussey, 2003, pp 47, 52).

There are various assumptions within the two main research paradigms. The assumptions pertinent to this research are ontological, epistemological, and methodological (Collis & Hussey, 2003, pp 48-50). The following paragraphs will detail these assumptions in terms of the *qualitative* and *quantitative* approaches, and how they relate to this thesis.

The ontological assumption is concerned with the nature of reality. In terms of the *qualitative* paradigm, reality is socially constructed and can only be understood by examining the acuity of the human actors. In terms of the *quantitative* paradigm, reality is objective and external to the researcher. In the context of this research, from an ontological perspective, reality is seen as a pattern of symbolic relationships sustained through a process of human action and interaction. Further, reality is believed to be created by individuals through actions and routines. These assumptions place the greater part of this research resolutely on the *phenomenological*, or *qualitative*, side. However, in the milieu of this research, reality could also be seen as derived from the communication of information which leads to constantly shifting forms and behaviours. This assumption leans more toward the *positivistic* paradigm.

The epistemological assumption is concerned with the study of knowledge and what is accepted as legitimate knowledge. In terms of the *qualitative* paradigm, the researcher interacts with that being researched to attempt to minimise the distance between the researcher and what is being researched. In terms of the *quantitative* paradigm, researchers believe that only phenomena which are observable and measurable can be validly regarded as knowledge, and the researcher is independent from that being researched. In this thesis, the researcher will be independent and not directly involved with that which is being researched. However, the research data itself will be *qualitative* and not *quantitative*.

The methodological assumption is concerned with the process of research. In terms of the *qualitative* paradigm, a number of different research methods will be used to obtain different perceptions of the phenomena to attempt to understand what is happening in a situation and looking for patterns which may be repeated in similar situations. In terms of the *quantitative* paradigm, concepts should be described in such a way that they can be measured. Large samples should be used and the phenomena will be reduced to their simplest parts.

Therefore, as can be seen from these assumptions, and as stated previously in this section regarding most research, this research study can not be compartmentalized into purely *phenomenological* or *positivistic*. Rather, this research draws on certain aspects from both paradigms and involves theory building and critical thinking through an inductive process to build knowledge.

In terms of the research methodology, an extensive literature study was conducted where every endeavor was made to ensure the content is as current as possible and the literature was selected from respected authorities in the relevant fields. This research study utilises an inductive process and uses solid arguments and theory building to argue towards the Model for Information Security Shared Tacit Espoused Values or MISSTEV. The various components of information security, corporate culture and organisational learning, uncovered through the literature study, will be integrated into MISSTEV using modeling techniques to assist in its presentation. MISSTEV will illustrate the learning process of employees from the time they are made aware of their information security responsibilities until information security becomes part of the corporate culture.

Additionally there were five papers written where the research components and results of this study were documented through publications. Three of these papers were published in accredited journals and two presented at subject specific conferences and published in the conference proceedings (see appendices A-E).

1.6 Chapter Road Map

This thesis consists of nine chapters, with Chapters 2, 3 and 4 mainly conducting a literature study. From Chapter 5 onwards preliminary solution components from MISSTEV will be argued.

The first chapter is an introduction, which includes identification of the problem area, outlining the research objectives and research methodology. Chapter 2 explores the discipline of corporate culture. The definition of corporate culture will be discussed and the Three Levels of Culture, as defined by Schein, will be detailed. The various classifications of culture and forms of power in an organisation will be discussed, as well as how to maintain the corporate culture. The third chapter expands on a few of the concepts from Chapter 2 by exploring senior management's role in corporate culture. The symptoms of a corporate culture that could be detrimental to an organisation, where senior management is not taking an active role in shaping the culture, will be detailed, together with the types of organisational environments that could exist in an organisation based on the style of management. The vital role that policies play in shaping the culture and the factors that would influence a culture change will be examined.

The fourth chapter will detail both the management and human dimensions of information security. The aim of information security in an organisation will be examined, as well as the impact that the human element has on the success of information security in an organisation. The integration of information security in the corporate culture of an organisation and the role that senior management should play in shaping that culture will be detailed.

The first of the components forming part of the solution will be discussed in Chapter 5 as it will tie together the discussions from the previous chapters into the relationship that should exist between information security, corporate culture and corporate governance. The Three Levels of Corporate Culture and the organisational environments, discussed in previous chapters, and the links that exist between them will also be evaluated.

The knowledge creation processes within an organisation, for both tacit and explicit knowledge, will be studied in Chapter 6. This chapter will also include a study of the organisational learning process where single- and double-loop learning will be detailed.

A further solution component that will be relevant in the construction of MISSTEV will be investigated in the seventh chapter. The importance of awareness, training and education in terms of information security will be detailed and the learning process of employees will be examined.

The penultimate chapter, Chapter 8, is a solution chapter and will discuss the proposed Model for Information Security Shared Tacit Espoused Values or MISSTEV. The solution components from previous chapters will be integrated and merged to form MISSTEV. The final chapter provides a cumulative conclusion and will evaluate the research to determine whether the research objectives have been met. This chapter will also include a discussion for further research. The chapter road map, as seen in Figure 1.3, illustrates the logical order of the research of this thesis.

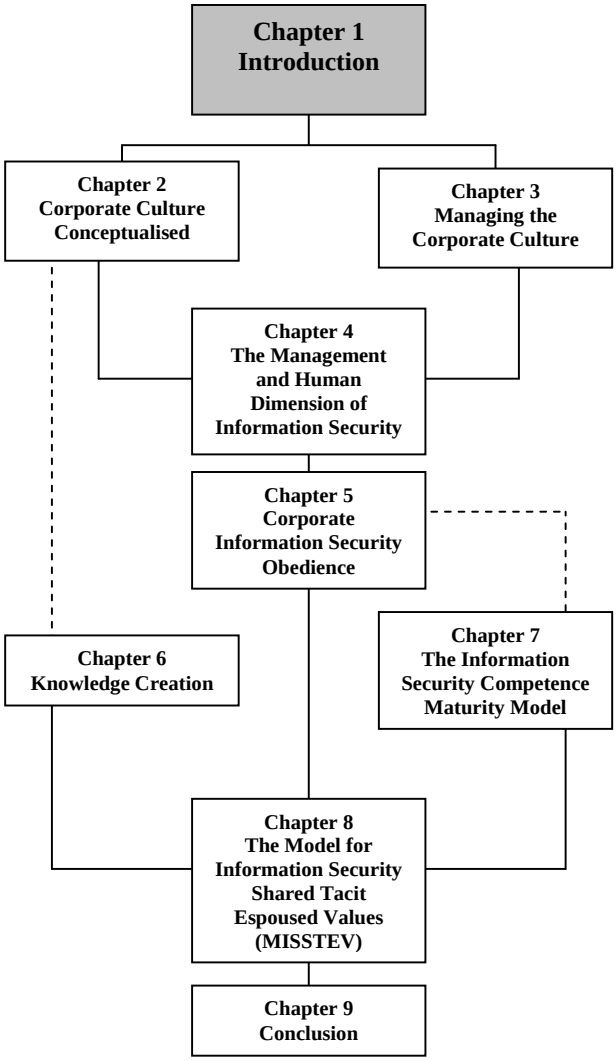

Figure 1.3: Chapter road map

CHAPTER 2

CORPORATE CULTURE CONCEPTUALISED

2.1 Introduction

Corporate culture is a particularly intricate aspect of any organisation. Culture exists in an organisation whether management and employees are aware of it or not. In many cases, however, a corporate culture simply exists and does nothing to positively influence the organisation. The influence of corporate culture on the actions and behaviour of employees, and the various features and characteristics of corporate culture, if understood and utilized properly, could possibly enhance the operations of an organisation.

The objective of this chapter is to explore different facets of corporate culture in order to gain a deeper understanding of this complex concept. Various definitions of culture, the three levels of culture and the types of power that influence these levels will be explored. The four classifications of corporate culture that could be found in organisations, and the relationship between dominant cultures, sub-cultures and counter-cultures will also be examined. The chapter will conclude with a synopsis of how a corporate culture can be maintained.

2.2 Conceptualising Corporate Culture

Culture is the sum total of all the shared, taken-for-granted assumptions that a group has learned throughout history, and culture provides people with a common viewpoint that ties them together as a group (Sathe, 1983, pp 6-7; Schein, 1999, pp 28-29). It is a powerful, underlying and often unconscious set of forces that determines both individual and group behaviour, thought patterns and values (Schein, 1999, p 14). Culture can be likened to personality. Like personality, culture affects in predictable ways how people

conduct themselves when no one is instructing them on what to do (Hellriegel, Jackson, Slocum, Staude, Amos, Klopper, Louw & Oosthuizen, 2004, p 357). Further, the concept of corporate culture can be a powerful analytical tool in the examination and interpretation of human action within complex organisations (Meek, 1988, p 454).

Corporate culture has a number of important implications in an organisation as it offers an interpretation of an organisation's history that employees can use to interpret how they will be expected to behave in future. In addition, corporate culture can generate commitment to corporate values or management's vision so that employees feel they are working for something they believe in. Another implication is that corporate culture serves as an organisational control mechanism, unofficially encouraging or discouraging certain patterns of behaviour. Corporate culture has the potential to enhance organisational performance and provides a sense of certainty about how problems are to be handled in an organisation (Martin & Siehl, 1983, p 52; Hellriegel et al, 2004, p 368).

Corporate culture provides meaning and direction for an organisation and is often described as the social or cultural energy that moves an organisation into action (Kilmann, Saxton, Serpa and Associates, 1985, pp 353-354). Cultural assumptions in organisations develop around how people in the organisation relate to each other. However, this is only a fraction of what culture covers. Corporate culture drives strategy, goals and decision making in organisations (Schein, 1999, pp 14, 28-29).

Every organisation develops a culture, whether it attempts to or not, and this culture operates at both a conscious and subconscious level (Hagberg Consulting Group, 2002, online). It is important to note that no culture is wrong in itself, only inappropriate to its circumstances (Handy, 1978, p 26). Therefore, there is no 'right' or 'wrong' culture – except in relation to what the organisation is trying to achieve, as well as the environment in which it operates (Schein, 1999, p 21). In many organisations, the 'cultural energy', mentioned earlier, has scarcely been tapped. The energy is not mobilized towards anything, and employees seem apathetic towards their jobs (Kilmann et al, 1985, p 353). In other organisations, the energy is actively flowing, but it is moving employees in the

wrong direction. The resulting behaviour is working against the organisation and is not in line with the wishes of management (Kilmann et al, 1985, p 354).

Therefore, as suggested by Kilmann et al, "to understand the essence or soul of the organisation requires that we travel below the charts, rulebooks, machines, and buildings into the underground world of corporate culture" (1985, p 351). In order to gain a deeper understanding of corporate culture, it is essential to understand the different levels that can be identified as defined by Edgar H. Schein's Three Levels of Corporate Culture.

2.3 Three Levels of Corporate Culture Defined

One of the challenges when trying to understand corporate culture is to oversimplify this complex concept. Stated simply, culture could be seen as "the way things are done around here" – but it is far more than this. Culture should be regarded as something that an organisation 'is', not as something that an organisation 'has'. Culture is an abstraction, and, as a result, it only has use in relation to the interpretation of the observed tangible behaviour (Meek, 1988, p 470). Consequently, a far better way of thinking is to realise that culture exists at several levels. According to Edgar H. Schein, these levels range from the very visible and tangible to the tacit and invisible. Furthermore, it is imperative that these levels are managed and understood (Schein, 1999, p 15). The following sub-sections address the existence of corporate culture at various levels in an organisation.

2.3.1 Level 1: Artifacts

The first and most visible expression of culture observed in an organisation is that of *artifacts* (Hagberg Consulting Group, 2002, online). *Artifacts* can be described as observed concrete behaviour, or what an individual can see, hear and feel as they observe an organisation (Schein, 1999, p 15). These include the architecture and decor, the clothing people wear and organisational practices. Other tangible expressions of culture are found in commonly used language and jargon, logos, brochures,

organisational slogans and narratives. An outsider can often spot these *artifacts* easily upon entering an organisation. For employees, however, these *artifacts* have often become part of their subconscious thinking (Hagberg Consulting Group, 2002, online).

It is not, however, reliable to base the judgment of an organisation's culture on simply observing the *artifacts*. By doing this, all that is known is that the organisation has particular ways of presenting itself and dealing with customers and employees. It is still unclear as to what all these observations mean. In other words, at the level of *artifacts*, the corporate culture is clear and has an immediate emotional impact. The behaviour of individuals is clear, but it still is not clear why the employees of an organisation are behaving in a certain way, and why each organisation is constructed as it is.

The observations of the actions and behaviour of individuals that have been made should be further explored by talking to employees to attempt to gain an understanding of their perceptions about the *artifacts* and culture. The questioning of the employees in this regard leads to the next level of culture – the *espoused values* (Schein, 1999, pp 15-17).

2.3.2 Level 2: Espoused Values

The second level of culture is the *espoused values* of an organisation. 'Espouse' means to adopt or support a cause (Oxford Dictionary of Current English, 1993, p 295). Therefore, the *espoused values* of an organisation should be those that the organisation is supporting. This level of culture requires questions to be asked about the organisation's *artifacts*, especially those *artifacts* that seem somehow inconsistent with what would be expected. For this purpose, employees who can explain the organisation need to be found. Anthropologists refer to these employees as 'informants' and depend heavily on such conversations to understand

what is going on in an organisation. Examples of *espoused values* are teamwork and good communication.

In many cases, organisations that advocate the same values can have very different physical layouts, working styles and *artifacts*. By only examining *espoused values*, organisations cannot be categorised into a specific 'typology' as these organisations are still not understood at the deeper cultural level.

There could be obvious inconsistencies between some of the *espoused values* and the visible behaviour of the employees of an organisation. Organisations may espouse teamwork, yet seem to reward and promote initiatives that are highly competitive and individualistic. An organisation may also espouse customer orientation, for example, and yet does not employ people who seem very polite or service-oriented.

What these inconsistencies indicate is that a deeper level of thought and perception is driving the obvious behaviour. What an organisation strives to do, and the values it hopes to endorse, may be different from the values, beliefs, and norms expressed in the actual practices and behaviour of the organisation (Hagberg Consulting Group, 2002, online). The deeper level of culture may or may not be consistent with the values and principles that are espoused by the organisation. Therefore, to truly understand the culture of an organisation, one must understand what is happening at the deeper level of *shared tacit assumptions* (Schein, 1999, pp 17-19).

2.3.3 Level 3: Shared Tacit Assumptions

'Tacit' means something that is understood or implied without being stated (Oxford Dictionary of Current English, 1993, p 927). *Shared tacit assumptions*, therefore, are unspoken assumptions that are shared by a group of people. *Shared tacit assumptions* are the underlying thoughts

> and feelings that members of a culture take for granted and believe to be true (Hellriegel et al, 2004, p 358). To understand this deepest level of *shared tacit assumptions*, the history of an organisation needs to be examined. What were the values and beliefs of the founders that contributed towards the success of the organisation? Organisations are initiated and managed by individuals or small teams who originally impress their own beliefs, values and assumptions on employees. As the organisation progresses successfully in its life cycle, the established beliefs, values and assumptions of the founder (s) become shared amongst employees and taken for granted. They become tacit assumptions about the nature of the organisation's environment and how to succeed in it. As a result, the established values, beliefs and assumptions guide the observable behaviour of employees in their daily activities.
>
> Corporate culture is, therefore, mutually learned values, beliefs and assumptions that become taken for granted as an organisation continues to grow (Schein, 1999, pp 19-20).

After examining the Three Levels of Corporate Culture, as defined by Edgar Schein, it is evident that it is the learned, *shared tacit assumptions* on which people base their daily behaviour (Schein, 1999, p 24). Several of the most important elements of culture are essentially tacit or invisible (Schein, 1999, p 21). It is essential that the levels of culture are recognised by management to fully appreciate the depth of culture in the organisation.

The 'culture iceberg', represented n Figure 2.1, illustrates that values, beliefs and assumptions form the base of corporate culture, but cannot be observed in an organisation as they are lying 'under the surface'. Corporate culture can be inferred from the more visible and observable elements in an organisation – its practices, language, narratives and slogans, as represented in Figure 2.1 (Hellriegel et al, 2004, p 357).

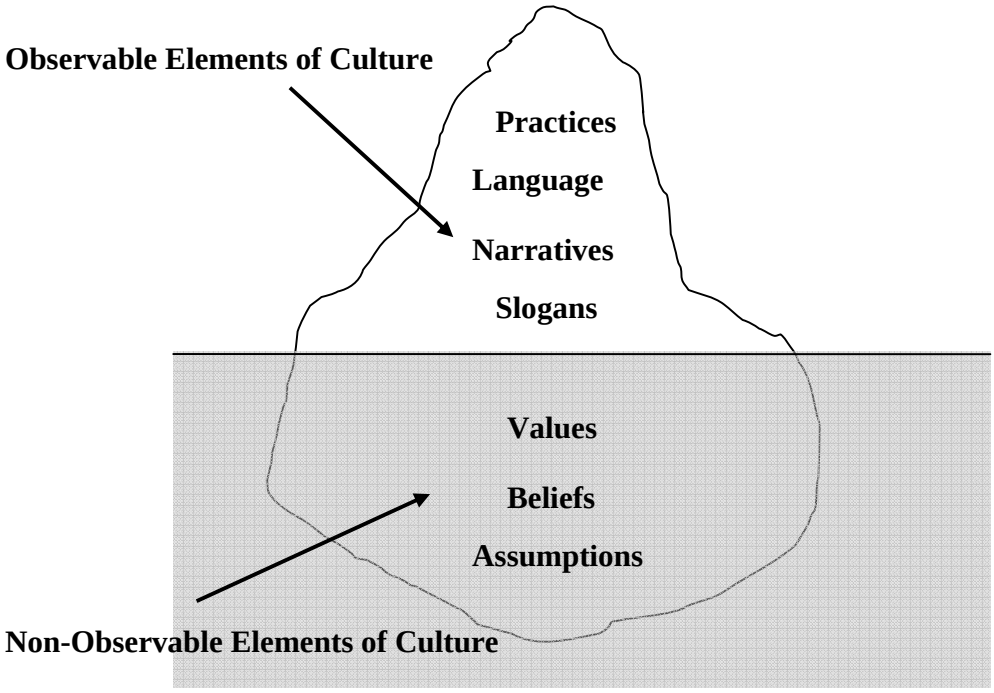

Figure 2.1: The culture iceberg
Source: Adapted from Hellriegel, Jackson and Slocum, 2002, p 487

Figure 2.1 illustrates that many of the more crucial aspects of corporate culture are essentially invisible. The values, beliefs and assumptions of the employees in an organisation form the foundation for corporate culture.

A contributing factor that influences the corporate culture in an organisation, and, consequently, the Three Levels of Corporate Culture, is the distribution of power in an organisation. In most organisations, power is held by senior management and should be used by management to direct employees' behaviour. There are typically three types of power that can exist in organisations. The types of power, namely; condign, compensatory and conditioned power, and the effect they have on an organisation and its employees are discussed in the following section.

2.4 The Influence of Power on the Three Levels of Corporate Culture

Power is often, mistakenly, seen as no more than domination, conflict, violence and hierarchy. However, power is both the ability to make changes and control or guide (Gjerstad, 2005, online). Organisations, for example, exert power in society through their ability to condition their own employees (Galbraith, 1983, p 23). The type of power exercised in an organisation strongly influences the corporate culture, and its three levels discussed in the previous section.

Organisations have access to three primary instruments of power:

i.) Condign power (physical)

ii.) Compensatory power (economic)

iii.) Conditioned power (belief)

Organisations may impose or enforce their will through the use of condign or compensatory power. Condign power (physical) refers to consequences or punishment, whereas compensatory power (economic) wields power by offering rewards. Condign power and compensatory power have one similarity - in both cases obedience is obtained through submission. These two types of power should primarily influence the *artifacts* level, or visible behaviour, of employees. Through condign or compensatory power, it is the overt behaviour of employees that should be manipulated and not their beliefs and values at the *shared tacit assumptions* level.

Of the three types of power, conditioned power (belief) is the most important in society, and an organisation should be the embodiment of conditioned power. It is through persuasion, education and social commitment to what seems natural or right that the organisation causes the individual to submit to the will of others. Power should be exercised through changing the beliefs and values of the obedient person, or, in other words, the *shared tacit assumptions* level of corporate culture.

There is a symmetric relationship between how power is exercised and how it is challenged: condign power could be met with violence, compensatory power, or

economic power could be met with the regulation of the market and conditioned power could be met with contradicting beliefs and ideologies (Galbraith, 1983, p 23).

The way that power is distributed in an organisation will result in different types of corporate culture, depending on the type of power that is exercised. The following section will describe these different corporate culture types, namely; Creative, Quality, Supportive and Productive. It is important to note that, regardless of the type of corporate culture evident in an organisation, each type of culture exists at the Three Levels of Corporate Culture discussed in the previous section.

2.5 Classifications of Corporate Culture

Usually, when an organisation is first started, it can be described as a group of people with a common purpose. There is a unique culture that is necessary for the group to survive and progress. As the group evolves, the original culture that served all of the members in earlier times becomes less practical as the group becomes an organisation (Beach, 1993, p 18). As time progresses, the culture may develop into one of the classifications of corporate culture that have been identified, or a combination thereof.

As can be seen in Table 2.1, there are many classifications of corporate culture, as suggested by various sources. Despite the many classifications that exist, they all share certain commonalities. For this reason, not all the classifications of corporate culture will be discussed in detail. This is because the description of the Creative classification, for example, shares commonalities with the Prospectors, High risk/fast feedback, Achievement and Entrepreneurial classifications. The classifications as suggested by Rowe, Mason, Dickel, Mann and Mockler (1994) will be outlined in depth in Sections 2.5.1 to 2.5.4. The various classifications of corporate culture and how they relate to one another are illustrated in Table 2.1.

Miles & Snow (1978)	Deal & Kennedy (1982)	Harrison (1993)	Rowe et al. (1994)	Hellriegel et al. (2004)
Prospectors: innovative	High risk / fast feedback	Achievement: based on competence	Creative: initiates change	Entrepreneurial: risk-taking, creativity
Analysers: in search of efficiencies	High risk / slow feedback	Role: based on structure	Productive: resists change	Market: competitiveness
Defenders: conservative beliefs	Low risk / fast feedback	Support: based on relationships	Supportive: responds to change	Clan: tradition, loyalty, socialization
Reactors: forced to adjust	Low risk / slow feedback	Power: based on strength	Quality: accepts change	Bureaucratic: hierarchical coordination, rules

Table 2.1 Classifications of corporate culture

The four classifications of corporate cultures, namely; Creative, Productive, Supportive and Quality, as suggested by Rowe et al. (1994), will be discussed in the following sub-sections.

2.5.1 Creative Culture

In the Creative Culture, employees have a high internal motivation, which leads to innovation and entrepreneurialism. In this culture, the inclination is towards risk taking as employees work towards mutually valued goals. The Creative Culture initiates change and promotes rapid learning and adaptation to change. The darker side of an achievement culture is that employees become competitive towards one another and, for many tasks, the end justifies the means. This often encourages employees to operate outside their rules and responsibilities to accomplish the necessary tasks.

2.5.2 Quality Culture

The Quality Culture is based on effective planning and problem solving. Efficient operations are promoted and the time taken to learn a new job is reduced by well-designed structures and systems. Authority and responsibility is clearly defined and reduces the need for individual decision making. In a Quality Culture, change is accepted.

2.5.3 Supportive Culture

The Supportive Culture is based on relationships and has good internal communication and commitment to decisions. High levels of trust exist between individuals and the organisation and this culture is characterized by teamwork, cooperation and reinforcement. A Supportive Culture readily accepts change. A shortcoming of the Supportive Culture is that there is a tendency to put the needs of individuals ahead of the needs of the organisation

2.5.4 Productive Culture

The Productive Culture concentrates on efficiency and consistency. Individual efforts are unified behind the vision of the leaders and management. The Productive Culture tends to employ rigid procedures and rules and, thereby, reduces conflict within an organisation. However, the downside of a Productive Culture is that dynamic change is often stifled and this culture is resistant to change (Rowe, Mason, Dickel, Mann & Mockler, 1994, pp 473-474).

It must be emphasized, once more, that despite the classification of corporate culture evident in an organisation, it exists at the *artifacts, espoused values* and *shared tacit assumptions* levels. As stated previously, there is no correct or incorrect culture, or mix of cultures, in an organisation – there is no generically correct culture (Hagberg Consulting Group, 2002, online). It is rather about ensuring that the most suitable culture for an organisation is guiding the behaviour of employees. Typically, one of the classifications of corporate culture described in this section is the dominant culture in the

organisation. Together with the dominant culture, it is likely that a few sub-cultures could exist in an organisation. In addition, it is always possible that a counter-culture exists that opposes many of the core components of the dominant culture. The relationship between the dominant, sub-cultures and counter-cultures will be explored in the following section.

2.6 Dominant Cultures, Sub-cultures and Counter-cultures

Most organisations have a dominant or central corporate culture that unifies employees. In addition to this, it is possible that sub-cultures can coexist with one dominant culture and counter-cultures. The following section will detail dominant, sub-cultures and counter-cultures.

Through *artifacts*, a dominant corporate culture expresses core values that are shared by a majority of the organisation's members (Martin & Siehl, 1983, p 53). It is pervasive throughout the organisation and indicates a high level of cultural integration (Hagberg Consulting Group, 2002, online). A dominant corporate culture exerts a stabilizing force on an organisation by encouraging cohesion and organisational commitment among employees (Boisnier & Chatman, 2002, online).

Sub-cultures emerge from the dominant corporate culture's values. Some of a sub-culture's values may conflict with the dominant culture's values while others may not. Sub-cultures represent accepted differences that do not upset the commonality of the dominant corporate culture's values. Three types of sub-cultures are *enhancing*, *orthogonal* and *counter-culture* (Boisnier & Chatman, 2002, online).

Employees who are part of *enhancing* sub-cultures adhere to dominant corporate culture values more enthusiastically than other employees in the rest of the organisation. Employees are concerned with fundamental values that are in line with the dominant corporate culture.

In an *orthogonal* sub-culture, the employees would simultaneously accept the core values of the dominant culture, as well as a set of distinct, but unconflicting values. Employees embrace the essential organisational values but also hold values that are peripheral to those of the overarching culture.

However, in contrast to sub-cultures, members of counter-cultures hold opposing values and could resist certain aspects of the dominant corporate culture. In *counter-culture* some core values of the counter-culture present a direct challenge to the core values of a dominant corporate culture. Counter-culture employees hold values that are in conflict with the fundamental or pivotal values of the dominant culture and could, ultimately, threaten the strength of the overall corporate culture (Martin & Siehl, 1983, pp 53-54).

It may be undesirable and unrealistic to attempt to assimilate all values and beliefs into one dominant corporate culture. It is, therefore, acceptable for sub-cultures to exist in an organisation. However, it is important that a core set of values is common to all sub-cultures (Hagberg Consulting Group, 2002, online). If all sub-cultures in an organisation have a common set of values, and the culture is beneficial to the organisation, it is imperative that this corporate culture is maintained.

2.7 Maintaining a Corporate Culture

As mentioned previously, corporate culture develops in an organisation over time. Once a corporate culture has developed, there are factors within an organisation that interact to maintain it by giving employees a similar set of experiences. These experiences ensure that those hired fit in with the culture, reward those who support it and reprimand those who challenge it (Robbins, 1993, p 610).

There are three factors that play an important part in maintaining a culture, namely; the *selection* process, the *actions of top management* and *socialization*. These three factors will be discussed in the following sections.

The first factor is the *selection* process. The explicit goal of the *selection* process is to identify and employ individuals who have the knowledge, skills and abilities to perform the jobs within the organisation successfully. But, typically, more than one candidate will be identified who meets any given job's requirements. The final decision as to who will be employed will be significantly influenced by the decision maker's judgment of how well the candidates will fit into the organisation's corporate culture.

This attempt to ensure a proper match, whether intentionally or unintentionally, results in the employing of people who have values essentially consistent with those of the organisation, or, at least, a good portion of those values. Additionally, the *selection* process provides information to applicants about the organisation and its culture. Candidates learn about the corporate culture, and, if they perceive a conflict between their values and those of the organisation, they can self-select themselves out of the application pool.

Selection, therefore, allows either employer or applicant to discontinue the relationship if there appears to be a mismatch in beliefs or values. In this way, the *selection* process maintains an organisation's culture by not selecting those individuals who might undermine its core values (Robbins, 1993, p 610).

The second factor is the *actions of top management*. The *actions of top management* also have a major impact on the organisation's culture. Through what is expressed and its actions, senior management establishes norms that filter down through the organisation (Robbins, 1993, p 611). The role of senior management in corporate culture will be discussed in more detail in Chapter 3.

The final factor is *socialization*. Employees, who have been chosen through the *selection* process, are not, as yet, fully indoctrinated in the organisation's corporate culture. New employees are likely to disturb the beliefs and customs that are in place. The organisation will, therefore, want to help new employees adapt to its culture. This adaptation process is called s*ocialization* (Robbins, 1993, p 612).

The most critical *socialization* stage is at the time of entry into the organisation. However, the organisation will be socializing every employee, though maybe not as explicitly, throughout his or her entire career in the organisation. This further contributes to sustaining the culture.

Socialization can be further divided into a three-stage process: pre-arrival, encounter and metamorphosis. The first stage, pre-arrival, encompasses all the learning that occurs before a new member joins the organisation. In the second stage, encounter, the new employee sees what the organisation is really like and confronts the possibility that expectations and reality may be different. If expectations prove to have been more or less accurate, the encounter stage merely provides for a reaffirmation of the perceptions gained earlier.

Where expectations and reality differ, the new employees should undergo *socialization* that will detach them from their previous assumptions and replace them with another set that the organisation deems desirable. This leads to the metamorphosis stage. In this third stage, the relatively long-lasting changes take place. The new employees master the skills required for their job and successfully perform their new roles.

The metamorphosis stage of the *socialization* process impacts on the new employee's work productivity, commitment to the organisation's objectives and eventual decision to stay with the organisation. The metamorphosis and the entry *socialization* processes are complete when the new member has become comfortable with the organisation and his or her job (Robbins, 1993, pp 612-613).

2.8 Conclusion

Corporate culture is a powerful, underlying, but often misunderstood, force within all organisations that contributes to the actions and behaviour of its employees. In order to gain a better insight into corporate culture, various definitions of corporate culture and

the types of power found in organisations were examined. In addition, it was seen that diverse classifications of culture exist, but regardless of the classifications of culture, each culture exists at the Three Levels of Corporate Culture.

It is vital that the senior management of an organisation understands, and is involved in, the shaping of the corporate culture, as it is the corporate culture that helps give the organisation its meaning and direction. It is also vitally important that a corporate culture that is contributing to the success of an organisation should be maintained.

The following chapter will investigate the role that management should play in the corporate culture of an organisation. The extent to which senior management should be responsible for shaping and moulding the corporate culture will be investigated, as well as what management should do to actively supervise the behaviour of employees through the corporate culture.

CHAPTER 3

MANAGING THE CORPORATE CULTURE

3.1 Introduction

As stated by Schwartz and Davis, “Getting one’s hand around a company’s culture is like putting one’s hands into a cloud”. Yet, this is what senior management should strive to do – understand the corporate culture in its organisation (1981, p 47).

In the previous chapter a comprehensive look was taken at corporate culture and the role that it plays in an organisation. Corporate culture was defined, the Three Levels of Corporate Culture were explained, as well as the dominant, sub- and counter-cultures that could exist in an organisation. This chapter will further explore corporate culture by investigating the contribution that senior management should be making in the shaping of a culture in its organisation.

This chapter will begin by examining the effects of a detrimental corporate culture and what management’s role should be in an organisation. The different management styles that result in different organisational environments will be explored, as well as the role that policies should play in influencing a corporate culture.

As mentioned in the previous chapter, an organisation develops a corporate culture whether it is aware of it or not. An organisation’s culture and its current traditions, and general way of doing things are largely due to what it has done before, and the degree of success it has had with those endeavors. As a result, the ultimate source of an organisation’s culture is its founders (Robbins, 1993, p 609).

When an organisation is first established, the founders and managers are concerned with establishing a particular corporate culture. In the early stages, the organisation's corporate culture is not, as yet, well established and mature and the founders have the most impact on an organisation's early corporate culture. This is because the founders have a vision of what the organisation should be and they are unconstrained by previous customs or ideologies. The founders' objectives, principles, values and behaviour provide important clues as to what is required from employees. The small size that typically characterizes new organisations further facilitates the founders' imposition of their vision on all employees. Over time, these cultural values and beliefs, established in the foundation of the organisation, become embedded in the daily routines of employees.

As the culture continues to evolve, the founders continue to attempt to entrench their own assumptions and beliefs in the organisation. This becomes more and more difficult for the founders as, increasingly, the learning process becomes shared amongst all employees. The cultural assumptions begin to reflect, not only the founders' initial assumptions, but also the total group's experiences. As such, strong leadership is required to sustain a corporate culture that enhances the successful running of an organisation (Quick, 1992, p 54; Kilmann, 1985, pp 62-63; Robbins, 1993, pp 609-610; Schein, 1990, p 115).

Therefore, management has a vital role to play in the shaping of a corporate culture in its organisation. Corporate culture will become an asset when shared beliefs and values generate a high degree of cooperation and commitment that would not necessarily be possible otherwise. This makes the organisation efficient. However, efficiency does not necessarily mean effectiveness. Efficiency is when something can be done with a minimum overhead of resources or with the least waste of effort. Effectiveness, however, is the degree to which the task that is being done is the appropriate or correct thing to do. Culture could, therefore, become a liability if it guides behaviour in inappropriate ways and there is efficiency but not effectiveness (Sathe, 1983, pp 5, 9-10).

3.2 Perpetuation of a Detrimental Corporate Culture

Unfortunately, in many organisations, senior management does not fully understand the culture in its organisation and, consequently, does not play an active role in shaping the corporate culture. Without a comprehensive understanding of the existing culture in its organisation, it can be very difficult for management to effectively evaluate whether new policies and strategies will be compatible with its corporate culture (Bettinger, 1989, p 38).

If the culture is not understood by management and, consequently, not managed properly, the corporate culture could actually be working against the goals of an organisation and could be detrimental to the organisation. Aspects of a corporate culture that could be detrimental to an organisation include, but are not limited to, miscommunication, lack of cooperation from employees, lack of commitment to the organisation and a great sense of complacency about the organisation's performance (Sathe, 1983, p 10; Tan, 2001, online).

Miscommunication is a common factor in everyday life and becomes even more complex in organisations. Miscommunication could occur between employees, but more importantly, between management and its employees. Even though establishing a corporate culture will not eliminate miscommunication completely, it does reduce the possibility that the members of an organisation will misunderstand one another. Corporate culture enables this in two ways. Firstly, there is no need to communicate things about which shared beliefs and values exist. Secondly, shared beliefs and values assist employees in interpreting the messages from senior management in the same way (Sathe, 1983, p 10).

A lack of cooperation from employees is a further sign of an unfavorable corporate culture. Management may force employees to comply with its policies through rewarding correct behaviour and disciplining incorrect behaviours. While this approach may succeed in trying to change or shape the culture, as will be discussed in Section 3.6, management cannot anticipate all the contingencies that could arise in its organisation.

When an unexpected contingency arises, management should rely on the cooperation of the employee to adhere to what is best for the organisation. The degree of true cooperation on the part of employees is influenced by shared beliefs and values, or, in other words, the corporate culture (Sathe, 1983, pp 10-11).

Another indicator of a detrimental corporate culture is where employees have a lack of commitment to their organisation. Employees will only feel a sense of commitment to management's vision and objectives if they identify with them. The shared beliefs and values of a corporate culture help develop this identification and sense of commitment to an organisation (Sathe, 1983, p 11). Factors that further encourage the commitment of employees to an organisation will be discussed in Chapter 6.

In an organisation with a corporate culture that is potentially detrimental, employees are reactive, taking little initiative to change and improve, and they adopt the 'wait for the top' attitude, while senior management is slow in taking action against non-performers in the organisation. A significant indicator of a detrimental corporate culture is where senior management is apathetic towards the corporate culture and does not implement change (Tan, 2001, online).

If management is apathetic, the employees will exhibit a sense of complacency as well. Management may have a vision, but because of complacency, this vision remains part of the *espoused values* of the organisation and not the *shared tacit assumptions*. To instill a more beneficial corporate culture in an organisation, the *espoused values* and *shared tacit assumptions* should be aligned with one another. However, if nothing is done to achieve the alignment of the *espoused values* and *shared tacit assumptions* levels of corporate culture, the detrimental corporate culture will be perpetuated through *socialization*. Therefore, as discussed in Chapter 2, new employees joining the organisation will, through *socialization*, be indoctrinated into the detrimental corporate culture and the miscommunication, lack of cooperation from employees, lack of commitment to the organisation and complacency will be continued.

Therefore, it is vital for the vision and goals of senior management, expressed at the *espoused values* level, to be aligned with the beliefs and values of employees, expressed at the *shared tacit assumptions* level. Furthermore, senior management should have the influence and authority to achieve the alignment of these two levels. To achieve this alignment, senior management has certain tasks to perform. The next section will focus on these tasks that senior management should execute in its organisation.

3.3 Management's Role in an Organisation

The alignment of the *espoused values* and *shared tacit assumptions* levels of corporate culture should be undertaken by the management of an organisation. These levels should be aligned to ensure that the vision of senior management becomes part of the corporate culture. As will be discussed in the following section, creating the vision for an organisation is a corporate governance duty of senior management. The senior management of an organisation has many responsibilities as part of its corporate governance duties in increasing the effectiveness and efficiency of its organisation. These duties, the pillars of corporate governance and risk management will be discussed in the following section.

Corporate governance is a modern expression for an issue which organisations have faced for decades – that of 'accountability'. At its most basic level, corporate governance is about how those entrusted with day-to-day management of an organisation's affairs are held to account for their decisions and actions and whether the organisation has the appropriate corporate structures to strengthen accountability. Accountability is an essential pillar in building and supporting corporate governance in an organisation. Together with accountability, three other pillars, equally essential to corporate governance, are recommended by South Africa's King II Report. These are responsibility, fairness and transparency (Brooks, 1997, online; King Report, 2001, p 17) and will be discussed briefly.

The first pillar of accountability ensures that individuals or groups in an organisation who make decisions and take actions are answerable for them. Mechanisms must exist in an organisation to allow for accountability. This provides investors with the means to question and evaluate the actions and decisions of senior management (King Report, 2001, p 14). The second pillar of responsibility, with regard to senior management, allows corrective action and counteracts mismanagement and misconduct. Responsible senior management would, when required, put in place what it would take to provide the guidance necessary in making the organisation effective and efficient. While the Board is answerable to the organisation, it must act responsively to and with responsibility towards all shareholders of the organisation. The third pillar of fairness ensures that systems within an organisation are balanced and take into account all those that have an interest in the organisation. The rights of various groups must be acknowledged and respected for fairness to be evident in an organisation. The final pillar of transparency is a measure of how good senior management is at making essential information available in an accurate and opportune manner. Transparency reflects whether or not investors attain a factual picture of what is happening inside the organisation (King Report, 2001, p 14).

One of the main duties of the managing director, together with senior management, is to set a clear vision and strategic direction for the organisation in a responsible manner that is accountable to stakeholders and ensures the protection of the assets and the reputation of its organisation (King Report, 2001, pp 45-47). According to the King II Report on corporate governance, senior management must lead its organisation through 'direction-giving' and strategy implementation. 'Direction-giving' is achieved through the creation and implementation of management policies (Planting, 2001, online; King Report, 2001, p 46). Consequently, senior management should ensure that policies and procedures are in place in the organisation to provide direction and the protection of assets. In doing so, the principles of corporate governance are adhered to. Management policies and their effect on corporate culture will be discussed in more detail in Section 3.4.

In addition, an organisation's policies should assist in management's corporate governance duty of risk management. Corporate governance can be viewed as an organisation's strategic reaction to mitigating unavoidable risks, in exchange for measurable rewards. As mentioned previously, senior management should provide strategic direction, while being mindful of the restraining forces that hinder the realisation of the vision (Charlton, 2000, p 42). These restraining forces are known as risks. A risk is an uncertainty about a potential event, or the possibility that a negative event is going to occur without an organisation being equipped to handle it (The Alliance, 2001, online; King Report, 2001, p 96). Risk management is necessary to mitigate the risks that an organisation could face. These risks may impede the attainment of the vision expressed at the *espoused values* level of corporate culture. Risk management can be defined as the identification and assessment of potential risks facing an organisation and encompasses all the collective processes used to decide what risks to avoid, control or accept. It is management's responsibility to establish the acceptable level of risk necessary to pursue the growth of its organisation (King Report, 2001, p 97).

This section detailed the essential functions that senior management should perform in the organisation as part of its good corporate governance duties. As discussed in this section, an organisation's policies should assist senior management in the achievement of acceptable corporate governance in an organisation. The role of policies in an organisation is discussed in the following section.

3.4 The Role of Policies in an Organisation

As discussed in the previous section, senior management should be held accountable for developing and communicating a clear and concise vision of the future for an organisation. The vision, and associated strategic direction, should also enable the organisation to compete. This vision might imply that, currently, the existing corporate culture does not require any change, as a natural evolution of the corporate culture will be sufficient to realise senior management's vision. Conversely, the vision might necessitate a slight, or extensive, change in the corporate culture of an organisation

(Beach, 1993, p 17; Charlton, 2000, p 42; Tan, 2001, online). Further, senior management's vision is implemented through the policies of an organisation.

The core objective of any policy, and the resulting procedures, is to influence and determine the decisions, actions and behaviour of employees by specifying what behaviour is acceptable and what behaviour is unacceptable (Whitman & Mattord, 2003, p 194). As such, organisational policies and procedures are necessary as guidelines to help employees do a consistently good job for their organisation (Drennan, 1992, p 23).

An organisation's corporate culture should be an important consideration for senior management when developing policies. For example, policies with substantial restrictions in an 'open' corporate culture will most likely encounter resistance from employees. The workplace is more than merely a place where people work. It is a place where people congregate, not only to perform their assigned work, but to socialise and exchange ideas about their jobs and their lives (Hare, 2004, p 925). Therefore, corporate culture should be a concern of senior management when developing policies. The role of senior management should, however, go beyond setting the vision and developing policies for the organisation. Management should communicate and change the mindsets of employees to win their commitment towards the change, or new direction, of the organisation. Management should address the critical shared values and beliefs the employees must possess in order to achieve the organisation's vision. By changing the shared values and beliefs of employees, senior management should address the *shared tacit assumptions* level of employees and, ultimately, the behaviour of employees (Tan, 2001, online).

As seen in Chapter 2, corporate culture should be maintained through the *socialization* process. New employees move through the pre-arrival stage, where the *espoused values* of the organisation are described in detail to them and on to the encounter stage. In the encounter stage, these new employees are exposed to the reality of the organisation and the behaviour of their peers, which may or may not agree with the organisation's *espoused values*. If the actions of fellow employees match the *espoused values* and

related policies of the organisation, this contributes to sustaining the corporate culture as the new employees will 'take their cue' from their peers. Likewise, if fellow employees' behaviour does not match the organisation's policies, the new employees will soon match the behaviour that is in contradiction to the organisation's policies. Similarly, senior management's attitude towards the policies of the organisation plays a large part in the acceptance of the policies. This is because employee behaviour is essentially driven by the urge to conform to expectations. If senior management treats policies and procedures as being inconsequential then the employee will treat the process with the same contempt. On the other hand, if management expressly describes what is expected in detail and continually expresses how imperative the policies and procedures are, then employees should follow suit (Drennan, 1992, p 17).

The actions and behaviour of employees will also be affected by the organisational environment evident in an organisation. The three general organisational environments that could exist within an organisation's corporate culture, namely; Coercive, Utilitarian and Goal Consensus, will be detailed in the following section.

3.5 Organisational Environments within an Organisation's Corporate Culture

There are generally three key environments that could exist in organisations. These environments dictate how the organisation is run and how employees react in certain circumstances. These environments are Coercive, Utilitarian and Goal Consensus Environments (Schein, 1992, online).

The Coercive Environment is one where employees feel alienated in their environment and seek to leave it if possible. Typically, it is condign power that is exerted in the Coercive Environment. As a result, peer relationships in this environment develop in defence of the authority in the organisation, in other words, senior management. These employees perform tasks because they are obliged to do so, rather than because they agree with the actions and decisions of senior management (Schein, 1992, online).

The Utilitarian Environment is one where employees participate in their organisation by evolving workgroups based on an incentive system. In this environment, employees will do as senior management wishes because of the rewards that they will receive as a result of compensatory power. They still do not necessarily agree with senior management (Schein, 1992, online).

The third organisational environment, the Goal Consensus Environment, is one where employees are morally involved with the organisation. They identify with the organisation, share the same beliefs and values of senior management and they are striving towards the vision of senior management. In this environment, employees' actions are not as a result of being forced to do so or because of a reward, but because they are in agreement with the way things are done in the organisation (Schein, 1992, online). Conditioned power is predominant in this environment. This Goal Consensus Environment could be seen as a corporate culture which is in line with the vision of senior management. This would mean that 'right' decisions and actions of employees become second-nature and part of their culture (Schein, 1999, pp 15-17).

These organisational environments affect the entire organisation and influence the behaviour of employees and will be discussed further in relation to the Three Levels of Corporate Culture in Chapter 5. The alignment of the corporate culture with the vision of senior management, as is evident in the Goal Consensus Environment, is easier said than done, however. As mentioned in Chapter 2, many of the essential components of corporate culture are, in essence, invisible and particularly complex to change. The subsequent section will detail the fundamental components of corporate culture that must be addressed to encourage culture change.

3.6 Changing the Corporate Culture

Employee attitudes are fundamentally an artifact or result of the corporate culture environment in which they work. External conditions may have an influence on the behaviour and attitude of employees as well. For example, if unemployment is on the increase and employees feel they need to protect their jobs, they may provisionally

become more amenable and supportive. Nevertheless, the environment which has the most influence on employee attitude and behaviour is the internal environment. Therefore, the power to change corporate culture is largely senior management's responsibility (Drennan, 1992, pp 3-4).

One of the most stable aspects of an organisation is the corporate culture, and because of this, transforming it is a complex task. Corporate culture cannot be addressed directly by simply issuing slogans or making speeches. Changing the culture involves having to unlearn beliefs and assumptions and learn new ones. The attitudes, values and behaviour of employees in an organisation should also change to foster the development of the culture. Employees, however, are opposed to change because unlearning is uncomfortable and creates apprehension. Further, employees prefer structure and a known framework within which to work, so that they can adapt their behaviour to manage their environment successfully. Anxiety will arise if this framework requires change. Employees can be coerced into changing their overt behaviour, but such behaviour change is not stable unless the deeper levels undergo transformation (Schein, 1999, p 26; Drennan, 1992, p 4). Therefore, it is vital that the *shared tacit assumptions* level of corporate culture, detailed in Chapter 2, is addressed when attempting culture change.

Both the articulation and communication of a clear vision for an organisation is essential in developing a strategy for change. Until senior management formulates a clear vision and persuades employees to be dedicated to that vision, they will not be able to generate the enthusiasm and resources needed for significant cultural change (Hellriegel et al, 2004, p 372).

Once the vision has been formulated, senior management's role in changing corporate culture, at a minimum, should be to demonstrate clear, visible actions in support of the organisation's cultural values. Employees need to know what is important, and one way for employees to gain this information is to observe and pay attention to those in higher positions. The culture of an organisation is not formed by what management preaches or

publishes, but what it accepts in practice. When senior management not only espouses that something is important, but also consistently behaves to support this message, employees will begin to believe what is espoused (Drennan, 1992, p 3).

An additional means to change and shape the corporate culture is to instill a comprehensive reward system in an organisation. Many organisations have a system of punishing divergent behaviour that is not in line with organisational policies. The focus is on negative reinforcement. Other organisations identify behaviour that supports the organisation's objectives and rewards that behaviour in positive ways. The focus is on positive reinforcement. It is generally considered that positive reinforcement is far more effective than negative reinforcement. However, this reward system should not merely be monetary rewards, but should rather focus on acknowledgment and approval of correct behaviour. There should not be any ambiguity about what management espouses and what behaviour is rewarded, as is often the case. For example, management might espouse that it supports innovation, but even the slightest failure is punished, which does not encourage innovation at all. Therefore, if there are inconsistencies between what senior management espouses and what is actually rewarded, employees will be confused (Bettinger, 1989, p 40).

Even though changing an organisation's culture is extremely difficult, the corporate culture can be changed. Culture change is most likely to take place when one or more of the following conditions exist (Robbins, 1993, p 625):

- *Dramatic crisis*

  A dramatic crisis is a shock that undermines the status quo of the organisation and questions the relevance of the current corporate culture. The existing corporate culture is seen as inadequate, and management and employees see a need for a more suitable corporate culture. A crisis could include an unforeseen financial setback or loss of a major customer.

- *Turnover in leadership*

  As discussed previously, senior management should play a large role in shaping the corporate culture of its organisation. Usually, if there is a change in the management of an organisation, there is a shift in its vision and values. It is possible that the new management may be perceived as more capable than previous leadership, and the new vision and values are accepted.

- *Young and small organisation*

  The corporate culture of an organisation will be less entrenched if an organisation is still in its formative years. The younger the organisation, the simpler it will be to change the trajectory of the corporate culture. Similarly, it is easier for management to communicate its vision and values to employees when the organisation is small.

- *Weak culture*

  Over time, a corporate culture stabilises and becomes embedded in the organisation. The more widely held a culture is, and the higher the agreement among members on its values, the more difficult it will be to change. Conversely, weak cultures are more amenable to change than strong ones.

In addition to these conditions, a culture change may be forced in organisations if a merger occurs between two organisations with two distinct corporate cultures. Unfortunately, the compatibility of the two organisations' corporate cultures usually only becomes a consideration once the merger has taken place. The failure to successfully integrate two differing cultures could cause the financial results to fall below expectations (Bettinger, 1989, p 38).

This leads, in many cases, to what Schein refers to as cultural 'indigestion' and to corporate cultures that cannot successfully be integrated. When merging, organisations must avoid reaching agreement at the *artifacts* and *espoused values* level only, while disagreeing at the *shared tacit assumptions* level. However, even if the *shared tacit*

assumptions are mostly in agreement, conflict is inevitable when the corporate culture of two organisations merge. Each culture must change to some extent, and the process of adjusting to the merger is known as acculturation (Schein, 1990, p 117; Malekzadeh & Nahavandi, 1990, p 56). There are four general methods of acculturation: namely, Integration, Assimilation, Separation and Deculturation (Malekzadeh & Nahavandi, 1990, pp 56-57), which will be discussed in the following subsections.

- *Integration*

  This first method of acculturation is integration. With this method, there is a rather balanced exchange of cultural and managerial practices between the merger partners, and neither of the two corporate cultures is imposed on the other. This method is common when the two organisations have much in common.

- *Assimilation*

  The second method of acculturation is assimilation. This method results in one organisation's corporate culture dominating the other – but the domination is not forced. Instead it is welcomed by the employees of the non-dominant organisation, who may believe that their current corporate culture and practices are not favourable for success. In other words, the non-dominant organisation has a weak culture and, as mentioned previously, weak cultures are more open to change.

- *Separation*

  The third method of acculturation is separation. With this method, the corporate cultures of both organisations remain separate with restricted cultural and managerial exchange. The key for the separation method to succeed is for the organisation that is acquiring the other to allow its acquisition a high degree of independence and only enforce essential cultural features.

- *Deculturation*

  The fourth method of acculturation is deculturation. Of all the methods, it is this one that is the most destructive. Unfortunately, it is also the method that is used most often. This method involves the disintegration of one of the organisation's corporate cultures, as a result of intense pressure from the dominant organisation to conform to its culture and practices. This method is usually accompanied by a high amount of confusion and conflict.

Regardless of the ultimate goal, changing the corporate culture of an organisation takes dedication and time. There must be commitment at all levels of the organisation, from management to employees, in order for change to be accomplished. If nothing changes in the procedures of the organisation, or the attitudes of its management, employee attitudes will not change either (Drennan, 1992, p 3). The most profound culture change takes place when employees buy into the vision and strategies of senior management.

3.7 Conclusion

Senior management has a significant role to play in shaping the corporate culture in its organisation. In order to address the corporate culture, senior management must ensure that correct corporate governance practices are entrenched in its organisation. The pillars of accountability, responsibility, fairness and transparency are necessary to ensure good corporate governance. In addition, as part of management's duties, an organisational vision must be expressed in management policies. These policies should be enforced to assist management in curbing incorrect behaviour in its organisation and, ultimately, change the corporate culture.

Transforming the corporate culture, however, takes time and perseverance. Unlearning beliefs and changing the attitudes of employees can be a painful process. Further, it is senior management's task to lead this transformation in attitude by setting an example, so that the change can 'filter down' throughout the organisation. If management demonstrates that the need for changing the 'way things are done' is vital to the

sustainability of the organisation, it will highlight and encourage the change in corporate culture.

The sustainability of many organisations is largely dependent on the protection of its information assets. The subsequent chapter will detail the realities of information security in many organisations and both the human and management aspects of information security.

CHAPTER 4

THE MANAGEMENT AND THE HUMAN DIMENSION OF INFORMATION SECURITY

4.1 Introduction

Thomas Jefferson stated that maintaining freedom requires 'eternal vigilance'. When it comes to a society where information is its lifeblood, maintaining privacy and security of information requires no less (Mitnick & Simon, 2002, p 103; Gordon, 2002, online).

The previous chapter examined the role that the senior management of an organisation should play in shaping the corporate culture in its organisation. The foundation and evolution of a corporate culture was investigated and the influence that the corporate culture has on the behaviour and actions of employees was explored.

This chapter will investigate the realities of information security in most organisations and the important role that information security should be playing in protecting one of the most essential assets of an organisation. Moreover the crucial effect that employee behaviour and actions have on the success of information security in an organisation will be analyzed. The role of senior management in the development of a Corporate Information Security Policy, and the effect it should have on an information security culture will be explored, as well as the common misconceptions that senior management has concerning information security.

4.2 Information Security Facts

"Many UK businesses are a long way from having a security-aware culture". This is according to PriceWaterhouseCoopers' Information Security Breaches Survey (ISBS) 2006. In numerous organisations, very little emphasis is placed on the protection of information and the expenditure on security is low. Two-fifths of organisations spend

less than one percent of their IT budget on information security. Further, even though three times as many organisations have security policies than six years ago, three-fifths of all organisations are still without an overall security policy. There does, however, seem to be a correlation between the priority senior management gives to information security and the existence of a Corporate Information Security Policy. In 55 percent of organisations where senior management views security as having a high priority, a policy exists, whereas only 13 percent of those organisations that see security as a low priority have a policy. The role of senior management in information security will be explored in more detail later in this chapter.

Information security should be a senior management concern as an organisation and its reputation can be severely tarnished if its information security procedures are perceived as being inadequate or unsatisfactory (Freeman, 2004, p 917). The average cost of the worst security incident for large organisations ranged from £65,000 to £130,000, while smaller organisations' cost ranged from £8,000 to £17,000. Of this total cost, £5,000 to £10,000 in large organisations, and £100 to £400 in smaller organisations, was as a result of damage to reputation. Overall, the cost of security breaches in United Kingdom organisations has increased over the past two years and is in the order of ten billion pounds (PriceWaterhouseCoopers, 2006, online).

When it comes to the human side of information security, one in eight organisations does nothing to educate their employees about security responsibilities. In addition, recruitment processes at a quarter of the organisations do not include any background checks on potential employees and, of those organisations that believe security is a very high priority, 19 percent do not perform background checks (PriceWaterhouseCoopers, 2006, online). These facts emphasise the impact that information security breaches could have on an organisation and the often insufficient attention that is paid to the human side of information security.

4.3 The Protection of Information Assets

Where once computers and technology were regarded with trepidation and mistrust, they are now firmly embedded in the structure of industry and commerce. It is now understood that there are two keys to effective technology use. One is managing the information. The other is ensuring that information remains secure. The value of information to an organisation cannot be overemphasised, especially in a contemporary knowledge based economy. Information is probably the most valuable asset of most organisations (Sharp, 2004, p 768).

As one of the most important assets of an organisation, information must be properly protected. Although there are six pillars of information security as defined by the ISO standard, namely: confidentiality, integrity, availability, nonrepudiation, assurance and auditing, the focus of this research will be on the more traditional ones, i.e. confidentiality, integrity and availability. These three pillars of confidentiality, integrity and availability are briefly described in the following subsections.

4.3.1 Confidentiality

Confidentiality, with regards to information security, is concerned with ensuring that information of a specific classification is not distributed to persons outside the category for which it is classified. Confidentiality ensures that sensitive information is prevented from being disclosed to unauthorised parties (Krige, 1999, p 8; Bruce & Dempsey, 1997, pp 36-37).

4.3.2 Integrity

Integrity is concerned with the quality and reliability of information, such that management can be assured that information on which decisions are based has not been modified dishonestly or otherwise. Integrity means that an asset or information can only be modified by authorised parties or only in authorised ways (Krige, 1999, p 9; Bruce & Dempsey, 1997, p 37).

4.3.3 Availability

> Availability is concerned with guaranteeing the availability of systems and information on a timely basis such that strategic and business decisions can be effected as rapidly as possible. In the event that systems or data are unavailable, opportunities may be lost, deadlines missed or commitments defaulted. Even if the information is exactly what is needed to meet business requirements, it must be available to complete the task in a reasonable time (Bruce & Dempsey, 1997, p 41).

It is vital that these three pillars are ensured as the protection of the information assets of an organisation takes on a slightly different dimension compared to other assets. When money or goods are stolen, somebody will notice they are gone. When information is stolen, most of the time no one will notice because the information is still in their possession (Mitnick & Simon, 2002, p 140). It is difficult to estimate the exact value of the information assets of an organisation. However, if the confidentiality, integrity and availability of information are not protected, it could lead to the depreciation of shares, loss of customer confidence in the organisation and irreversible damage to the organisation's reputation (Zylt, 2001, online). Therefore, the protection of information should lead to the protection of the organisation as a whole. An aspect of information security that must be considered is that security breaches do not only occur from external sources. Many security incidents occur within an organisation due to careless internal security or because organisations have the incorrect impression that all employees are adhering to the correct information security practices (Zylt, 2001, online).

The aim of information security should never be to secure an organisation absolutely, as this will almost always lead to failure. The aim of information security should be to ensure an adequate level of information security that is sustainable, such that information assets are protected and kept safe, and to ensure information is valuable to the organisation (Deloitte & Touche, 2002, online). Further, information is valuable in proportion to its timely availability and, in most cases, to its secure availability (Sharp, 2004, p 768).

However - even if the best physical and technical controls have been put in place in an organisation to ensure the confidentiality, integrity and availability of the information – it is not guaranteed that the information will be secure. As Kevin D. Mitnick says in his book *'The Art of Deception – Controlling the Human Element of Security'* (2002, p 79) – "Don't rely on network safeguards and firewalls to protect your information. Look to your most vulnerable spot. You'll usually find that vulnerability lies in your people".

4.4 Human Factor of Information Security

An organisation's employees are considered a corporate resource and asset, requiring constant care and management in their daily activities. For the majority of these employees, their first priority at work is to get the job done. As a result of the pressure related to an employee's job, any tasks that are not deemed essential to 'getting things done' are often overlooked or regarded as hindrances. Therefore, if employees see security as something that is an obstacle to their work, they might not take on proper responsibilities, and worse, might go out of their way to find a 'workaround' to any security measure they do not consider necessary (Freeman, 2004, p 917; Mitnick & Simon, 2002, p 72; Shorten, 2004, p 924).

In addition, the security industry appears to have overlooked the fact that computers and related technologies are simply tools, and that it is humans that are using, configuring, installing and, often, abusing these tools. This is because the security industry has mainly been focused on hardware, software and technical aspects of security (Berti & Rogers, 2004, p 147). Technologists have systematically developed information security solutions to minimise the risks connected with the use of computers. However, they have not sufficiently addressed the most important vulnerability, the human factor. The human part of any information security solution is the most essential. Almost all information security solutions rely on the human element to a large degree and employees continue to be the most severe threat to information security (Mitnick & Simon, 2002, p 8; Berti and Rogers, 2004, pp 150-151). Therefore, information security should be more than just

implementing an assortment of technical controls. It should also address the behaviour and resulting actions of employees (Berti & Rogers, 2004, p 147).

In order to safeguard its information assets it is imperative for organisations to stimulate a corporate culture that promotes employee loyalty, high morale, and job satisfaction. Through the corporate culture, employees should be aware of the need for protecting information and of the ways inappropriate actions could affect the organisation's success (Freeman, 2004, p 922). It is vital to get employees committed to and knowledgeable about their roles and responsibilities with regard to information assets. Further, it is imperative for senior management to create, enforce and commit to a sound security program (Henry, 2004, p 663).

Instilling a sound security program and making employees knowledgeable about their information security responsibilities will, in most cases, make employees more aware of the threats facing the information assets. If employees are unaware of their security responsibilities and are not alert to the threats facing information assets, this human vulnerability could be exploited. An example of this exploitation is social engineering. The widely accepted definition of social engineering is "successful or unsuccessful attempts to influence a person(s) into either revealing information or acting in a manner that would result in unauthorized access, unauthorized use, or unauthorized disclosure, to an information system, network or data" (Berti & Rogers, 2004, p 148).

It is often said that the only secure computer is an unplugged one. However, through skillful, clever techniques, a social engineer could persuade someone to plug the computer in and switch it on. Social engineering concentrates on the weakest link in the information security chain and, as a result, the computer, and the information it houses, is still vulnerable. The more aware employees are, however, the less likely a social engineer will succeed.

Becoming a victim of a social engineering attack has nothing to do with intelligence, but has everything to do with being human and not having the correct mindset and training to

recognise this type of attack (Berti & Rogers, 2004, p 148). In addition to human nature, rapid advances in technology have made the business environment favourable for social engineering attacks. It is not unusual to have never met the people that one deals with on a regular basis and face-to-face communication is becoming more scarce. In addition to this, people are usually trusting, cooperative and eager to help. However, it is often this eagerness to help out a co-worker with a problem that is an issue. On the one hand, this cooperation and aid is part of what ensures successful business practices. While, on the other hand, this helpfulness can be a major vulnerability that a social engineer will attempt to exploit (Mitnick & Simon, 2002, p 89; Berti & Rogers, 2004, p 148). It is vital, therefore, that employees know their information security responsibilities and are alert to any potential attacks or attempted security breaches.

Since information security in an organisation is only as good as the people implementing it, senior management needs to enlist the support of every employee in the organisation. Much of this support can be accomplished through understanding. When employees understand why security is needed the atmosphere and environment will lead to greater security and trust (Henry, 2004, p 675). In other words, the corporate culture in an organisation should evolve to become more security conscious to ensure employees are no longer a significant threat to information assets.

4.5 Information Security as Part of the Corporate Culture

As seen in the previous section, it is often the behaviour and actions of employees that are the weakest link in the information security chain in an organisation. Furthermore, given that even seemingly innocuous information in the hands of a malicious person could be exploited to obtain the key to an organisation's most valued secrets, employees should be alert to possible threats to an organisation's information (Martins & Eloff, 2002, p 204; Mitnick & Simon, 2002, p 29).

Many information technology professionals have the mistaken belief that their organisations are impervious to attack as they have deployed security features such as

authentication, intrusion detection and firewalls. Likewise, as many aspects of information security involve technology, many employees believe that security issues are being handled by firewalls and other security technologies deployed by the information technology professionals at their organisation. However, the reality is that most employees are the 'front line' required to protect the overall security of the organisation (Mitnick & Simon, 2002, p 250).

Employees must learn to fully appreciate that a severe loss of sensitive corporate information could not only jeopardise the organisation, but their own personal information and jobs as well. It is vital that employees realise the importance of protecting information assets and the role that they should be playing in the security of information. Employees who do not fully understand their roles are very often apathetic to information security and may be enticed to overlook or simply ignore their security responsibilities.

To be genuinely effective information security needs to become part of the way every employee conducts his or her daily business (Deloitte & Touche, 2002, online). Information security should become an organisational lifestyle that is driven from the top.

In order for information security to become part of the daily activities of an organisation, it is imperative that information security concepts and practices become part of an organisation's corporate culture. Senior management has an important part to play in cultivating the corporate culture in its organisation. This topic is discussed in the following section.

4.6 Management's Role in Shaping an Information Security Conscious Corporate Culture

One of the common complaints from security professionals is related to the fact that they feel management does not understand, or properly appreciate, the problems related to ensuring the protection of an organisation's information (Hall, 2001, online). This could be as a result of the fact that senior management can normally only allocate a limited

amount of time and consideration to information security. As a consequence, management's attention is often limited to a small set of acute threats and countermeasures that relate to the issues of the day. More comprehensive security measures are often not paid the attention they deserve as management is not aware of their importance to the organisation (Buren, van der Meer, Shahim, Barnhoorn & Roos Lindgreen, 1999, p 76).

However, as emphasised by Deloitte & Touche, "Information security requires a whole-hearted organisational commitment of resources (financial, human and technological) to an enterprise-wide program designed to evolve and adapt to new dangers" (2002, online). Therefore, senior management should not just be made aware of the need to protect information. The organisational commitment to information security should be driven by senior management and a great deal of emphasis should be placed on the employees of an organisation to highlight their role in protecting information.

Conscientious and suitably educated employees can be one of the strongest links in an organisation's information security infrastructure. Employees can respond rapidly, absorb new information and react in inventive ways to new situations, whereas a machine, and the related technology, is constrained by the rules which it has been given. Conversely, a machine will enforce a rule it does not understand, while employees will not implement a rule they do not believe in (Henry, 2004, p 663). This is an important consideration for senior management when attempting to shape an Information Security Conscious Corporate Culture in its organisation.

As described in Chapter 3, corporate policies play a large role in shaping the corporate culture in an organisation. Policies are instrumental in forming a 'rules of behaviour' for employees as they define what is allowed and what is not allowed in the corporate context. It follows that the Corporate Information Security Policy should do exactly that. The policy, and associated procedures, must clearly define appropriate and inappropriate behaviour in the context of protecting information assets (Mitnick & Simon, 2002, p 73; Fenton & Wolfe, 2004, p 888).

A Corporate Information Security Policy needs to be created in order to provide guidelines for the correct handling and release of information considered critical and sensitive within an organisation. A Corporate Information Security Policy should also make management's attitude to any actions that threaten the security of information assets explicit (Robiette, 2001, online; Berti & Rogers, 2004, p 154). The Corporate Information Security Policy, and the related procedures, should outline for employees what actions are permissible, what actions are not permissible, what they must do, and what their responsibilities are towards information assets (Shorten, 2004, p 917). If an organisation's Corporate Information Security Policy leaves an issue unaddressed, employees may use the 'path of least resistance' and take whatever action is most convenient for them (Mitnick & Simon, 2002, p 193).

To be effective, information security must span the entire organisation — from the top to the bottom, from the managers to the end users. A successful Corporate Information Security Policy requires the leadership, commitment, and active participation of senior management (Mitnick & Simon, 2002, p 7; Berti & Rogers, 2004, p 152). As a result, senior management has specific responsibilities in the development and the implementation of the Corporate Information Security Policy. Firstly, senior management must clearly articulate its vision for information security in the policy. As seen in Chapter 3, the foundation for any policy is the vision of senior management. This is particularly true in the case of information security. An information security vision should not be unattainable or unrealistic, but should rather be to achieve an adequate level of information protection that is sustainable. Complete, 100 percent security is not, and never should be, the goal – this vision will never be realised (Henry, 2004, p 664; Deloitte & Touche, 2002, online). Secondly, senior management must explicitly communicate the policy to the entire organisation. Communication is, arguably, the key to the accomplishment of a thriving information security infrastructure. The Corporate Information Security Policy should convey the corporate attitude towards information security and senior management must ensure that it is leading by example in information

security practices. Lastly, senior management must ensure that the necessary resources are available for the implementation of the policy (Hare, 2004, p 926).

If the Corporate Information Security Policy is communicated properly to employees, so that the appropriate behaviour described in the policy is implemented on a daily basis, the result should be an organisation that is more vigilant at all levels, and an organisation comprised of employees who believe they are 'contributing' to the well-being of the overall organisation (Berti & Rogers, 2004, p 152). A successful Corporate Information Security Policy should generate a high degree of consensus amongst all of those involved, and should foster a positive attitude towards security in terms of its benefits to the organisation. In addition, a successful policy can foster a corporate culture that is essential to leverage advantages while limiting the risk to information assets (Robiette, 2001, online; Gordon & Glickson, 2001, online).

However, even though there are clear benefits to incorporating information security practices into the corporate culture; the senior management of many organisations still has mistaken beliefs regarding information security and the role of senior management in its implementation, which hinders the creation of an Information Security Conscious Corporate Culture.

4.7 Management Myths about Information Security

For numerous organisations' senior management, information security may seem like a cavernous blackhole into which huge amounts of cash are poured with few measurable outcomes. In addition, in many organisations, senior management has erroneous beliefs regarding information security. This contributes to poor enforcement of information security standards and practices in organisations as senior management does not fully understand or appreciate the role of information security in its organisation. The consequences for an organisation's financial health and reputation could be devastating if information is accidentally or deliberately disclosed to the wrong people, falsified or corrupted or rendered unavailable for a period of time (Gordon, 2002, online). The

following subsections will describe a few of the common myths of senior management with regard to information security that could impede the implementation of a comprehensive information security infrastructure.

- **All problems will be solved with physical and technical controls**

  In the past, physical and technical controls may have been sufficient to protect the information assets of an organisation, but in contemporary organisations these are no longer enough. Hardware, software and technologies are only a few of the components in the overall security program. Physical and technical controls are tangible and are easier to enforce and, consequently, usually receive more attention from management than the operational controls needed to sustain information security in an organisation. Operational controls determine the actions employees must use in order to sufficiently protect information. The effectiveness of information security controls largely depends on the competency and dependability of the people who are implementing and using them. Management must have a vision for how information security will be addressed and must recognise that something more than physical controls and hardware and software solutions are necessary to provide a holistic information security solution. As detailed earlier in the chapter, the human element is a fundamental component of an information security solution, which management often overlooks (Shaurette, 2004, p 650).

- **Information security has been accomplished once the policy has been written**

  The Corporate Information Security Policy should be the foundation for a comprehensive information security implementation and not the ultimate goal. Information security has not been accomplished once the policy has been written, as it is not enough for senior management to merely outline the vision for information security in the Corporate Information Security Policy. Once a policy has been created, the organisation should begin striving towards the

vision outlined in the policy. If a Corporate Information Security Policy is written but never implemented or enforced, or if the policy is enforced inconsistently, it is almost certainly worse than if no policy existed at all. As detailed previously, policies inspire what behaviour is acceptable and what behaviour is unacceptable and it is through procedures that the behaviour is prescribed. Therefore, as described in Chapter 3, policies and procedures must be decisively implemented in an organisation to be effective. Over time, the behaviour prescribed in procedures should become a way of life in the organisation. If employees do not understand the importance of acceptable information security practices, or have the belief that information is not significant to the organisation, they may be apathetic in their information security practices and procedures. Therefore, the communication of the policy to the employees of an organisation becomes essential (Shaurette, 2004, p 651).

- **All employees will comply once the policy is published**

  However, even once the Corporate Information Security Policy has been published and communicated to employees, there is still no guarantee that they will comply with what is written. It should be ensured that employees understand the policy and the part they must play in the protection of information. Simply publishing the policy will not guarantee that employees will comply with it. Simply making employees aware is also not enough – this will most likely lead to superficial security. In fact, Information Security Awareness alone could have a negative effect by teaching employees how to avoid information security in their activities. Information Security Awareness will be discussed in more detail in Chapter 7. It is likely that employees will find a way to circumvent security measures if they do not fully comprehend the benefits of protecting information. Employees must be educated about the Corporate Information Security Policy, and the corresponding procedures, in order for them to fully understand their roles and responsibilities in the

protection of information. In addition, there must be motivation for complying with the policy (Shaurette, 2004, p 652).

These myths represent three of the major areas of information security that need to be addressed in organisations. Firstly, information security cannot be successful with only physical and technical controls. The human aspect of information security, as described previously, must be addressed in an organisation. Secondly, even though a Corporate Information Security Policy may exist on paper in organisations, very often this policy is never enforced and has no influence in an organisation. And, thirdly, even if a Corporate Information Security Policy is published and employees are made aware of the policy, it does not mean that employees will adhere to what is written in the policy.

4.8 Conclusion

In a holistic view, information security should be a triad of people, process, and technology. Appropriate technology must be combined with management and employee support to ensure the protection of information. A clear Corporate Information Security Policy, which outlines the vision that senior management has for information security, must be drafted. However, it is not enough for the policy just to be created. Through the policy, employees must begin to understand their roles and responsibilities towards the protection of information. It is through understanding that employees will begin to incorporate the correct information security practices into their daily behaviour. Further, as these information security practices become part of the everyday activities of employees, an Information Security Conscious Corporate Culture will begin to emerge. As seen from this chapter, however, senior management's incorrect perceptions concerning information security often hinder the implementation of effective information security practices in an organisation.

It is imperative that the misconceptions are overcome and that senior management's attitude towards information security is supportive and that management helps shape the corporate culture. By cultivating an Information Security Conscious Corporate Culture,

diligent and security conscious employees can become the strongest link in an organisation's security infrastructure.

The following chapter will explore the relationship that should exist between corporate culture, corporate governance and information security. The term Corporate Information Security Obedience will be defined and the link between the organisational environments detailed in Chapter 3 and the Three Levels of Corporate Culture will be explored.

CHAPTER 5

CORPORATE INFORMATION SECURITY OBEDIENCE

5.1 Introduction

In Chapters 2, 3 and 4, the relationships between corporate culture, corporate governance and information security have been explored. The Three Levels of Corporate Culture of which all cultures consist, and the importance thereof, were investigated. The distribution of power and the three types of power in organisations were looked at, as well as the classifications of culture that could be found in organisations. The roles of sub- and counter-cultures in organisations and how best to maintain a corporate culture were also investigated.

Further, the role that senior management should play in shaping the culture in its organisation was explored. The indicators of a corporate culture that could be detrimental to an organisation and the various organisational environments, which result from different management styles, were investigated. In addition, the vital role that corporate policies play in shaping the corporate culture was explored.

Additionally, the management and human dimensions of information security were examined. The importance of the human factor in the protection of information security and why information security should become part of the corporate culture were highlighted. Management's role in shaping an Information Security Conscious Corporate Culture, and the myths often held by senior management regarding information security were also investigated.

The first three sections of this chapter will reiterate the relationships expressed in previous chapters between, firstly, corporate culture and corporate governance, secondly,

information security and corporate governance and, thirdly, corporate culture and information security. Subsequently, this chapter will synthesise the three disciplines of corporate culture, corporate governance and information security and define the relationship that should exist between these three fields to promote the protection of the information assets of an organisation. This relationship will be defined as Corporate Information Security Obedience.

5.2 Relationship between Corporate Culture and Corporate Governance

As described in Chapter 3, senior management has an imperative role to play in shaping the corporate culture of its organisation and strong leadership is required to ensure the organisation continues to be successful.

Through its corporate governance duties, senior management must set a clear vision and strategic direction for the organisation. This vision should manifest in the corporate policies of an organisation. The corporate culture of an organisation should be a key concern of management when developing the policies for its organisation as the culture will largely influence the response the employees will have to a policy once approved and introduced. Further, the main objective of a policy, together with the consequential procedures, is to determine the actions and behaviour of employees by outlining what should be and what should not be done in an organisation. However, simply developing and publishing a policy will not necessarily positively influence the behaviour of employees and the resulting corporate culture. The corporate governance duties of senior management, however, should go beyond setting the vision for an organisation and policy development.

Management should effectively communicate the vision and corporate policies to employees, and even more importantly, lead by example. Employees will, most often, not react to what is preached by senior management, but rather to its attitude and actions. Thus, if senior management treats corporate policies and procedures as ‘window dressing’ and negligible then employees will usually adopt the same attitude.

Alternatively, if management stresses the importance of adhering to corporate policies employees are more likely to follow corporate procedures and adhere to the correct behaviour. Therefore, the power to change the behaviour of employees, and the resulting change in corporate culture, lies largely in the hands of senior management. The relationship that should exist between corporate governance and corporate culture is represented in Figure 5.1.

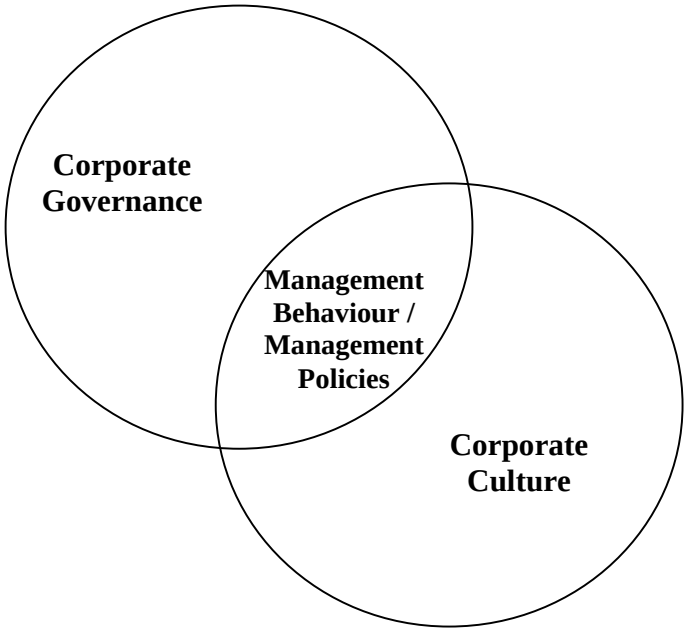

Figure 5.1: The relationship between corporate governance and corporate culture

Figure 5.1 illustrates that it is through senior management's corporate governance duty of directing that the corporate culture should be changed. These management policies must then be communicated to employees to be truly effective. Figure 5.1 further illustrates that one of the most effective ways that management can communicate the corporate policies to employees is through its own actions and behaviour.

5.3 Relationship between Information Security and Corporate Governance

Part of senior management's corporate governance duties, as discussed in Chapter 3, includes both accountability and responsibility for the protection of the assets and reputation of its organisation. Further, senior management should ensure that the

necessary policies and procedures are in place in its organisation to guarantee the protection of assets.

As discussed in Chapter 4, information is often described as the lifeblood of an organisation and is one of the most essential assets of any organisation. It follows, therefore, that one of the most significant corporate governance duties of senior management should be the protection of information. One of the main complaints from security professionals is the lack of support from senior management when it comes to ensuring the protection of information. In addition, as seen in Chapter 4, there does seem to be a close connection between the priority senior management gives to information security and the existence of a Corporate Information Security Policy. The higher management's priority of protecting information, the more likely a policy will exist.

It is of vital importance that senior management commits to an information security program in its organisation. One way to demonstrate such commitment is through the creation and dissemination of a Corporate Information Security Policy. This policy, and its procedures, must clearly define what is expected from employees in the protection of information assets. It is imperative that the Corporate Information Security Policy makes senior management's vision for information security clear. In addition, senior management should lead by example in the protection of information assets and must ensure that the resources required are available for the Corporate Information Security Policy to be implemented. The relationship that should exist between information security and corporate governance is represented in Figure 5.2.

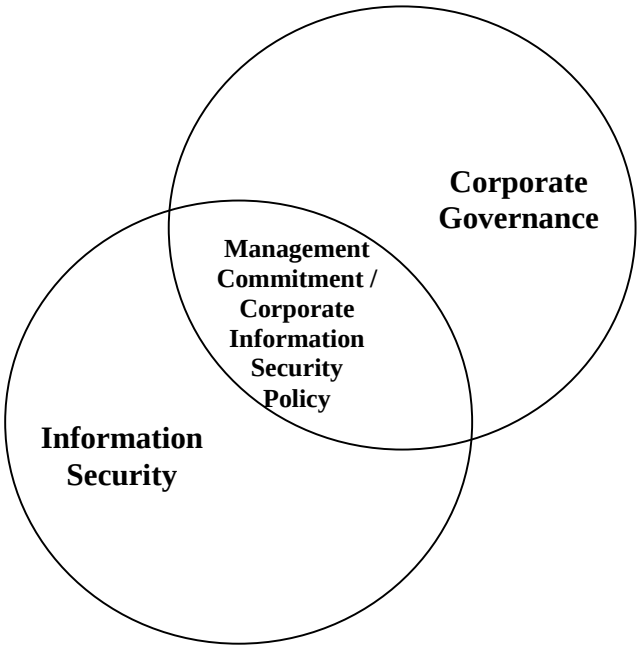

Figure 5.2: The relationship between corporate governance and information security

Figure 5.2 illustrates that senior management has a crucial role to play in the relationship between information security and corporate governance. Senior management should demonstrate its commitment to information security by setting a vision for information security through the Corporate Information Security Policy. This policy must be effectively communicated to employees and management should demonstrate the correct behaviour outlined in the policy.

5.4 Relationship between Corporate Culture and Information Security

As highlighted in Chapter 4, employees are repeatedly singled out as the weakest link in many information security environments. Further, almost all information security solutions rely on the human element to a large extent, but the human factor of information security is often left unaddressed. Employees are often unaware of their responsibilities towards the protection of information assets and, as such, a security vulnerability is created. However, employees must not only be aware of the need to protect information assets, but they must be able to fully comprehend their role in

information security. Employees who do not fully understand their roles are often indifferent to information security and may neglect their security responsibilities as they do not realise the importance thereof.

The corporate culture of an organisation, as described in Chapter 2, is largely responsible for the actions and behaviour of employees. Further, as it is the actions and behaviour of employees that are often the weakest link in information security, it follows that information security should become part of the way employees conduct their daily activities. As pointed out in Chapter 3, an organisation's corporate policies largely influence the behaviour of employees. As it is the incorrect behaviour and actions of employees that are often an issue in protecting information assets, a Corporate Information Security Policy should be developed to influence the behaviour of employees.

Therefore, in order to be truly effective, information security must become part of the corporate culture of an organisation. Diligent, and properly educated, employees can then become one of the strongest links in an information security environment. The resultant relationship that should exist between corporate culture and information security is represented in Figure 5.3.

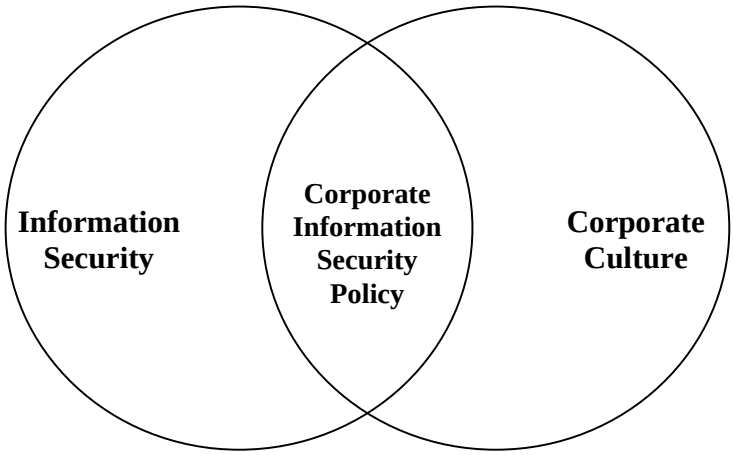

Figure 5.3: The relationship between information security and corporate culture

Figure 5.3 illustrates that in order to build a successful and effective relationship between information security and corporate culture, a Corporate Information Security Policy must be created to serve as the foundation. The Corporate Information Security Policy, and its resulting procedures, should be used to stipulate the actions and behaviour required of employees to successfully protect information assets.

5.5 Relationship between Corporate Culture, Corporate Governance and Information Security

In Chapters 2, 3 and 4 the three fields of corporate culture, corporate governance and information security have been studied. The previous sections of this chapter, explored the relationships between corporate governance and information security, corporate governance and corporate culture, and information security and corporate culture. All of these relationships were represented through figures in previous sections. These figures can be combined into one integrated figure that represents all relationships between the three fields, as detailed in this chapter. This combination is represented by Figure 5.4.

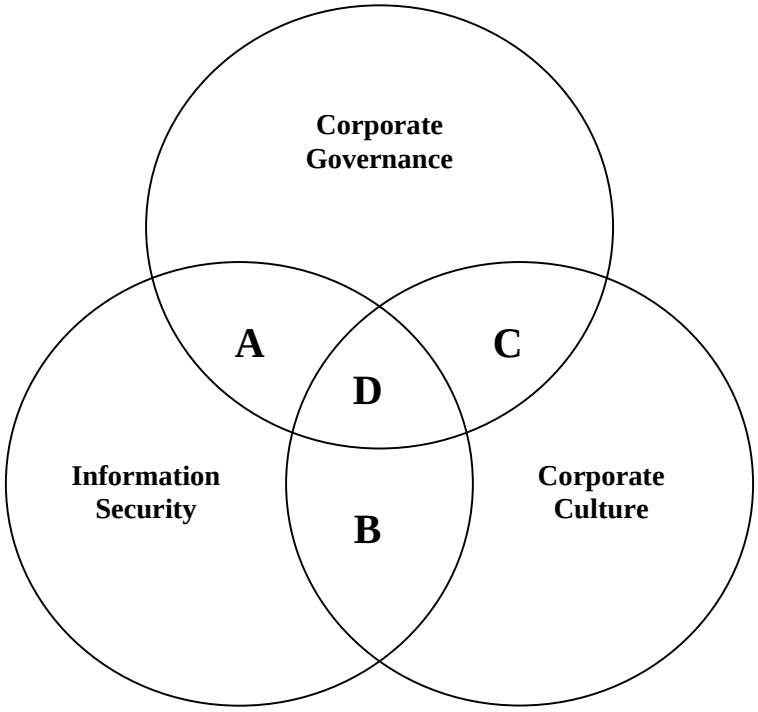

Figure 5.4: The relationships between corporate culture, corporate governance and information security

The relationship that should exist between information security and corporate governance, represented by ‘A’ in Figure 5.4, is best described by the following quote from Michael Cangemi, President of the Etienne Aigner Group Inc. He states, “The information possessed by an organisation is among its most valuable assets and is critical to its success. The Board of Directors, which is ultimately accountable for the organisation's success, is therefore responsible for the protection of its information. The protection of this information can be achieved only through effective management and assured only through effective board oversight” (March 2000, online). This highlights that there should be a very strong relationship between the fields of information security and corporate governance.

As explained in Chapter 4, information security is often seen as an overhead, and not as an investment. The senior management of an organisation tends to view information security as a technical problem that the Information Technology department should be concerned with. However, the information that resides on an organisation’s systems is owned by the organisation as a whole, not the IT manager. Therefore, it is the senior management of organisations that needs to direct the approach to protecting the information.

Senior management must provide clear directives as to exactly what it expects from its employees as far as information security is concerned. Employees require guidelines and direction for information security practices to shape their behaviour and actions. The Corporate Information Security Policy can address both these issues. Thus, one of the best ways to develop the relationship between information security and corporate governance is for senior management to implement and sustain information security practices through the Corporate Information Security Policy.

The relationship, represented by ‘B’ in Figure 5.4, represents the relationship between information security and corporate culture. When investigating information security, it is often seen that the procedures employees use in their daily work and their behaviour

represents the weakest link in information security. In addition, it has been pointed out that the corporate culture of an organisation, to a large extent, determines the behaviour and actions of employees. Therefore, the corporate culture in an organisation should be used to influence the behaviour of the employees towards information security in a positive way. Understanding the corporate culture in terms of information security is crucial, and assessing employees' awareness and commitment determines the best method for the implementation and distribution of the Corporate Information Security Policy.

The Corporate Information Security Policy, and resulting procedures, should outline the behaviour expected from employees with regard to protecting information. Employees must adhere to this acceptable behaviour, which should then begin shaping the corporate culture into one that is more security conscious. A Corporate Information Security Policy should assist in cultivating a corporate culture in which the actions and behaviour of employees are in line with the policy. Therefore, as information security is highly dependent on the behaviour of the users of information, the behaviour should preferably be instilled through corporate culture to ensure that acceptable behaviour becomes the *de facto* behaviour of the employees.

The relationship between corporate governance and corporate culture is represented by 'C' in Figure 5.4. This relationship should be one where senior management creates general management policies using effective corporate governance strategies. These policies should play a primary role in shaping the culture in the organisation by specifying the acceptable and unacceptable behaviour for the employees. These guidelines are crucial in cultivating a beneficial corporate culture for an organisation. However, the culture in an organisation is not determined solely by what management stipulates in the policies, but rather by the example set by management.

Therefore, the behaviour senior management accepts in the organisation should be the behaviour reflected in its corporate policies. The policies created by senior management

should influence and, ultimately, alter the behaviour of the employees in an organisation and should, therefore, start to change the corporate culture in that organisation.

The relationship represented by 'D' in Figure 5.4 represents the incorporation of all three fields of corporate governance, information security and corporate culture. Corporate culture, to a large extent, determines the actions and behaviour of the employees of an organisation. As seen in Chapter 3, the power to change the corporate culture of an organisation resides, to a large extent, with senior management. Therefore, senior management should be able to influence the behaviour of the employees in the organisation into behaviour that will benefit the organisation. As it is the behaviour of employees that is often the weakest link in information security practices, senior management should be able to influence the behaviour of employees into behaviour that will promote proper information security practices. Ideally, to protect information, the *de facto* behaviour of employees should reflect the desire to protect information. In other words, the *shared tacit assumptions* level of culture, which influences the *artifacts* level of culture, should be aligned with the *espoused values* level of corporate culture. If the alignment of the Three Levels of Corporate Culture has been achieved, where the *espoused values* of senior management are reflected in both the *shared tacit assumptions* of employees, and their resultant behaviour at the *artifacts* level, then a *Goal Consensus Environment* has been achieved. The three possible organisational environments, as discussed in Chapter 3, and their relation to the Three Levels of Corporate Culture will be discussed in more detail in the next section.

As discussed previously, to be successful, information security needs to become part of the way the employees conduct their daily tasks, from senior management, right throughout the entire organisation. Therefore, information security should become an intricate part of the corporate culture of the organisation, as it is the culture that determines how employees conduct their daily tasks. This relationship should represent the situation whereby senior management's vision for the protection of information in the organisation is conveyed through the Corporate Information Security Policy. This policy should be drafted, advocated and implemented in such a way that it positively influences

the corporate culture with regard to information security. The related procedures of the policy must outline the behaviour that employees should adhere to in protecting information assets. Further, as information security is highly dependent on the correct behaviour of users, the corporate culture should contribute towards changing the *de facto* behaviour of employees to ensure this behaviour is indeed what senior management envisaged as acceptable behaviour.

The relationship between corporate culture, corporate governance and information security, represented by 'D' in Figure 5.4, can be encompassed by the term 'Corporate Information Security Obedience'. In assessing the acceptability of the term 'Corporate Information Security Obedience', several people expressed concern over the negative implications of the term 'obedience'. The view is that when using the term 'obedience', a 'master/slave' relationship exists, where employees would be forced to submit to the authority of senior management. This, however, is not the case, as is detailed in the following paragraphs.

Obedience is defined as "compliance with that which is required by authority" (Dictionary.com, 2003, online). The authority in this case is the senior management of the organisation, striving towards effective corporate governance. Senior management should create a Corporate Information Security Policy to outline exactly what employees should comply with. Another definition is, "words or actions denoting submission to authority" (Dictionary.com, 2003, online). These words or actions translate into the practices and behaviour of employees, which senior management should have deemed acceptable or unacceptable. As detailed previously, the practices and behaviour of employees are, to a large extent, determined by the corporate culture in an organisation.

Therefore, by using the term 'Corporate Information Security Obedience', it binds together all three fields of corporate culture, corporate governance and information security. The term does this by stating that the actions of the employees must comply with that which is required by senior management in terms of information security. 'Corporate Information Security Obedience' is not something that should be forced on

the employees of an organisation, but should rather become part of the overall corporate culture. Therefore, 'Corporate Information Security Obedience' is defined, for the purpose of this thesis, as "*de facto* user behaviour complying with the vision of senior management as defined in the Corporate Information Security Policy".

It must be highlighted, however, that even though Corporate Information Security Obedience should become part of the way of life in an organisation, it is likely that not all employees will conform. As in society, there will always be employees who 'operate outside the rules'. As such, consequences should exist for failure to comply with information security best practices. However, the majority of employees would adhere to the correct behaviour as it is part of the corporate culture and not because of consequences or rewards.

As Corporate Information Security Obedience evolves in an organisation, the organisational environment, as detailed in Chapter 3, is prone to evolve as well. An organisation that begins as a *Coercive* or *Utilitarian Environment* should evolve into one that is focused on *Goal Consensus* in order to become Information Security Obedient. The next section will explore the organisational environments in relation to the Three Levels of Corporate Culture.

5.6 Organisational Environments and the Three Levels of Corporate Culture

The Three Levels of Corporate Culture, as seen in Chapter 2, range from explicit actions and behaviour at the *artifacts* level of culture to the invisible beliefs and values found at the *shared tacit assumptions* level. It is often found that the *espoused values* and *shared tacit assumptions* levels of corporate culture are not aligned with one another. Thus, the vision of senior management for its organisation is not being realised. As described in Chapter 3, generally one of possibly three key environments could exist in an organisation. In the *Coercive Environment* employees feel isolated and seek to leave the environment if possible. Employees in this environment conduct their daily activities because it is mandatory, rather than because they agree with or understand the wishes of

senior management. The *Utilitarian Environment* is one where employees conduct their daily activities mainly because of an incentive system in the organisation. Employees do not necessarily agree with or understand the wishes of senior management, but adhere to the correct behaviour because of the rewards they will receive. In the *Goal Consensus Environment* employees identify with and feel a sense of loyalty towards the organisation. Employees share the same beliefs and values as senior management and they fully understand the role they should play in the success of the organisation. In the *Goal Consensus Environment* senior management and employees are striving towards the same goals. It does not mean that rewards and consequences do not exist in this environment, but that they are not the driving factor in adhering to correct behaviour.

This section will investigate the possible effect that an organisational environment could have on the corporate culture of an organisation. The three organisational environments will, therefore, be examined in relation to the Three Levels of Corporate Culture.

Figure 5.5 illustrates the *Coercive* and *Utilitarian Environments* mapped onto the Three Levels of Corporate Culture. It shows that, in the *Coercive* and *Utilitarian Environments*, the *artifacts* level of both management and employees are in concurrence with one another. In the *Coercive Environment* this indicates that there is stringent management control and employees adhere to the behaviour specified by management, or else harsh corrective action will be taken against them. In the *Utilitarian Environment* this concurrence indicates that employees will do as management wishes in return for a reward. However, as indicated in the Figure 5.5, the *shared tacit assumptions* level in both environments is not aligned at all – the beliefs and values of management and employees are not the same. Without either strict management or incentives, the correct behaviour of employees would fade.

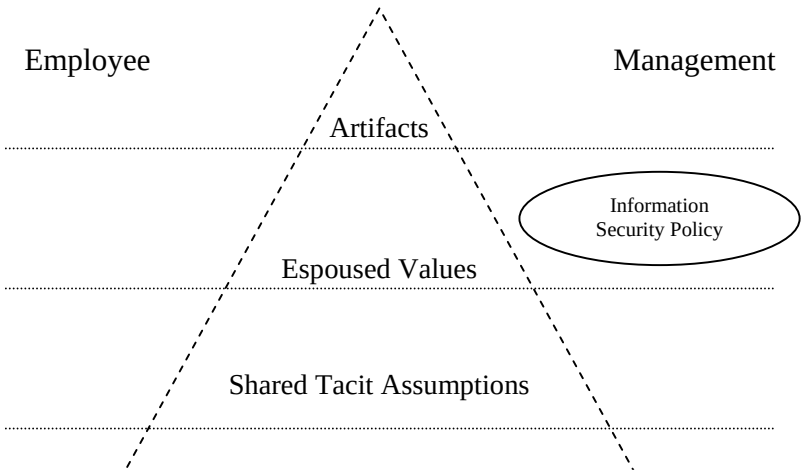

Figure 5.5: The coercive and utilitarian environments and the three levels of corporate culture

From an information security point of view, in Figure 5.5 the Corporate Information Security Policy can be positioned at the *espoused values* level of the Three Levels of Corporate Culture and it is situated on the Management side. This indicates that the contents of the policy reflect senior management's vision for information security and the policy is in agreement with what management wishes. However, the Corporate Information Security Policy is clearly an autocratic management policy, and not at all in line with the beliefs and values of the employees.

It is vital that employees are in agreement with their work policies, as it is indicated that productivity and performance in an organisation could increase by 30 percent to 40 percent if employees are satisfied with the corporate policies (Schafer, 2003, online). One of the policies that employees should be in agreement with is the Corporate Information Security Policy. If the Corporate Information Security Policy is not supported, evaluated and fully understood by management and employees, the policy is in danger of remaining a 'piece of paper'. The benefit to adhering to the Corporate Information Security Policy should also be highlighted for employees. If the environment in which employees work is changing and employees do not keep pace with the changes around them, they may find themselves on the 'endangered species' list (Charlton, 2000, p 22).

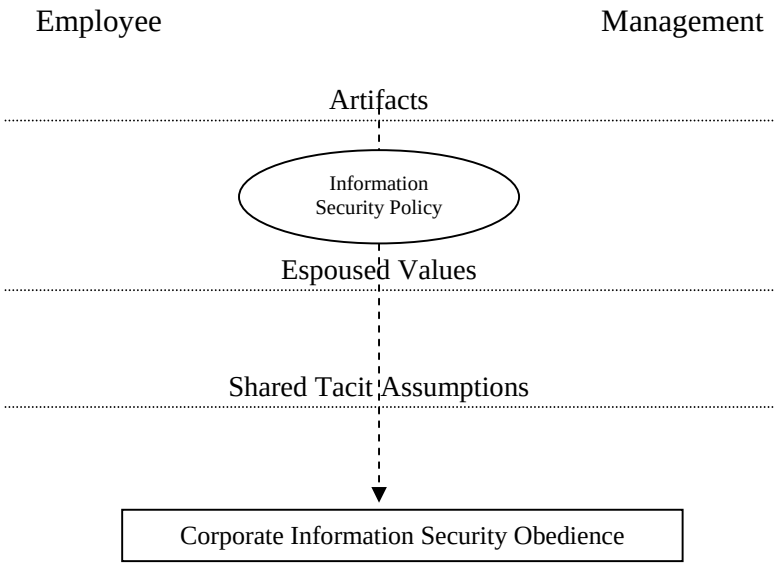

Figure 5.6: The goal consensus environment and the three levels of corporate culture

Figure 5.6 illustrates that in the *Goal Consensus Environment*, all three levels of corporate culture are aligned with one another. This is an ideal corporate culture, in terms of information security, as the information security vision expressed through the Corporate Information Security Policy at the *espoused values* level by senior management is supported by the actions and behaviour of employees at the *artifacts* level. Further, as the *artifacts* level of corporate culture is determined by the *shared tacit assumptions* level of corporate culture, this would indicate that the *espoused values* and *shared tacit assumptions* levels are aligned. In Figure 5.6, the Corporate Information Security Policy is found at the intersection of management and employees. This indicates that the beliefs and values of the employees are in agreement with senior management's vision for information security. A situation of Corporate Information Security Obedience, therefore, can be observed in an organisation, as all three levels of corporate culture are aligned (Thomson & von Solms, 2005, p 74).

5.7 Conclusion

For information security practices and procedures to be truly effective in an organisation, a situation of Corporate Information Security Obedience should evolve in an organisation

and describe the relationship that exists between the three fields of corporate culture, corporate governance and information security.

Through this relationship, senior management is both accountable and responsible for the information assets in its organisation. As such, a Corporate Information Security Policy should be developed to outline the vision that senior management has for information security in its organisation. As corporate policies, and the related procedures, influence and dictate the actions and behaviour of employees, the Corporate Information Security Policy should influence the actions and behaviour, and underlying beliefs and values, of employees in the protection of information assets. As employees' beliefs towards the importance of information change and they begin to understand their role in protecting information assets, so too will the corporate culture of an organisation change into one that is more information security conscious.

As beliefs and values begin to change, employees will need to create new knowledge to accommodate the new beliefs. The following chapter will detail how knowledge is created in an organisation and organisational learning processes. The Modes of Knowledge Creation, as suggested by Nonaka, and the interaction between tacit and explicit knowledge will be detailed. Further, the relationship between the Modes of Knowledge Creation and the Three Levels of Corporate Culture, as discussed in Chapter 2, will be examined.

CHAPTER 6

KNOWLEDGE CREATION

6.1 Introduction

"Knowledge is power", as stated by Francis Bacon, while Confucius stated that "real knowledge is to know the extent of one's ignorance" (The Quotations Page, 2006, online). There is constant pressure on any given corporate culture to change and grow, and, as such, organisations create and propagate knowledge on a daily basis. The rapid creation and circulation of knowledge should be a key concern of senior management, as knowledge can be a source of competitive advantage for organisations (von Krogh, 1998, p 133).

As new knowledge is propagated throughout an organisation, the culture must adapt to incorporate it. In addition, a key factor in the creation of knowledge is to distinguish the areas in which an organisation is ignorant and take measures to surmount this lack of knowledge (Schein, 1990, p 116; Argyris & Schon, 1978, p 9).

In order to survive, organisations must change and adapt to the often unpredictable conditions, both internal and external to it. Essential to change in an organisation is the development of both tacit and explicit knowledge, and the interaction between the two. Explicit knowledge refers to knowledge that is transmittable in formal, organised language. Explicit knowledge can be likened to the *espoused values* level of corporate culture. Tacit knowledge, on the other hand, has a personal quality, which makes it difficult to formalise and communicate. Tacit knowledge drives action, commitment, and involvement in an organisation. Tacit knowledge can be likened to the *shared tacit assumptions* level of corporate culture (Nonaka, 1994, p 16).

This chapter will investigate both tacit and explicit knowledge in more detail. Organisational learning, and the concepts of single- and double-loop learning, as proposed by Argyris and Schon (1978), will be discussed. Further, the theory of knowledge creation within organisations will be detailed. The Modes of Knowledge Creation, as proposed by Nonaka, and the concepts of *socialization, externalization, combination* and *internalization* will be explored. The chapter will conclude by examining the Modes of Knowledge Creation in relation to the Three Levels of Corporate Culture.

6.2 Organisational Learning

Organisations are not merely collections of individuals, but there is no organisation without such collections. Likewise, organisational learning is not simply individual learning, yet organisations learn only through the experience and actions of individuals (Argyris & Schon, 1978, p 9). Organisational learning entails both the detection and correction of error in an organisation. The following section will detail concepts of organisational learning, including single- and double-loop learning.

There are two important concepts relevant to organisational learning that must be explored. These are *theory-in-use* and *theory of action*. Organisational *theory-in-use* is derived from the observation of organisational behaviour, or, in other words, organisational decisions and actions. The decisions and actions carried out by individuals are organisational if they are governed by the organisation's rules for decisions and actions (Argyris & Schon, 1978, p 15). The *theory-in-use* of an organisation is often tacit and correlates with the *shared tacit assumptions* level of corporate culture. Alternatively, *theory of action* is reflected in formal corporate documents, such as organisation policies and charts (Argyris & Schon, 1978, p 15). *Theory of action* is often referred to as the espoused theory of an organisation and correlates to the *espoused values* level of corporate culture.

Every employee in an organisation constructs his or her own depiction, or image, of the *theory-in-use* in an organisation. It is this image that employees use to understand themselves in the context of the organisation, and these images are private to an employee. However, the continuity and stability of an organisation cannot rely on the employees' private images. Essential to organisational continuity is the public representation of an organisation's *theory-in-use*, which is referred to as organisational maps. These are the shared descriptions of an organisation which employees jointly construct and use to guide them. Organisational maps have a dual function – they describe actual patterns of activity, and they are guides for future action. Therefore, organisational *theory-in-use*, which is largely tacit, is 'encoded' in private images and public maps. The public maps of employees in an organisation are often in conflict with the *theory of action*. This is essentially the same as the conflicting *espoused values* and *shared tacit assumptions* levels of the Three Levels of Corporate Culture, as discussed in Chapter 2.

The private images and public maps of employees are continuously modified to adjust to changing conditions in their environment, and this brings about changes in organisational *theory-in-use*. The changes in organisational *theory-in-use* are referred to as organisational learning (Argyris & Schon, 1978, p 17).

The two primary methods for organisational learning are single- and double-loop learning. Single-loop learning occurs when the detection and corrections of errors allows an organisation to continue with its current policies and procedures. Double-loop learning occurs when the detection and correction of errors requires the modification of an organisation's policies and procedures. These two learning methods will be explored in greater detail in the following sub-sections.

6.2.1 Single-loop Learning

With single-loop learning, employees respond to changes in the internal and external environments of the organisation by detecting errors or faults in these environments. These errors can then be corrected to maintain the

central features of the organisational *theory-in-use*. Single-loop learning is sufficient where error correction can proceed by changing organisational strategies within a constant framework of norms or assumptions. Single-loop learning is concerned mainly with effectiveness. In other words, how best to achieve existing goals and objectives as specified by existing organisational norms (Argyris & Schon, 1978, pp 18, 21). Therefore, single-loop learning ensures the existing goals and objectives of an organisation remain intact, whereas the approach to achieving these goals may need to be modified through the single-loop learning process.

6.2.2 Double-loop learning

There may be cases, however, where error correction requires a learning cycle in the organisation in which the organisational assumptions themselves must be changed. In such cases, a double feedback loop connects the detection of error not only to strategies, but to the underlying norms and assumptions in an organisation. The organisation may require a restructuring of its norms and assumptions, as well as a restructuring of organisational strategies. These new strategies and associated assumptions should be embedded into the images and maps which encode the tacit organisational *theory-in-use.* Double-loop learning will occur when differences between the actual and desired states are corrected by first examining and altering the governing variables and then taking action. These governing variables are not the values people espouse. They are the underlying beliefs that can be inferred, by observing the actions of individuals, to drive and guide their actions (Argos Press, 1999, online; Argyris & Schon, 1978, pp 21-22).

Double-loop learning, however, should not be a method that needs to be 'put into practice' in an organisation. It should be part of the daily activities of an organisation. Organisations are continuously creating new knowledge by reconstructing existing

perspectives and assumptions on a day-to-day basis. Therefore, the double-loop learning ability should be 'built into' the knowledge creation model of an organisation (Nonaka, 1994, p 19). The following section will discuss knowledge and the process of organisational knowledge creation.

6.3 Theory of Knowledge and Knowledge Creation

To understand knowledge creation, it is necessary to have a comprehensive understanding of the term 'knowledge'. Knowledge is considered a personal 'belief' and, equally important, is the 'justification' of that belief. Information and knowledge are often used interchangeably, but there is a clear distinction between information and knowledge. Information is a flow of messages, while knowledge is created by this flow of information and manipulated by the commitment and beliefs of its holder (Nonaka, 1994, p 15).

There are two leading views on knowledge – the 'cognitivist' and 'constructionist' perspectives. The cognitivist perspective sees cognition, or conscience, as a 'machine' for information processing and logical reasoning. Two cognitive systems should reach the same conclusions or representations of an event or object. 'Learning', from the cognitivist perspective, implies developing increasingly comprehensive representations of objects and events. In addition, cognitivist knowledge is seen as explicit, capable of being encoded and stored, and easy to transmit to others (von Krogh, 1998, p 134).

The constructionist perspective sees cognition as an act of construction or creation, and not representation. Knowledge resides in a person's body and is closely tied to a person's senses and prior experiences. Therefore, individuals see the environment from their own unique viewpoint. However, in an organisation, knowledge creation is a social process where more than one employee is involved. From the constructionist perspective, some knowledge is explicit, but some is tacit, not easily expressed and is complex to share with others (von Krogh, 1998, p 134).

As mentioned previously, at a fundamental level, knowledge is created by employees and an organisation cannot create knowledge without employees. Employees are constantly committed to recreating their environment in accordance with their own perspectives, and commitment underlies human knowledge creating activities. Therefore, commitment is a significant component for encouraging the creation of new knowledge within an organisation (Nonaka, 1994, p 17).

There are three factors, *inter alia*, that encourage individual commitment in an organisation and, ultimately, will lead to knowledge creation. These three factors are 'intention', 'autonomy' and a certain level of environmental 'fluctuation'. The following subsections will discuss these three factors.

6.3.1 Intention

Intention is concerned with how individuals shape their approach to the world and try to make sense of their environment. Intention involves the process of obtaining information for better adaptation to their environment. The meaning of information differs according to what an individual aims to do with the information. Therefore, without intention, it would be impossible to judge the value of the information or knowledge created (Nonaka, 1994, p 17).

6.3.2 Autonomy

Individuals within an organisation may have different intentions as every individual has his or her own personality. By allowing employees to act autonomously, an organisation is more likely to maintain greater flexibility in obtaining and interpreting information. Individual autonomy increases the possibility that individuals will motivate themselves to create new knowledge (Nonaka, 1994, p 18).

6.3.3 Fluctuation

> While intention is internal to the individual, knowledge creation at the individual level involves constant interaction with the external world. The interaction with the external environment often leads to 'breakdowns' in an individual's perception. A breakdown refers to the disruption of an individual's comfortable, existing 'state-of-being'. When breakdowns occur, individuals question the value of habits and beliefs, which might lead to a realignment of commitments. When employees face a breakdown of their perceptions, they have an opportunity to reassess their thinking and attitudes (Nonaka, 1994, p 18).

Effective knowledge creation places particular demands on the way employees relate to each other in an organisation. For example, untrustworthy behaviour, constant competition and apathetic, lacklustre attitudes, endanger effective sharing of tacit knowledge. On the other hand, constructive and helpful relations speed up the communication process and enable employees to share their personal knowledge. Senior management plays a critical role in revealing tacit knowledge held by employees and provide the environment for a 'spiral of knowledge' creation through the Modes of *socialization*, *combination*, *externalization*, and *internalization*. These four Modes of Knowledge Creation will be discussed in the subsequent section (von Krogh, 1998, p 136; Nonaka, 1994, p 34).

6.4 Modes of Knowledge Creation

As discussed previously, tacit, or implicit, knowledge is subjective and experience based. This knowledge is difficult to formalise and communicate and includes beliefs, attitudes and intuition, as well as technical skills. Knowledge in the tacit form is actionable, or can be used, by the owner. Tacit knowledge is found at the *shared tacit assumptions* level of corporate culture and influences the *artifacts* level. Explicit, or overt, knowledge, on the other hand, is objective and rational knowledge that can be communicated in words and

sentences and includes theoretical approaches and problem solving. Explicit knowledge is found at the *espoused values* level of corporate culture (Nonaka, 1994, p 16).

There are four different processes of interaction, suggested by Nonaka, between tacit knowledge and explicit knowledge. These four processes are represented in the Modes of Knowledge Creation, the purpose of which is to identify existing knowledge and 'convert' it to new knowledge. These processes are classified as *socialization*, *externalization*, *combination* and *internalization* (Nonaka, 1994, p 18).

6.4.1 Socialization

The key initiator in the process of organisational knowledge creation is the individual. An individual's knowledge must be broadened and amplified to be translated into organisational knowledge. This process should begin with *socialization*. *Socialization* is the process whereby one person's tacit knowledge is transferred to tacit knowledge in another person through interaction between these individuals. *Socialization* involves capturing knowledge through direct interaction with individuals both inside and outside an organisation, and employees can acquire tacit knowledge without language. For example, apprentices work with their tutors and learn skills, not through language, but by observation, imitation and practice.

Socialization depends on having shared experience, and results in acquired skills and common mental models. The key to acquiring tacit knowledge is experience. Without some form of shared experience, it is extremely difficult for people to share each others' thinking processes. Shared experience facilitates the creation of 'common perspectives' which can be shared by individuals as a part of their respective bodies of tacit knowledge. Individuals bring their own perspectives to an organisation, and this tacit knowledge is converted through co-experience to form a common base for understanding (Nonaka, 1994, pp 19, 21, 24).

6.4.2 Externalization

Once a common, implicit perspective has been formed through a shared experience, the employees need to articulate the perspective. *Externalization* is the process whereby tacit knowledge is made explicit. One way to do this is through 'articulation' of tacit knowledge by expressing beliefs and values in words, metaphors or analogies. A second way is through 'eliciting and translating' the tacit knowledge of others into an understandable form or explicit knowledge. Dialogue and discussion are important means for both methods. During such communication, people share beliefs and can learn how to better articulate their thinking. *Externalization* is a process among individuals within a group (Nonaka, 1994, pp 19, 25).

6.4.3 Internalization

Internalization is the process of understanding and absorbing explicit knowledge into the tacit knowledge held by an individual. *Internalization* is largely practical as explicit knowledge is transferred to tacit through the actual doing of a task or skill or through simulations. The *internalization* process transfers organisational explicit knowledge to the individual employee. This process is often referred to as crystallization. In other words, the explicit knowledge created must be crystallized into a form that can be internalized (Nonaka, 1994, p 20).

6.4.4 Combination

Once knowledge has become explicit, it can be transferred to explicit knowledge of many through a process Nonaka calls *combination*. This involves the use of social processes to combine different bodies of explicit knowledge held by individuals. Explicit knowledge can be exchanged, combined and conveyed in, for example, documents and email, as well as through meetings and training. The collection and dissemination of

relevant information becomes very significant in this process. *Combination* should utilise the double-loop learning process of organisational learning, as double-loop learning requires the modification of an organisation's strategies or policies. These policies are *espoused values* or explicit knowledge that must be transferred, through *combination*, to many. *Combination* allows knowledge transfer among groups across organisations (Nonaka, 1994, pp 19-20).

The four processes of interaction between tacit and explicit knowledge are represented in Figure 6.1. It shows that the *socialization* process transfers tacit knowledge to tacit knowledge. The *externalization* process transfers tacit knowledge to explicit knowledge. The *internalization* process transfers explicit knowledge to tacit knowledge. And the *combination* process transfers explicit knowledge to explicit knowledge.

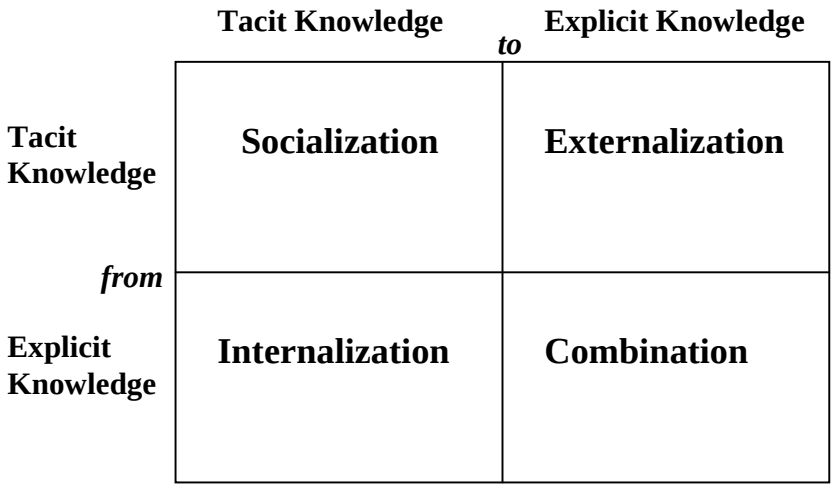

Figure 6.1: Nonaka's modes of knowledge creation
Source: Nonaka, 1994, p 19

The interaction of the four Modes of Knowledge Creation is encouraged by what Nonaka terms 'enablers' within an organisation. These enablers will trigger the knowledge creation and conversion process within an organisation. Nonaka identifies five enablers

for knowledge creation within an organisation: *vision*, *strategy*, *structure*, *system* and *staff* (1997, online).

The first enabler, a knowledge *vision*, is a working premise for knowledge. For example, Walt Disney's vision is "continuous progress via creativity, dreams and imagination. No cynicism allowed". This vision stimulates ingenuity and knowledge creation. The second enabler, *strategy*, conceptualises what knowledge to develop. Knowledge *strategy* identifies core knowledge and results in efficient new product development. Knowledge *strategy* focuses on disseminating knowledge.

The third enabler, *system*, is described as networking communities of knowledge, which include competitors, customers and related industries. The fourth enabler is *structure*. According to Nonaka (1997), there are two forms of organisations that management must strike a balance between – fractal organisation and bureaucracy. Fractal organisation is largely self-organising, flexible and extremely adept at *socialization* and *externalization*. Bureaucracy has a hierarchy, division of labour and *combination* and *internalization* flourish. The final enabler of knowledge creation in an organisation is *staff*. Nonaka stresses the importance of middle management in the knowledge creation process. The role of middle managers is to initiate, support, and complete the knowledge spiral. They play the critical role between the vision from the top, and what the reality is.

While each of the four Modes of Knowledge Creation can create new knowledge independently, the success of the model of organisational knowledge creation relies on the dynamic interaction between the different Modes of Knowledge Creation. Organisational learning, discussed in section 6.2, can be compared to *internalization* and *combination*, which are just two of the four Modes of Knowledge Creation. Organisational learning has limited, static implications, whereas organisational knowledge creation is a more dynamic concept. Organisational learning is one aspect of the knowledge creation process within an organisation. Organisational knowledge creation focuses on creating both tacit and explicit knowledge and, more significantly, on the exchange between these types of knowledge through *internalization* and

externalization. Therefore, while tacit knowledge held by individuals lies at the heart of the knowledge creation process, realizing the practical benefits of that knowledge relies on its *externalization* and amplification through dynamic interactions between all four Modes of Knowledge Creation (Nonaka, 1994, pp 20, 34).

The interactions between tacit and explicit knowledge will have a tendency to become more frequent and occur faster as more employees in and around the organisation become involved. The process of organisational knowledge creation is an infinite, circular process. Accordingly, organisational knowledge creation can be viewed as an upward spiral process, starting at the individual level, moving up to the collective or group level, and then to the organizational level (Nonaka, 1994, pp 20, 27). It must be noted that this is a spiral process, not a cycle, because as learning is achieved, understanding moves to deeper and deeper levels.

6.5 Relationship between Modes of Knowledge Creation and the Three Levels of Corporate Culture

As discussed in section 6.4, the Modes of Knowledge Creation detail how knowledge can be created and converted in organisations through the interaction of tacit and explicit knowledge. As seen in Chapter 2, the Three Levels of Corporate Culture also entail the interaction of tacit and explicit knowledge. This section will explore a comparison of the Modes of Knowledge Creation and the Three Levels of Corporate Culture.

The Three Levels of Corporate Culture are the *artifacts*, *espoused values* and *shared tacit assumptions* levels. The *shared tacit assumptions* level consists of the collective tacit knowledge of all employees in an organisation. The *espoused values* level consists of the values that an organisation states it is supporting. These values are articulated in organisational policies and are, therefore, explicit knowledge. The *artifacts* level consists of observed, visible behaviour which has its roots in the *shared tacit assumptions* of employees.

The first of the Modes of Knowledge Creation is the process of *socialization. Socialization* transfers tacit knowledge from one individual to another. As this process only involves tacit knowledge, *socialization* impacts employees at the *shared tacit assumptions* level of corporate culture. In terms of corporate culture, *socialization*, as described in Chapter 2, is necessary to perpetuate a corporate culture. *Socialization* in this context is not only the transfer of implicit knowledge among individuals, but it is the development of the collective *shared tacit assumptions* level of corporate culture.

The second Mode of Knowledge Creation, *combination*, transfers explicit knowledge to the explicit knowledge of many. The explicit knowledge or *espoused values* of an organisation are conveyed to employees through management policies. Initially these values will become the *espoused values* of employees before becoming tacit knowledge. Therefore, the *combination* process only involves explicit knowledge as it only impacts the *espoused values* level of corporate culture. The third Mode of Knowledge Creation, *externalization*, transfers tacit knowledge to explicit knowledge. As both tacit and explicit knowledge are utilised, it follows that the *externalization* process involves both the *shared tacit assumptions* and *espoused values* levels of corporate culture. When *externalization* takes place, tacit knowledge is translated into *espoused values*. The final Mode of *internalization* transfers explicit knowledge to tacit knowledge. Once again, both the *shared tacit assumptions* level and the *espoused values* level are involved in the process. When *internalization* takes place, explicit knowledge is translated into *shared tacit assumptions* level of corporate culture. The relationship between the Three Levels of Corporate Culture and the Modes of Knowledge Creation is depicted in Figure 6.2.

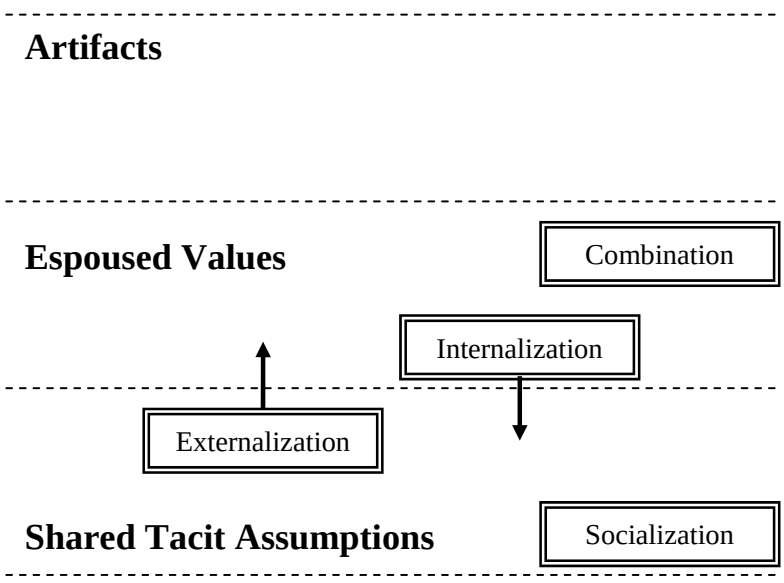

Figure 6.2: Three levels of corporate culture and modes of knowledge creation

As can be seen from Figure 6.2, *socialization* is solely concerned with the tacit knowledge at the *shared tacit assumptions* level of corporate culture. *Combination*, on the other hand, is concerned purely with the *espoused values* of an organisation. Both *externalization* and *internalization* rely on the interaction between the *espoused values* level and the *shared tacit assumptions* level. All of the Modes of Knowledge Creation are vital in the development of knowledge within an organisation.

6.6 Conclusion

Knowledge creation is an essential part of any organisation and, as such, all organisations must adapt to changing conditions both in their internal and external environments. Without the creation and effective use of new knowledge, organisations would, most likely, lose their competitive edge. As new knowledge is disseminated throughout an organisation, the corporate culture must change and adapt to this freshly acquired knowledge.

The four Modes of Knowledge Creation proposed by Nonaka are the processes used by organisations to create fresh knowledge. The ultimate goal for knowledge creation, in the context of corporate culture, would be for the four Modes of *socialization*, *combination*,

externalization and *internalization* to result in all employees sharing the same *espoused values*, or explicit knowledge, which aligns with the tacit knowledge at the *shared tacit assumptions* level. It must be emphasised that knowledge creation is a spiral process that leads to a deeper understanding of the knowledge that has been created or shared.

As employees create new knowledge and learn new skills related to information security they will progress through the four stages of the Information Security Competence Maturity Model. The next chapter will explore this Model, as well as the Information Security *Awareness*, *Training* and *Education* Programs needed to move employees through the four stages.

CHAPTER 7

THE INFORMATION SECURITY COMPETENCE MATURITY MODEL

7.1 Introduction

"An education isn't how much you have committed to memory, or even how much you know. It's being able to differentiate between what you do know and what you don't". This quote from Anatole France underlines a key factor in the learning or education of a new skill or task (The Quotations Page, 2006, online). A person should become conscious of what they do not know, and only then can he or she begin the learning process. In other words, once people become aware of the need for certain skills that they do not possess, the learning process is initiated.

However, in terms of information security, awareness is simply not enough. As discussed in Chapter 4, by only making employees aware of information security practices, and not affording them a deeper comprehension of information security, employees may find ways of evading their information security responsibilities. Employees will take the 'path of least resistance' to getting their jobs done, without appreciating the consequences for information security. When asking employees to do something different and develop new skills and attitudes, the focus should be on the people themselves and their learning experiences – technology should be an adjunct (Charlton, 2000, p 7).

This chapter will begin by detailing Information Security *Awareness*, *Training* and *Education* Programs. The significance of using all three Programs in an organisation to emphasise the importance of information security, and promote understanding, will also be highlighted. The Conscious Competence Learning Matrix, which describes the natural progression of people in learning a new skill, will be explored in detail.

Following this, an Information Security Competence Maturity Model will be proposed. This Model will encompass the learning stages that employees of an organisation should progress through in order to learn information security skills and practices, as well as how employees should move from Stage to Stage leading to Corporate Information Security Obedience.

7.2 Information Security Awareness, Training and Education

As discussed in Chapter 4, the protection of information assets through information security practices is essential for the well-being of an organisation. There is a necessity for a Corporate Information Security Policy, and the associated procedures, to detail the vision for information security and the expected behaviour required to ensure the confidentiality, integrity and availability of information assets. It is the responsibility of senior management to ensure that this policy is effectively communicated to all employees throughout the organisation. As a foundation for this communication, an Information Security *Awareness* Program is required. Many organisations disregard an *Awareness* Program altogether. However, an Information Security *Awareness* Program is an essential requirement to help mitigate security breaches (Mitnick & Simon, 2002, p 286). This section will investigate not only Information Security *Awareness*, but Information Security *Training* and *Education* as well.

Some authorities propose that 40 per cent of an organisation's overall information security budget be targeted to making employees aware of the role they should play in protecting information assets (Mitnick & Simon, 2002, p 246). However, developing and circulating a Corporate Information Security Policy, or directing employees to an intranet page that details security procedures will, alone, not diminish the threats to information assets. An Information Security *Awareness* Program is necessary. The purpose of an Information Security *Awareness* Program should be to focus employees' attention on information security. Through an Information Security *Awareness* Program employees usually play a passive role as they are the recipients of information and knowledge, and

they should learn to recognise threats to information assets. The central goal of any Information Security *Awareness* Program is to influence employees to change their beliefs and attitudes at the *shared tacit assumptions* level (and eventually their actions at the *artifacts* level) by convincing all employees that they are responsible for the protection of information assets (Mitnick & Simon, 2002, p 249; National Institute of Science and Technology Special Publication 800-16, 1998, p 15).

An Information Security *Awareness* Program should be designed bearing in mind that employees will most likely have a fairly short attention span and often 'tune out' the knowledge that is being given to them through a process called acclimation. In other words, if the same stimulus is used repeatedly to convey a concept, employees are prone to ignore the stimulus. Furthermore, it is often found that learning through an *Awareness* Program is immediate, short-term and specific and the learning objectives of an Information Security *Awareness* Program should be recognition and retention. Examples of Information Security *Awareness* components are awareness presentations, videos, posters and inspirational information security slogans (National Institute of Science and Technology Special Publication 800-16, 1998, pp 15, 18).

While *Awareness* relies on reaching a wide range of people, Information Security *Training* is more formal. Information Security *Training* has the goal of building knowledge and the necessary skills for employees to successfully protect information assets. Organisations cannot protect the confidentiality, integrity and availability of information without ensuring that all employees understand their roles and responsibilities and are sufficiently trained to perform them (National Institute of Science and Technology Special Publication 800-16, 1998, p 15).

Through an Information Security *Training* Program employees should gain the knowledge about how to defend against attacks on information assets, for example from social engineers, and employees should develop the appropriate skills necessary for the protection of information assets. Further, while this knowledge is important, it will only be effective if the *Training* focuses greatly on encouraging and motivating employees to

use that knowledge (National Institute of Science and Technology Special Publication 800-16, 1998, p 16; Mitnick & Simon, 2002, p 250).

As a minimum, all employees should receive basic *Training* in information security practices. The National Institute of Science and Technology (NIST) (1998) recommends three levels of *Training*: Beginning, Intermediate and Advanced, with each level linked to the roles and responsibilities of the employees. Therefore, *Training* should be tailored based on job responsibilities and needs (pp 5, 18, 43). Further to this, Information Security *Training* needs to be relevant to the job functions and risks of the employees. *Training* should not be a 'do not do this' program. The learning objectives of an Information Security *Training* Program should be skills to support the Corporate Information Security Policy. *Training* should promote the Corporate Information Security Policy, and procedures, but, in addition, *Training* should be an activity designed to instill a concept of best practice and understanding in employees. The organisation can consider the Program successful if all employees completing the *Training* are entirely convinced and motivated by one fundamental belief: that information security is part of their responsibilities and that they have the skills to fulfill these responsibilities (National Institute of Science and Technology Special Publication 800-16, 1998, p 16; Mitnick & Simon, 2002, p 250).

Once employees have acquired the necessary information security skills through *Training*, they should move on to an Information Security *Education* Program. This *Education* Program should enhance the insight of employees as to why the skills they learnt through the *Training* Program are necessary. The learning objective of an Information Security *Education* Program is a comprehensive understanding of information security practices and procedures.

An Information Security *Education* Program is essential for employees to become fully committed to information security given that, as discussed in Chapter 4, employees will not implement rules that they do not fully understand. The understanding developed in the Information Security *Awareness* and *Training* Programs should be used as a

foundation to establish an even deeper understanding of information security through the Information Security *Education* Program. Once people realise the reasons behind procedures and required behaviour, they will be more inclined to adhere to the correct behaviour than they would have if they were pressured into a firm set of rules (Henry, 2004, p 666). Together with *Education*, and in order for information security practices to become part of the daily routine and activities of employees, *Experience* is necessary for employees to become comfortable with their newly acquired skills. Once employees become experienced in information security procedures and practices these practices should become intrinsic to them (National Institute of Science and Technology Special Publication 800-16, 1998, p 18).

Information Security *Awareness*, *Training*, *Education* and, over time, relevant *Experience*, are essential programs that employees should move through in order to change their beliefs, attitudes and behaviour positively towards protecting information assets. As emphasised by Mitnick "If you don't have trained and alert employees following well-thought-out procedures, it's not a matter of if, but when you will lose valuable information" (2002, p 246).

7.3 Conscious Competence Learning Matrix

The Conscious Competence Learning Matrix details the learning process that people should go through whenever a new skill is learnt. For the purposes of this research, the Conscious Competence Learning Matrix will detail the learning process of employees in an organisation. Whenever a new skill or behaviour is learnt by employees, they move through certain phases or stages in mastering the change; referred to as the Conscious Competence Learning Matrix. The Stages are *Unconscious Incompetence*, *Conscious Incompetence*, *Conscious Competence* and *Unconscious Competence* (Charlton, 2000, p 7; Chapman, 2001, online). This section will detail the progression of employees through these four Stages as they adapt to change.

Stage 1 of the Conscious Competence Learning Matrix is *Unconscious Incompetence*. At this Stage, employees are not aware of the existence or relevance of a skill set. More

importantly, employees are not aware of the necessity for them to master that skill set and often deny the usefulness of the skills. In order for any learning to take place, employees must become conscious of their deficiency in skills, ideally, through the demonstration of the skill set.

Once employees are conscious of the skills needed, they can progress to Stage 2, or *Conscious Incompetence*. However, even though employees are aware of the skills needed, they still do not know how to implement these skills. Preferably at this Stage, employees should have an idea of the extent of their deficiency in the relevant skill and the employee must make a commitment to learning the new skill to progress to Stage 3.

Stage 3 of the Matrix, *Conscious Competence*, is reached when employees can perform the relevant skills without assistance. However, the skills are not yet second-nature to the employees and require concentration to perform the tasks reliably. In due course, as employees practice and become more experienced in these skills, they will progress to Stage 4 of the Matrix.

Unconscious Competence, Stage 4, is the ultimate Stage in the Conscious Competence Learning Matrix. At this Stage, employees have become so comfortable and experienced in the particular skills that the skills enter the subconscious thinking of employees and become second-nature to them. It is very likely that, having reached *Unconscious Competency*, employees may find it difficult to teach others the skills as the skills have become mostly instinctual.

The Conscious Competence Learning Matrix can be clarified using an everyday example. Any person wishing to learn how to drive a motor vehicle will have to progress through the learning stages as described by the Conscious Competence Learning Matrix. In the beginning, the person is unaware of the skills required for driving a motor vehicle (Stage 1). In addition, the person is not aware of the acceptable behaviour required when adhering to the rules of the road. Once the person has studied for and passed the Learner's Driving Licence test, he/she has the theory behind driving a motor vehicle.

The person has progressed to Stage 2 as he/she now knows what skills are required to drive a motor vehicle and the rules of the road. However, the theory of the road is not enough as the person still does not possess the skills required for driving a motor vehicle.

In order to do so, the person should attend driving lessons, or be taught by someone, to learn the skills essential for driving a motor vehicle. Once these skills have been developed, the person is now capable of driving a motor vehicle, but the person still requires a great deal of concentration and driving is by no means habitual (Stage 3). Over time, however, as the person drives regularly, becomes comfortable and develops into an experienced driver, the skills required will, largely, become automatic and the person will no longer require such intense concentration in driving a motor vehicle as in the beginning. The person will have progressed to the final learning stage, Stage 4, in the Conscious Competence Learning Matrix.

7.4 Information Security Competence Maturity Model

Chapter 5 detailed the concept of Corporate Information Security Obedience and why it should be strived for in an organisation. Section 7.2 detailed the requirement for Information Security *Awareness*, *Training* and *Education* Programs necessary in organisations for employees to learn and understand information security practices. Section 7.3 described the generally accepted Conscious Competence Maturity Matrix, detailing the Stages people go through in order to develop a new skill or behaviour. This section will combine the concepts from the three sections into the Information Security Competence Maturity Model.

As detailed in Chapter 4, employees often misguidedly believe that information assets are being taken care of and protected by firewalls and other physical and technical controls. They do not acknowledge or understand the role they should be playing in information security. As a result, when it comes to information security procedures and practices, most employees are incompetent and unskilled. Therefore, these employees are at Stage 1, or *Unconscious Incompetence* Stage, of the Information Security Competence Maturity

Model. At Stage 1, employees are unaware of their responsibilities towards protecting information assets and are ignorant of the skills needed to successfully execute information security practices. Employees at this Stage are oblivious to the need for information security practices in the organisation. Their behaviour could, consequently, be conflicting with what is needed for the protection of information assets without them even realising.

As seen in a previous section, an Information Security *Awareness* Program is necessary to focus the attention of the organisation on information security. An *Awareness* Program should broadcast to all employees, most of whom are at the *Unconscious Incompetence* Stage, the importance of information assets. The basic beliefs of employees towards information should be positively altered and the main aim of the Program should be to ensure employees are fervent in their desire to protect information assets.

Once employees have successfully completed an Information Security *Awareness* Program they should, at least, be aware of their information security responsibilities. The *espoused values* level of corporate culture has been impacted as the contents of the Corporate Information Security Policy, and related procedures, have now been made known to employees. Once employees can acknowledge that they have a role to play in protecting information assets, they move to the *Conscious Incompetence* Stage of the Information Security Competence Maturity Model. At this Stage, employees should understand the importance of information assets to the organisation and how information security benefits the entire organisation. Employees realise what is required of them, but, as yet, do not have the skills necessary to effectively protect information assets and are, therefore, still incompetent.

In order for employees to acquire these skills, it is necessary for them to attend an Information Security *Training* Program. As detailed in a previous section, all employees should receive a basic level of *Training* in information security skills and practices. Further to this basic *Training*, employees should receive additional *Training*, if

necessary, that is customised specifically to their job responsibilities. Through an Information Security *Training* Program, employees should learn how to most effectively protect information assets and recognise potential threats. Through the *Training* Program, the correct information security practices, actions and behaviour of employees, which should be observed at the *artifacts* level of corporate culture, will be shaped. As a result of the *Training* Program, employees should progress to Stage 3 of the Information Security Competence Maturity Model.

Stage 3 of the Model is *Conscious Competence*. At this Stage, employees have gained the crucial skills for information security practices. The employees are fully aware of what is desired from them in terms of information security and can complete any information security tasks assigned to them. However, the completion of these tasks requires a conscious effort on the part of the employees. The information security practices demand a high degree of concentration to be accomplished and they are by no means second-nature to employees. Furthermore, it is not uncommon for employees to be forgetful or negligent about things that seem peripheral to getting their jobs done. Therefore, even though employees know and understand what is expected of them they need to be reminded over and over again, in different ways, about their information security responsibilities (Mitnick & Simon, 2002, p 104). Therefore, the correct information security practices and procedures are in place in the organisation, but they are not part of the corporate culture as yet.

For the corporate culture of an organisation to begin to evolve and for employees to progress from Stage 3 to Stage 4 of the Model, a combination of techniques can be used. An Information Security *Education* Program, as discussed previously, will be effective in achieving *Unconscious Competence*. For employees to gain a deeper understanding of why information security is so vital to an organisation they should take part in an Information Security *Education* Program which will address the *shared tacit assumptions* level of corporate culture. Information Security *Education* provides insight to employees about the intricacy of information security practices and their responsibilities.

However, an Information Security *Education* Program alone is not enough. In addition to an Information Security *Education* Program, positive reinforcement could help in the advancement of employees from Stage 3 to Stage 4. Reinforcement should be used as validation that employees are performing the correct information security practices. These reinforcements or incentives that are used to motivate employees do not have to be financial. Positive reinforcement is widely used in behaviour modification in organisations, and it has been found that praise and social reinforcers are more common, and effective, than financial reinforcers (Arnold, Cooper & Robertson, 1998, p 232). Employees will only be able to justifiably advance to Stage 4, *Unconscious Competence*, when they can innately apply the information security skills and procedures they have learnt. Therefore, the employees, through Information Security *Awareness*, *Training* and *Education*, should aim to reach Stage 4. Employees should then be *Unconsciously Competent* in the significant information security practices which support the information security vision of senior management.

However, the ultimate goal should be for Corporate Information Security Obedience to be evident in an organisation. As the information security practices learnt by employees support the information security vision of senior management, they should become part of the *de facto* employee behaviour and, therefore, ultimately part of the corporate culture. Over time, through the *Experience* of performing the information security practices continuously, these information security practices will become *de facto* and employees will advance to Corporate Information Security Obedience through the *Experience* they have gained.

The progression of employees from Stage 1, *Unconscious Incompetence*, to Corporate Information Security Obedience is depicted in the Information Security Competence Maturity Model in Figure 7.1.

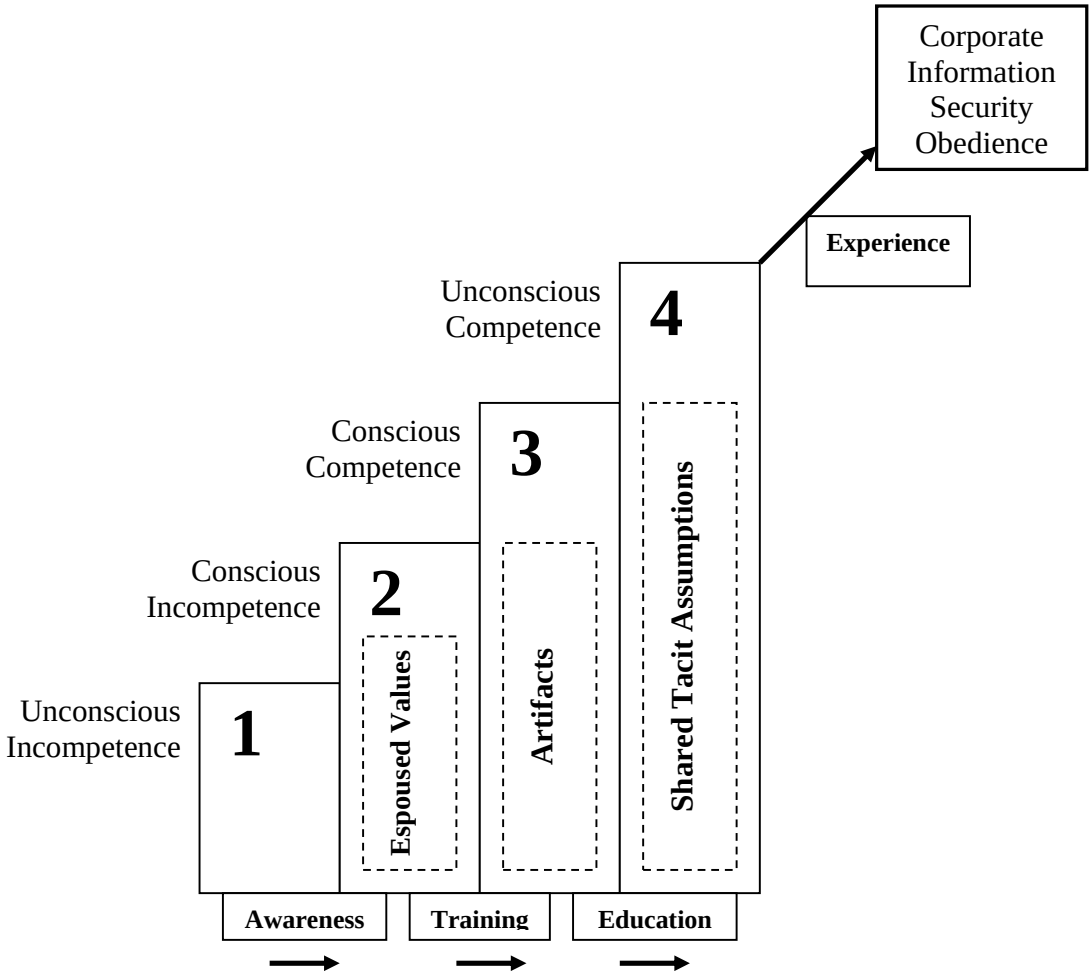

Figure 7.1: Information security competence maturity model

The majority of employees, having no information security knowledge, or skills, will be positioned at Stage 1, or *Unconscious Incompetence*. As depicted in Figure 7.1, in order for employees to advance to Stage 2 of the Model an Information Security *Awareness* Program is required which will affect the *espoused values* level of corporate culture. Through this, employees will be made conscious of the importance of information and what will be required from them.

Once employees have completed an Information Security *Awareness* Program, and are conscious of their information security responsibilities, they move to Stage 2, *Conscious Incompetence*. Employees are now conscious of what is expected from them in the

protection of information, but do not, as yet, have the skills to do so. For employees to move to the next Stage in the Model, they will have to complete an Information Security *Training* Program. Through this Program, employees will be taught the information security skills and practices necessary in their jobs and these skills and practices will impact the *artifacts* level of culture. Employees will, therefore, become competent in information security practices and will advance to Stage 3 or *Conscious Competence*.

Employees at Stage 3 possess the essential skills needed for the successful protection of information assets. Applying these skills, though, still requires a conscious effort on the part of the employee and the skills have not become part of the daily routine of employees. For the skills to become part of the daily routines and, eventually, the corporate culture of an organisation, an Information Security *Education* Program must be attended by employees. It is through the deeper understanding gained in the *Education* Program that employees will begin to follow information security practices in their everyday tasks as this deeper understanding will modify the *shared tacit assumptions* of employees. Eventually, once employees have gained sufficient *Experience* in the information security practices, they will move to Stage 4 or *Unconscious Competence*. Further, as more and more employees become *Unconsciously Competent*, the corporate culture will evolve into one that tends to be Information Security Obedient.

If a corporate culture has become Information Security Obedient, it follows that employees and management, through their attitudes and correct behaviour, are working towards the information security vision of senior management, as outlined in the Corporate Information Security Policy. At the *espoused values* level, the Corporate Information Security Policy, and related procedures, establishes the actions and behaviour required from employees. This behaviour is reflected at the *artifacts* level, which in turn results from the collective beliefs at the *shared tacit assumptions* level. Therefore, the *artifacts*, *espoused values* and *shared tacit assumptions* levels of corporate culture are in alignment with one another. Further, if all Three Levels of Corporate Culture are aligned it indicates that Goal Consensus, as seen in Chapter 5, has been achieved in an organisation.

7.5 Conclusion

The primary focus of any employee in an organisation is getting the job done. Therefore, if seemingly irrelevant tasks and responsibilities appear to be hindering employees as they conduct their daily tasks, they could very well look for ways to circumvent these 'irrelevant' tasks. Too often employees believe that firewalls, and other technical controls, are handling the protection of information and that they do not have a role to play or their role is negligible. Employees must be made to fully appreciate and understand the complexities involved in protecting information assets, as physical and technical controls alone are not enough.

This appreciation and understanding should be achieved through Information Security *Awareness*, *Training* and *Education* Programs in an organisation. All employees need the foundation of an Information Security *Awareness* Program, but learning must go beyond that. Employees should receive Information Security *Training* that is relevant to their particular jobs. The information security skills learned must be incorporated into the everyday tasks of employees over time. One of the most effective ways to ensure that this can be achieved is for all employees to go through an Information Security *Education* program to gain a comprehensive understanding of their information security responsibilities.

Over time, as the employees become accustomed to and experienced in the skills learned through Information Security *Training* and *Education*, these skills will become the norm and part of daily activities. These skills and the behaviour of employees should be in line with the information security vision of senior management. As such, Corporate Information Security Obedience will most probably have been achieved in an organisation.

The following chapter will merge the Three Levels of Corporate Culture, discussed in Chapter 2, Corporate Information Security Obedience, discussed in Chapter 5, the Modes

of Knowledge Creation, discussed in Chapter 6, and the Information Security Competence Maturity Model, discussed in this chapter, into the Model for Information Security Shared Tacit Espoused Values (MISSTEV).

CHAPTER 8

THE MODEL FOR INFORMATION SECURITY SHARED TACIT ESPOUSED VALUES (MISSTEV)

8.1 Introduction

As highlighted in previous chapters, one of the prevalent problems facing the success of information security practices in organisations is the incorrect behaviour and apathy of employees towards information security. In a Coercive Environment, employees' behaviour can be modified through consequences and in a Utilitarian Environment through incentives. In other words, incorrect behaviour is punished and correct behaviour is rewarded in the respective Environments. However, rewards and consequences alone will only change the overt behaviour of employees and, if these incentives and consequences are withheld, employees will more than likely regress.

In order to have a lasting impact on the behaviour of employees, it is vital that the root cause of the incorrect behaviour is identified and modified. As observed in the Three Levels of Corporate Culture, it is the underlying beliefs and values of employees at the *shared tacit assumptions* level that indirectly impacts on the behaviour of employees. Therefore, it is necessary that the tacit knowledge found at this level is addressed and modified to reflect the behaviour outlined in the resultant procedures of the Corporate Information Security Policy. In this way, the correct information security behaviour will become part of an Information Security Conscious Corporate Culture.

As emphasised in previous chapters, however, changing tacit knowledge at the *shared tacit assumptions* level and, ultimately, the corporate culture, is often an extremely complex task. This is because changing the corporate culture requires unlearning beliefs and assumptions and learning new ones. Corporate culture is one of the most stable

aspects of an organisation and employees must be fully motivated and understand the need for change in the organisation.

This chapter will outline the four essential building blocks necessary in the creation of an Information Security Conscious Corporate Culture. These building blocks will be integrated to create the Model for Information Security Shared Tacit Espoused Values or MISSTEV. These building blocks include the Three Levels of Corporate Culture, the Information Security Competence Maturity Model, the Modes of Knowledge Creation and Corporate Information Security Obedience, all of which have been discussed in previous chapters. These four building blocks will be merged together into MISSTEV which will illustrate the evolution of a corporate culture where information security practices and procedures are evident.

8.2 First Component of MISSTEV: Three Levels of Corporate Culture

As detailed in Chapter 2, the Three Levels of *artifacts*, *espoused values* and *shared tacit assumptions* are intertwined to form the basis of corporate culture. Corporate culture is, to a large extent, the essence of an organisation and not something that an organisation can own. Corporate culture exists in every organisation, regardless of whether the management and employees are aware of it. In the cases where management is not aware of the influence of the corporate culture in its organisation and does nothing to shape it, the corporate culture, and resultant behaviour of employees, is often working against the best interests of an organisation.

Also described in Chapter 2 were the classifications of corporate culture, namely; Creative, Quality, Supportive and Productive, as well as the likelihood of sub- and counter-cultures existing within an organisation. Once again, it must be emphasised that regardless of the culture classification in an organisation, or whether sub- or counter-cultures do exist, all corporate cultures consist of the *artifacts*, *espoused values* and *shared tacit assumptions* level. Corporate culture is interwoven throughout an organisation and many of the essential components of culture are, in effect, hidden. In an

attempt to comprehend this multifaceted discipline it is imperative that the Three Levels of Corporate Culture are understood. The deepest, and most intricate, level of the Three Levels is *shared tacit assumptions*. It is at this level that the beliefs, morals and values of employees, in relation to work, exist. These beliefs have been cultivated over time and have become generally accepted by all employees. Very often these beliefs are simply accepted as 'the way things are done around here' and are not challenged by employees who are comfortable in their working environment. New employees will, most often, follow the observed behaviour of their co-workers and will gradually adopt the *shared tacit assumptions* of the group as their own. For that reason, when change is attempted that questions the correctness or validity of the widely held beliefs and values of employees; it is often met with resistance.

The *shared tacit assumptions* level indirectly influences the *artifacts* level of corporate culture. Of all the levels, the *artifacts* level is the most straightforward as it consists of the observed behaviour and actions of the people in an organisation. The behaviour observed at this level is a result of the entrenched beliefs and values that guide the thinking, and consequent actions, of employees. Although the actions of employees at this level may be clear, the reasons behind them are not, unless the *shared tacit assumptions* level of corporate culture is understood. Therefore, in order to change the actions and behaviour of employees, the *shared tacit assumptions* level of corporate culture must be addressed.

Finally, the *espoused values* level of corporate culture is expressed, to a large extent, through the policies of an organisation. These are the values that an organisation is said to be supporting. A Corporate Information Security Policy, and the related procedures, can be found at this level and the policy would outline the behaviour expected from employees in terms of information security. Frequently, however, there are discrepancies between what is expressed at the *espoused values* level and what is seen in practice. If the beliefs and attitude of employees towards information security are not in agreement with the espoused information security values of the Corporate Information Security

Policy, then the observed actions and behaviour of employees towards information assets will not be in coherence with the wishes of senior management.

When it comes to organisational learning, as described in Chapter 6, there are two concepts relevant to the Three Levels of Corporate Culture. These are *theory-in-use* and *theory-of-action*. *Theory-in-use* is developed by observing organisational behaviour and correlates with the *shared tacit assumptions* level. *Theory-of-action*, however, is reflected in corporate policies and correlates with the *espoused values* level.

Every employee in an organisation develops his or her own representation of the *theory-in-use*, or tacit knowledge. This representation is a private image unique to that employee. However, more important to the organisation are the public representations of the *theory-in-use* common to all employees. These public representations are known as organisational maps. As seen in Chapter 6, these organisational maps help to guide the actions and behaviour of employees. Further, just as with the conflict that often exists between the *espoused values* and *shared tacit assumptions* level, so too is there often conflict between the public organisational maps of employees and the *theory-of-action*.

As seen by the potential discrepancies between the *espoused values* level and the *shared tacit assumptions* level and the discrepancies between organisational *theory-in-use* and *theory-of-action*, the behaviour and actions of employees at the *artifacts* level very often do not support the *espoused values* found in corporate policies. Further, this is one of the prevalent problems in the protection of information assets. Very frequently the correct behaviour, actions and practices espoused in the Corporate Information Security Policy, and associated procedures, are not displayed at the *artifacts* level of corporate culture. This indicates that the beliefs of employees towards information security are not in line with the vision of information security that senior management is promoting through the Corporate Information Security Policy.

The private images of individual employees and the public organisational maps of the group are constantly adapting to changes in the working environment. Changes in the

private images and public maps of employees lead to a change in the *theory-in-use* or tacit knowledge in an organisation. A change in the theory-in-use is known as organisational learning. Organisational learning can be compared to the *internalization* and *combination* processes of knowledge creation. The Three Corporate Culture Levels are absolutely essential in addressing the changing of a corporate culture and, therefore, an essential building block in MISSTEV.

8.3 Second Component of MISSTEV: Corporate Information Security Obedience

There are many issues facing the successful implementation of information security into an organisation. Information security is often treated as an overhead or afterthought rather than an investment in the protection of one of the organisation's most important assets. An additional, and arguably the most complex, problem facing the successful implementation of information security in organisations is the behaviour and actions of employees. Even if the best technical and physical controls are in place in an organisation to protect the technology, and the information it houses, careless or uneducated employee behaviour can seriously undermine information security. The corporate culture, to a large extent, is responsible for the behaviour and actions of employees. Therefore, the corporate culture of an organisation should be altered to positively influence the behaviour of employees towards information assets.

The power to change the corporate culture in an organisation lies largely with its senior management. One of the main corporate governance duties of senior management is that it must be accountable and responsible for the protection of the assets of an organisation. Further, senior management should set a clear vision for its organisation and lead through direction-giving. The direction-giving should be achieved through the implementation of corporate policies. Further, the corporate policies of an organisation, and the consequent procedures, should outline the desired behaviour required from all employees in an organisation for the protection of assets.

More specifically, the Corporate Information Security Policy should describe the vision that senior management has for information security in its organisation. Related procedures should outline the behaviour required from employees for the successful protection of information assets. The main aim of any policy, whether for information security or not, is to influence and determine decisions and actions by specifying what behaviour is acceptable and what behaviour is unacceptable. Policies and procedures are, therefore, organisational laws that determine acceptable and unacceptable conduct within the context of the corporate culture

The vision of senior management, as outlined in the corporate policies, may imply that the existing corporate culture is sufficient and will not require change, as the normal development of the culture will achieve the vision of management. Or else, the vision may imply that minor, or widespread, change is necessary to fulfill the vision of senior management. The desired corporate culture would be one where the vision expressed at the *espoused values* level of culture by senior management is supported by the actions and behaviour of employees determined by the *shared tacit assumptions* level of corporate culture.

To achieve the information security vision of senior management it is often necessary that the behaviour of employees will have to change to comply with this vision. In order for this vision to be achieved it is important that this correct behaviour desired by senior management becomes *de facto* or second-nature to employees and part of their daily activities. If the desired information security behaviour and actions become second-nature to employees and part of the corporate culture, then Corporate Information Security Obedience will be evident in an organisation.

For Corporate Information Security Obedience to be apparent in an organisation, it is required that the *shared tacit assumptions* level of corporate culture, or the beliefs and values of employees, is in line with the *espoused values* level of senior management. This indicates that a Goal Consensus Environment has been achieved in an organisation,

where both management and employees are working towards the vision of senior management.

8.4 Third Component of MISSTEV: Modes of Knowledge Creation

"The beginning of knowledge is the discovery of something we do not understand". This quote by Frank Herbert highlights that for knowledge creation to begin, it must first be discovered what knowledge is lacking (The Quotations Page, 2006, online). To maintain a competitive edge it is necessary for organisations to create and disseminate new knowledge on a daily basis. In most organisations, for information security practices to become part of the daily routine, it is required that this new information security knowledge is created. This new knowledge, pertinent to information security, will impact several levels of corporate culture as will be seen in this section.

The new knowledge created is either tacit or explicit knowledge. Tacit knowledge is difficult to communicate and includes beliefs, attitudes and values. Explicit knowledge, on the other hand, can be communicated effectively. The four processes of interaction between tacit and explicit knowledge are represented in the Modes of Knowledge Creation. These processes are *externalization*, *socialization*, *combination* and *internalization.*

Through *externalization* tacit knowledge is made explicit. Tacit knowledge is found at the *shared tacit assumptions* level of corporate culture and this tacit knowledge determines the actions and behaviour of employees. Therefore, through *externalization*, the beliefs and values that drive behaviour should be made known. *Externalization* can be achieved through the expression of beliefs and values in discussion and dialogues.

Socialization enables the tacit knowledge of an individual to be transferred to the tacit knowledge of another. Knowledge is captured through direct interaction and a good deal of knowledge can be created through observation. *Socialization* impacts the *shared tacit assumptions* level only as it creates tacit knowledge from tacit knowledge. *Socialization*

depends on the shared experiences of individuals to build the *shared tacit assumptions* level of corporate culture.

Combination is used for the transfer of explicit knowledge to the explicit knowledge of a group. Explicit knowledge can be disseminated through, for example, documents, policies and e-mails, as well as through meetings. *Combination* impacts only the *espoused values* level of corporate culture and deals with explicit knowledge. The collection of explicit knowledge and the way that knowledge is distributed throughout an organisation is of utmost importance for the success of *combination*.

Internalization is the process individuals use to absorb explicit knowledge into their own tacit knowledge. The explicit knowledge is found at the *espoused values* level of corporate culture and defines the desired behaviour required from employees. For *internalization* to be successful it is necessary for an individual to practice the skills, tasks or behaviour learnt through the explicit knowledge from the *combination* process. Gradually, explicit knowledge, and the related skills and tasks, will become tacit.

The Modes of Knowledge Creation are extremely significant to the learning process of an organisation and goes beyond the concept of organisational learning. Organisational learning entails the detection and correction of error in an organisation. Organisational learning can be compared to the *internalization* and *combination* processes of the Modes of Knowledge Creation as it deals chiefly with the conversion of explicit knowledge into organisational *theory-in-use*, or tacit knowledge, and explicit knowledge to explicit knowledge and, therefore, has limited implications. The Modes of Knowledge Creation deal with both tacit and explicit knowledge and the exchange between these types of knowledge.

In order to set the Modes of Knowledge Creation into motion, a degree of commitment is necessary from employees. As mentioned in Chapter 6, employees' commitment to an organisation plays an important role in encouraging the creation of new knowledge. Therefore, in order to change the way things are done in an organisation and to create

new knowledge requires that employees are committed to that change. It is vital, therefore, to encourage employees to be committed to information security in their organisation. One way to ensure this commitment is for employees to fully understand the significance of information security for the organisation.

Figure 8.1 represents the relationship between the first component of MISSTEV, the Three Levels of Corporate Culture, and the third component, the Modes of Knowledge Creation.

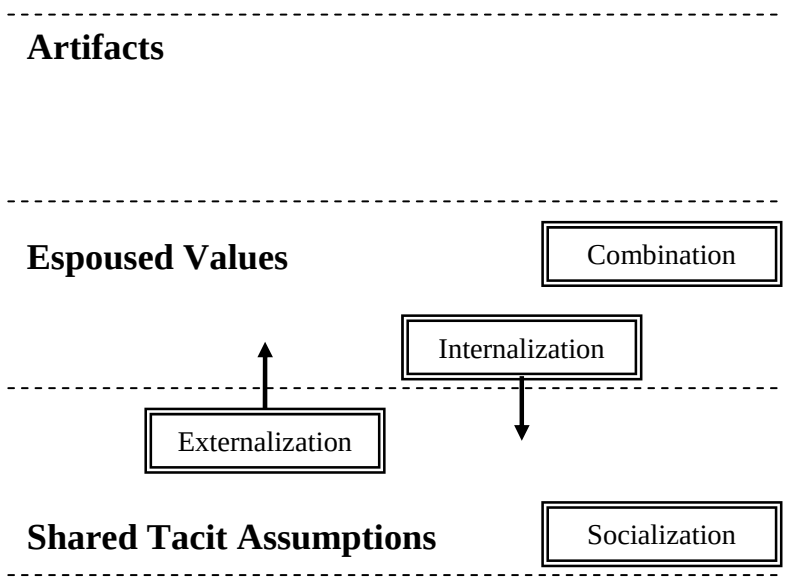

Figure 8.1: Three levels of corporate culture and modes of knowledge creation

As can be seen in Figure 8.1, the knowledge creation process of *combination* affects only the *espoused values* level of corporate culture as it deals only with explicit knowledge. The processes of *internalization* and *externalization* affect both the *espoused values* and *shared tacit assumptions* level of corporate culture as they deal with both explicit and tacit knowledge. The process of *socialization* affects the *shared tacit assumptions* level of corporate culture only as it deals with tacit knowledge alone.

8.5 Fourth Component of MISSTEV: Information Security Competence Maturity Model

In a quote by Abigail Adams she says, “Learning is not attained by chance; it must be sought for with ardor and attended to with diligence” (The Quotations Page, 2006, online). Employees in an organisation must be committed to change in order to learn new skills and behaviour. As they step through the Information Security Competence Maturity Model, employees should be motivated to reach the pinnacle of the Maturity Model. As detailed in Chapter 7, for employees to learn new skills and behaviour, they must move through four stages of learning, *Unconscious Incompetence*, *Conscious Incompetence*, *Conscious Competence*, and *Unconscious Competence*.

At Stage 1, *Unconscious Incompetence*, employees are unaware of the tasks, skills and behaviour necessary for the protection of information assets. Through an Information Security *Awareness* Program employees should be made conscious of the roles they should be playing in information security. At Stage 2, *Conscious Incompetence*, employees are aware of their role in information security, but as yet do not know how to go about protecting information assets. In order to progress to Stage 3 of the Maturity Model, employees must attend an Information Security *Training* Program. Through this Program employees will learn the skills and behaviour required of them to protect information assets.

At Stage 3, *Conscious Competence*, employees now have the skills to be competent in the protection of information assets. Employees have the necessary proficiency to complete any information security task. However, the completion of these tasks still requires a great deal of concentration. Therefore, even though employees are competent in information security skills, it is possible that they may still be careless or forgetful in the protection of information assets. This is as a result of the fact that information security has not, as yet, become part of the corporate culture. In order for this to happen and for information security to become part of the daily routine, employees must progress to Stage 4 of the Information Security Competence Maturity Model, *Unconscious Competence*.

An Information Security *Education* Program can be used to assist in the progression of employees from Stage 3 to Stage 4 of the Information Security Competence Maturity Model. The skills learnt in the Information Security *Training* Program and reinforced by the *Education* Program should, by this stage, have become second-nature to employees. In addition to the Information Security *Education* Program, *Experience* will contribute to making employees comfortable with the new information security practices. The more experienced employees become in the information security practices, the more rapidly these practices and skills will form part of the corporate culture of an organisation. *Experience* will, over time, ensure that Corporate Information Security Obedience becomes evident in an organisation.

Figure 8.2 represents the relationship between the second component of MISSTEV, Corporate Information Security Obedience, and the fourth component, the Information Security Competence Maturity Model.

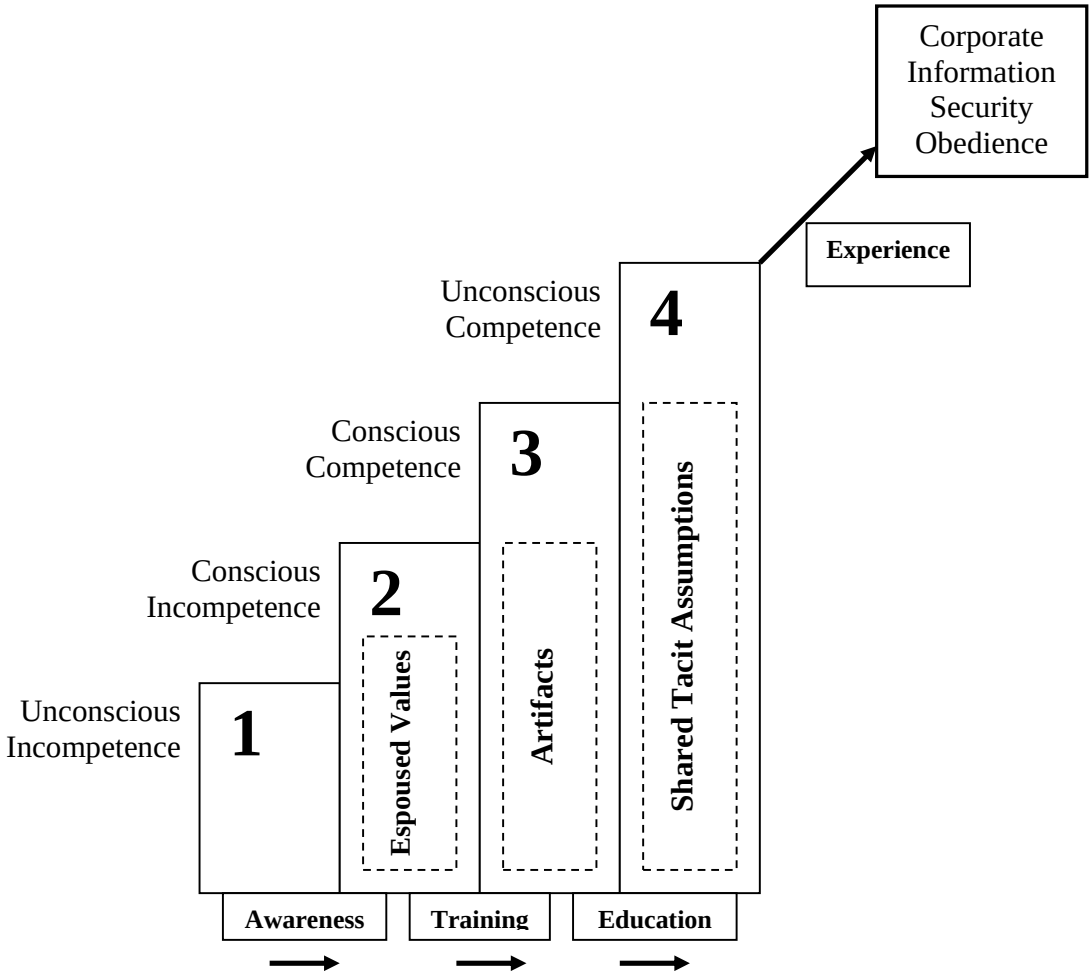

Figure 8.2: Information security competence maturity model

As can be seen from Figure 8.2, Corporate Information Security Obedience is the ultimate goal that should be strived for in an organisation in terms of information security. Through Information Security *Awareness*, *Training* and *Education* Programs, employees should progress from being *Unconsciously Incompetent* to *Unconsciously Competent* in information security procedures and practices. Over time, through *Experience*, the information security skills and practices that have become second-nature to employees will evolve and become part of the everyday activities of employees. Information security has, therefore, become part of the corporate culture of the organisation. This behaviour should reflect the desired behaviour outlined in the

Corporate Information Security Policy, and related procedures, and will indicate that Corporate Information Security Obedience has been achieved.

8.6 The Model for Information Security Shared Tacit Espoused Values or MISSTEV

The senior management of an organisation, through its corporate governance duties, is responsible and accountable for the protection of an organisation's assets. Information is one of the most important assets that an organisation possesses. Therefore, it follows that senior management is responsible and accountable for the protection of the information assets in its organisation.

A common grievance of information security professionals is that senior management does not give the protection of information the priority it deserves. Information security is most often thought of, by senior management, as the IT department's problem and not one for senior management. Management's focus is often limited to a small set of acute threats to information assets rather than a comprehensive information security solution.

A further obstacle in accomplishing the protection of information assets is the often indifferent attitude and corresponding apathetic behaviour of employees. Employees frequently do not fully appreciate the role that they should be playing in the protection of information assets and see information security as an 'add-on' that is not vital to completing their tasks. As a result, employees will regularly use any 'workaround' they can to avoid information security related tasks. However, if employees were to comprehend the importance of information security, how it relates to their job and the sustainability of the organisation, they will be more inclined to adhere to the information security practices prescribed by senior management. Over time, as these practices are used more often, information security should become embedded in the corporate culture of an organisation. This section will detail the construction and development of MISSTEV which tracks the progression of employees from the awareness of information security practices to an Information Security Conscious Corporate Culture. The Model

for Information Security Shared Tacit Espoused Values or MISSTEV is shown in Figure 8.3.

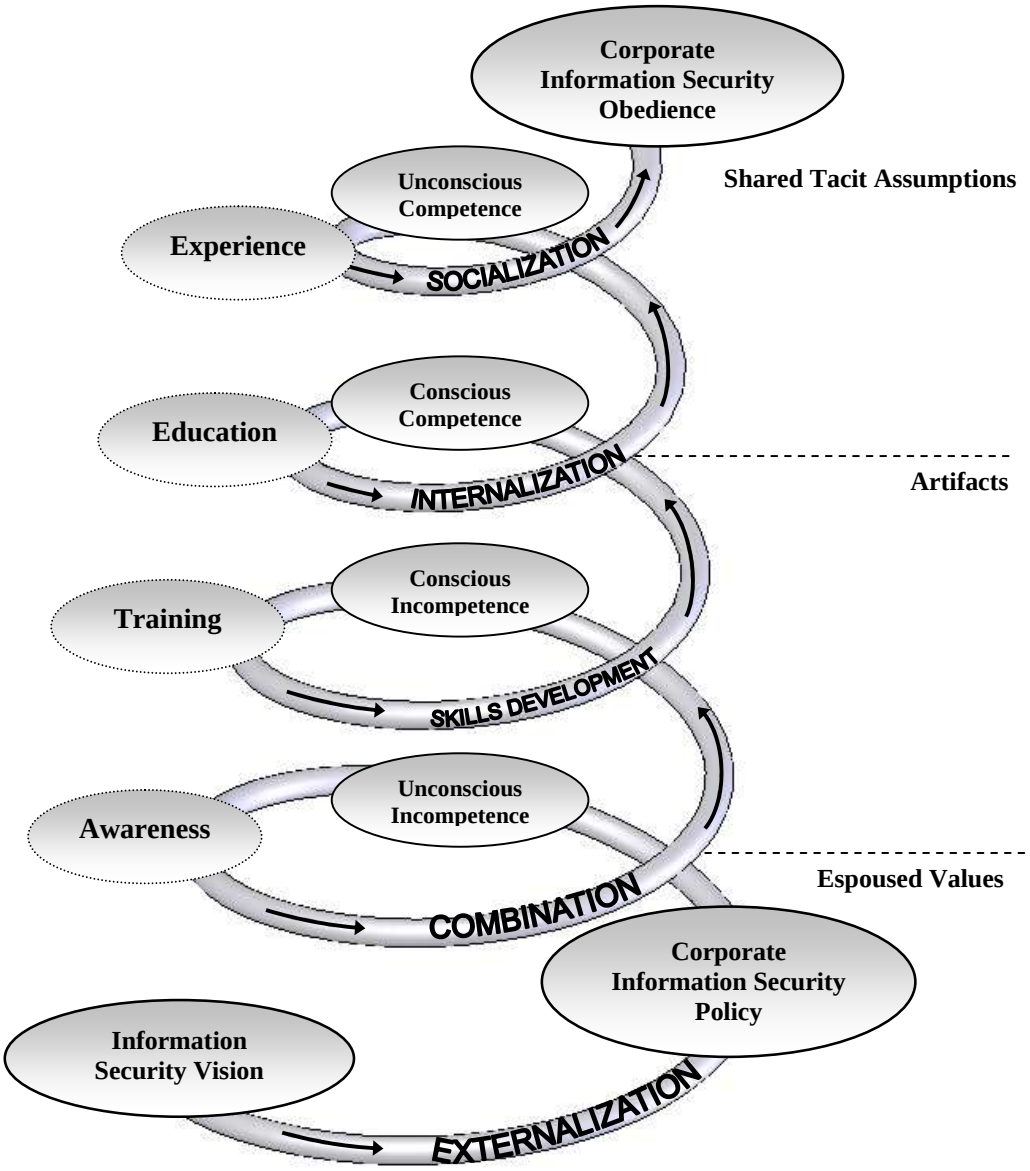

Figure 8.3: Model for information security shared tacit espoused values or MISSTEV

The foundation of MISSTEV, as seen in Figure 8.3, is the information security vision of senior management. Senior management must demonstrate its commitment to the protection of information assets by formalizing its vision for information security through

the Corporate Information Security Policy. The Corporate Information Security Policy, and the related procedures, describes the actions and behaviour that is required from employees for the protection of information assets. Through the creation of the policy, senior management is converting its tacit knowledge, concerning information security, into explicit knowledge. This is done through the *externalization* process of the Modes of Knowledge Creation. This process allows the tacit knowledge of the *shared tacit assumptions* level of senior management to be expressed as *espoused values* of the organisation.

As seen in the Model, once the *externalization* process is complete, and the Corporate Information Security Policy has been created, the competence of employees in terms of information security can now be addressed. For the purposes of the Model, all employees begin the spiral process at the *Unconscious Incompetence* stage.

At this stage, employees are unaware of the skills necessary to adequately protect the information assets of an organisation and they do not know the role they should play in information security as yet. At this stage, the employees' beliefs and values regarding information security, found at the *shared tacit assumptions* level of corporate culture, is not in alignment with the vision of senior management at the *espoused values* level. In other words, the tacit knowledge of employees is different to the explicit knowledge of the organisation.

In order for employees to become aware of the role they should play in information security all employees, as seen in Figure 8.3, must participate in an Information Security *Awareness* Program. The purpose of the program is to make employees conscious of the importance of information assets and the reason why it must be protected for the well-being of the organisation. The explicit information security knowledge included in the Information Security *Awareness* Program should develop into the explicit knowledge of employees through the process of *combination*.

Through *combination*, the vision of senior management, expressed in the Corporate Information Security Policy and found at the *espoused values* level of corporate culture, will be made known to employees and become their explicit knowledge. The vision is now known to employees, but as yet is not part of their *shared tacit assumptions*. As employees are now aware of the importance of information and the skills they lack, they progress to the *Conscious Incompetence* stage of MISSTEV.

At this stage employees know what they should be doing to protect information assets, but, as yet, do not know how this can be accomplished. Through the Information Security *Awareness* Program, employees have been made fully conscious of exactly what is required of them to achieve the information security vision of senior management. Further, employees must now learn the skills and practices necessary to support the Corporate Information Security Policy. This can be achieved, as seen in the Model, through an Information Security *Training* Program. This *Training* Program should be tailored according to the job descriptions of employees and their information security responsibilities. As seen in Figure 8.3, through the *Training* Program, employees will undergo *skills development* necessary for the implementation of information security in the organisation.

Employees will now be competent in the information security skills, procedures and practices necessary for the protection of information assets. As such, employees will progress to the *Conscious Competence* level of MISSTEV. However, even though employees are now competent, this does not mean that employees will necessarily implement the skills they have learned. The skills gained through the Information Security *Training* Program will only be effective if employees are continuously encouraged, monitored and motivated to use them. These information security skills and practices still require a good deal of concentration and thought to be implemented correctly. Therefore, even though the correct information security practices and procedures might be in place in an organisation, the underlying beliefs and values associated with the behaviour of employees are not, as yet, necessarily aligned with the

vision of senior management. This means that the information security vision, found at the *espoused values* level, is not in line with the *shared tacit assumptions* level.

In order to align the *espoused values* and *shared tacit assumptions* levels of corporate culture, it is necessary for employees, as seen in Figure 8.3, to attend an Information Security *Education* Program. This Program will give employees a deeper understanding of the information security vision of senior management and encourage employees to adopt this vision as their own. In conjunction with this, over time, as employees are constantly using the information security skills and practices they have learnt, these skills and practices will become intrinsic or second-nature to the employees. The protection of information assets will, therefore, become part of the daily activities of employees. The process of employees adopting the values espoused through the Corporate Information Security Policy, and actively using information security practices, is achieved through the process of *internalization*.

Through *internalization*, the explicit knowledge of employees becomes tacit knowledge. In other words, the information security vision espoused by senior management has become part of the *shared tacit assumptions* of employees. As both senior management and employees are now working towards the same information security vision and goals, employee behaviour at the *artifacts* level of corporate culture will support the Corporate Information Security Policy.

Once the *internalization* process is complete, employees will have progressed to the *Unconscious Competence* stage of MISSTEV. At this stage, information security practices and procedures, displayed at the *artifacts* level, are as a result of the modified beliefs and values found at the *shared tacit assumptions* level. The *shared tacit assumptions* level, in turn, is aligned with the *espoused values* level of corporate culture. Further, the Corporate Information Security Policy is found at the *espoused values* level. This indicates that the Three Levels of Corporate Culture are aligned with one another and aligned with the information security vision of senior management.

As seen in Figure 8.3, over time and through *Experience*, employees at the *Unconscious Competence* stage of MISSTEV will ultimately reach Corporate Information Security Obedience. For this to occur, *socialization* is necessary. The *socialization* process is needed to ensure that the tacit information security knowledge, learnt as they progressed through MISSTEV and through *Experience*, is shared among employees. This process becomes particularly significant for employees who are new to an organisation as it assists them in determining what is expected of them in terms of information security. The *socialization* process is, therefore, necessary for the sustainability of the corporate culture.

Once all employees have achieved *Unconscious Competence* in information security, the *socialization* process will allow, ultimately, for the evolution of the corporate culture into one where Corporate Information Security Obedience is evident in the organisation. This means that the everyday or *de facto* employee behaviour complies with the information security vision as outlined in the Corporate Information Security Policy. Once Corporate Information Security Obedience has evolved in an organisation, success has been achieved. The ultimate vision of senior management for information security has been realised in the organisation.

8.7 Conclusion

The corporate culture of any organisation is complex and multifaceted and greatly influences the behaviour and attitude of employees. The senior management of an organisation has the responsibility to shape the corporate culture into one that will support the vision senior management has for the future of the organisation. Senior management must outline its vision for the organisation through its corporate policies.

A general grievance of security professionals is the lack of support from senior management for information security as it is often seen as the responsibility of the Information Technology department. The development and creation of a Corporate

Information Security Policy should demonstrate the commitment of senior management to the protection of information assets.

The Corporate Information Security Policy, and the related procedures, will outline the behaviour necessary for achieving the successful protection of information assets. The challenge, however, is ensuring that the behaviour outlined by the information security procedures becomes the *de facto* behaviour of employees and part of an organisation's corporate culture. In order for this to occur, the tacit knowledge of employees, found at the *shared tacit assumptions* level of corporate culture, must be modified. The *shared tacit assumptions* level of corporate culture should be aligned with the vision outlined in the Corporate Information Security Policy found at the *espoused values* level. Employees must learn the behaviour and skills necessary for the protection of information as described in the policy.

The learning process of employees is outlined in the Model for Information Security Shared Tacit Espoused Values or MISSTEV. The building blocks for this Model were outlined in this chapter, namely; the Three Levels of Corporate Culture, Corporate Information Security Obedience, the Modes of Knowledge Creation and the Information Security Competence Maturity Model. MISSTEV tracks the progression of employees from the *Unconscious Incompetence* stage to the *Unconscious Competence* stage. Through MISSTEV, employees should be informed about the information security vision of senior management and their roles and responsibilities to protect information. Further, by following the spiral of the Model, employees should be made aware of and trained in the correct skills necessary to protect information assets, and these skills should become part of the *de facto* practices of the employees. Ultimately, if all employees follow the spiral of MISSTEV, Corporate Information Security Obedience should become evident in an organisation and the vision of senior management will have been realised.

CHAPTER 9

CONCLUSION

9.1 Introduction

This thesis is a report of the research undertaken with regard to the integration of acceptable information security practices into the corporate culture of an organisation. To accomplish this, the following topics, *inter alia*, were examined; corporate culture and management's role in corporate culture, information security and the impact of employee behaviour on the protection of information assets, and knowledge creation and the learning processes within an organisation.

It was argued that in order to address the research problem the focus should be on the beliefs and values of employees regarding information security. Only once employees believe in the importance of information assets for the sustainability of an organisation will they begin to integrate information security practices into their daily activities. The greater part of this concluding chapter will evaluate whether the research objectives of this thesis were met. Following this, areas for future research will be discussed.

9.2 Evaluation of the Research Outcomes

The primary objective of this research project was to develop a model that will assist in the integration of information security practices into an organisation. To achieve this primary objective, a number of secondary objectives were defined. This remainder of this section will address the secondary objectives, which were identified in Chapter 1, Section 1.4.

Research Objective: *An investigation into the role that management should play in the integration of information security into an organisation.*

This objective helped clarify the accountability and responsibility senior management should have towards the information assets in its organisation. Further, the role that senior management should play in the integration of information security practices into the corporate culture of an organisation was explained.

Senior management has many corporate governance responsibilities in its organisation. One of the main duties of the managing director, together with senior management, is to set the vision and strategic direction for the organisation in a responsible manner. Senior management is accountable to stakeholders and must ensure the reputation of its organisation and the protection of the organisation's assets. One such asset that must be protected is information.

Senior management should demonstrate its commitment to the protection of information assets by developing a Corporate Information Security Policy. However, it is not enough for the policy to just be created. Through the policy, employees must begin to understand their roles and responsibilities towards the protection of information. It is through understanding that employees will begin to incorporate the correct information security practices into their daily behaviour.

Therefore, this objective was achieved in Chapters 3 and 4 by detailing that management's role in integrating information security practices into an organisation should be part of its corporate governance duties in the protection of the organisation's assets.

Research Objective: *An examination of the impact that employee behaviour could have on the successful implementation of information security practices in to an organisation.*

It was highlighted how the apathetic or incorrect behaviour of employees can be an obstacle to the successful implementation of information security practices into an organisation.

The human element of information security is one of the most, if not the most, essential. This is because almost all information security practices rely on the human element to a large degree. However, employees continue to be the most severe threat to information security.

An organisation could have the best physical and technical controls in order to protect its information assets, but an employee, either inadvertently or maliciously, could circumvent these controls and information is placed at risk. For the majority of employees, their main concern at work is to complete the task at hand. As a result of the pressure related to an employee's job, any tasks that are not deemed essential to 'getting things done' are often overlooked or regarded as obstacles. Therefore, if employees consider security to be something that is a hindrance to completing their tasks, they might not take proper preventative measures, and worse, might find a 'workaround' to any security measure they do not consider necessary. In order for employee behaviour to positively impact the implementation of information security practices into an organisation, the beliefs and attitudes of employees must be addressed.

Therefore, as seen in Chapter 4, incorrect employee behaviour can severely, and negatively, impact the success of the implementation of information security practices into an organisation.

Research Objective: *A study of the theories and concepts underlying corporate culture and determining how corporate culture could influence the employees in an organisation.*

This study of the theories and concepts underlying corporate culture helped clarify the complex concept of corporate culture and why it is such an important consideration when attempting to change the behaviour and attitudes of employees.

Corporate culture is an underlying, but often misconstrued, force within all organisations that influences the behaviour and attitudes of its employees. In order to gain a better insight into corporate culture, it was established that the Three Levels of Corporate Culture, namely; *artifacts*, *espoused values*, and *shared tacit assumptions*, must be examined and understood in an organisation. The *espoused values* level represents the goals and strategy of an organisation. However, the values identified at the *espoused values* level is not always apparent at the *artifacts* level, which denotes the actions and behaviour of employees. This is because it is the beliefs and values of employees, found at the *shared tacit assumptions* level of corporate culture, that influence the behaviour of employees observable at the *artifacts* level.

Therefore, the concept of corporate culture was explored in Chapter 2 and the influence that the corporate culture has on the behaviour of employees, as a result of their beliefs and values, was detailed.

Research Objective: *An investigation into management's role in corporate culture and the influence of management policies in shaping the corporate culture.*

The investigation addressed and assisted in clarifying the significant role that senior management should be playing in the protection of information assets. It is

vital that senior management understands, and is involved in, the shaping of the corporate culture, as it is the corporate culture that assists in giving the organisation its meaning and direction. However, shaping and transforming the corporate culture takes time and determination. In order to change the corporate culture, employees' beliefs and values at the *shared tacit assumptions* level should be changed. Unlearning beliefs and changing the attitudes of employees can be a painful process. Further, it should be senior management's task to lead this transformation of the corporate culture by setting an example, so that the change can saturate the organisation. If management demonstrates the need for changing the current beliefs and values is imperative to the sustainability of the organisation, it will emphasise and encourage the change in corporate culture.

To assist in shaping the corporate culture, an organisational vision should be expressed by management in its policies. Management policies, and the related procedures, determine what behaviour and actions are acceptable and which are unacceptable. These policies should be enforced to assist management in curbing incorrect behaviour in its organisation and, ultimately, change the corporate culture.

Therefore, as detailed in Chapter 3, senior management has a significant role to play in shaping the corporate culture in its organisation. Senior management should be involved in the development and communication of management policies to employees, as the role of policies should be to influence and determine the behaviour and actions of employees. Consequently, senior management should shape the corporate culture through policies and through leading by example.

Research Objective: *Determining the role of the Corporate Information Security Policy in aligning management's information security vision with the behaviour of employees.*

This objective established the purpose of the Corporate Information Security Policy and why it is crucial in the alignment of the information security vision and the behaviour of employees. To demonstrate its commitment to information security, senior management should be involved in the development of a Corporate Information Security Policy. This policy should outline senior management's vision for information security in the organisation. In addition, the policy, and the related procedures, should provide guidance for employees as to what behaviour is acceptable and what behaviour is unacceptable in the protection of information assets.

The communication of the Corporate Information Security Policy is just as important as the policy itself. It is crucially important that the policy is effectively disseminated to all employees in the organisation for the employees to know what is expected of them. However, even though employees know what is expected of them, it is possible that they will not adhere to the behavioural guidelines in the policy if they do not believe them to be of any consequence. Therefore, senior management must emphasise the importance of the policy, and related procedures, to influence employees into paying attention to the policy and treating the policy with respect.

Therefore, as discussed in Chapter 4, the Corporate Information Security Policy should outline the information security vision of senior management. As the policy should influence the behaviour and actions of employees in an organisation, it should be used as the foundation for aligning the vision of senior management and the behaviour of employees by specifying what is expected of employees.

Research Objective: *A study of the knowledge creation process in an organisation and the learning process of employees.*

The study of the knowledge creation process highlighted the fact that knowledge creation is an essential part of any organisation. Without the creation and effective use of new knowledge, organisations would, in all probability, lose their competitive edge. Essential to change in an organisation is the development of both tacit and explicit knowledge, and the interaction between the two. Explicit knowledge refers to knowledge that is transmittable in formal, organised language. Tacit knowledge, on the other hand, has a personal quality, which makes it difficult to formalise and communicate. Tacit knowledge drives action, commitment, and involvement in an organisation. The four Modes of Knowledge Creation proposed by Nonaka, namely; *socialization, combination, internalization* and *externalization*, are the processes used by organisations to create fresh knowledge through the interaction of explicit and tacit knowledge. It must be emphasised that knowledge creation is a spiral process that leads to a deeper understanding of the knowledge that has been created or shared.

Whenever employees need to learn new skills and, possibly, develop new beliefs, there are four stages that they will progress through, namely; *Unconscious Incompetence*, *Conscious Incompetence*, *Conscious Competence* and *Unconscious Competence*. In terms of information security, it is important that employees understand the role they should play in the protection of information assets. This awareness and understanding should be achieved through Information Security *Awareness*, *Training* and *Education*.

Therefore, this objective was achieved through an extensive study of the Modes of Knowledge Creation in Chapter 6 and through detailing the learning process of employees in Chapter 7.

Research Objective: *An investigation into the relationship that should exist between information security, corporate culture and corporate governance.*

This objective was met through the definition of the term Corporate Information Security Obedience which can be used to describe the relationship between corporate culture, corporate governance and information security.

Through this relationship, senior management is both accountable and responsible for the information assets in its organisation. A Corporate Information Security Policy should be developed to outline the vision that senior management has for information security in its organisation. Furthermore, the Corporate Information Security Policy should influence the actions and behaviour, and ultimately the fundamental beliefs and values, of employees in the protection of information assets. As the beliefs and values of employees begin to change and become aligned with the Corporate Information Security Policy, so too will the corporate culture of an organisation change into one that is more information security conscious.

Therefore, as detailed in Chapter 5, the disciplines of corporate culture, corporate governance and information security should be inextricably linked, through Corporate Information Security Obedience, to ensure the satisfactory protection of information assets in an organisation.

In addition to these secondary objectives, the primary objective of developing a model to assist with the integration of information security practices into an organisation was met through the development of MISSTEV constructed in Chapter 8. MISSTEV should communicate the information security vision of management to employees, as well as the roles, responsibilities and skills needed by employees to protect information assets. Through the spiral process of MISSTEV the protection of information assets should become *de facto* behaviour for employees.

Therefore, one can assertively state that the primary objective of this thesis, the development of MISSTEV, as well as the secondary objectives of this thesis have been discussed and met.

9.3 Directions for Future Research

This research project proposed the Model for Information Security Shared Tacit Espoused Values or MISSTEV. This model was constructed from various components which were detailed in this thesis. There remain, however, certain aspects of the model that can be refined and investigated further. This section will outline these aspects and the areas for future research.

The *externalization* process of senior management's information security vision and the translation of this vision into the Corporate Information Security Policy can be investigated further.

Further, it was established that in order for employees to progress from the *Unconscious Incompetence* to the *Conscious Incompetence* stage of MISSTEV employees will have to take part in an Information Security *Awareness* Program. This study, however, did not detail the elements that should be included in the *Awareness* Program. Future research should investigate how an Information Security *Awareness* Program should be structured to be most beneficial for an organisation. Similar investigations should be undertaken to establish the structure and components that should be included in an Information Security *Training* and *Education* Programs.

An Information Security *Training* Program is necessary for employees to progress from the *Conscious Incompetence* to the *Conscious Competence* stage of MISSTEV. Future research should include an investigation into the skills that will be necessary for employees to adequately protect information assets in an organisation. In addition, ideally, an Information Security *Training* Program should be tailored to fit the roles and

responsibilities of employees. Future research may be able to establish how this can be achieved.

An Information Security *Education* Program is necessary for employees to progress from the *Conscious Competence* to the *Unconscious Competence* stage of MISSTEV. The details of what should be included in the *Education* Program should form part of future research.

Therefore, future research should attempt to refine aspects of MISSTEV. This should provide added depth to the model and further detail to the learning process of employees as they progress through MISSTEV.

9.4 Epilogue

The most important asset of many organisations is information. It is crucial that this significant asset is protected through adequate information security practices. One of the major stumbling blocks, however, to the successful implementation of information security practices is the incorrect and apathetic behaviour of employees. Incorrect employee behaviour could have an enormously detrimental impact on the protection of information.

Therefore, the issue of employee behaviour must be addressed in an organisation to assist in ensuring the protection of information assets. Employees could adhere to the correct behaviour because of rewards they might receive or because of the consequences they will face if they do not. Rewards and consequences, however, should not be the reason for employees adhering to the correct behaviour and practices. Further, rewards and consequences are not the ideal in an organisation, as both rewards and consequences require strict management to ensure their effectiveness. Ideally, the corporate culture of an organisation should be shaped to include correct information security practices into the everyday tasks and behaviour of employees. In order to address the behaviour of employees it is imperative that the beliefs and values of employees are addressed.

As the beliefs of employees regarding information security change to reflect the importance of information security to an organisation, so the behaviour of employees should also change. Over time, and through experience, the correct information security practices and behaviour should become part of the corporate culture of the organisation.

Thereby, the *shared tacit assumptions* of employees and the *espoused values* of management, regarding information security, should be aligned to create a corporate culture that is information security competent.

REFERENCES

The Alliance (2001). *What is risk management?* [online]. [cited 20 August 2002] Available from Internet: URL http://www.allianceonline.org/faqs.html

Accel-Team (2000). *Change Management. Achieving Goal Congruence - Integration of Goals and Effectiveness.* [online]. [cited 18 June 2005] Available from Internet: URL http://www.accel-team.com/techniques/goal_congruence.html

Argos Press. (1999). *What is the meaning of double loop learning?* [online]. [cited 4 April 2004] Available from Internet: URL http://risk-management.argospress.com/doublloopylearn.htm

Argyris, C. and Schon, D.A. (1978). *Organizational learning: a theory of action perspective.* Reading, Massachusetts : Addison-Wesley Publishing Company.

Arnold, J., Cooper, C.L & Robertson, I.T. (1998). *Work psychology – understanding human behaviour in the workplace.* Edinburgh Gate, England : Prentice Hall.

Atkinson, P. (1997). *Creating culture change – strategies for success.* Bedfordshire, England : Rushmere Wynne.

Beach, L.R. (1993). *Making the right decision. Organizational culture, vision and planning.* Eaglewood Cliffs, New Jersey : Prentice Hall.

Berti, J. and Rogers, M. (2004). *Social engineering: the forgotten risk.* Information security management handbook – fifth edition. Boca Raton, London, New York, Washington D.C. : Auerbach Publishers.

Bettinger, C. (1989). Use corporate culture to trigger high performance. *The Journal of Business Strategy*, March/April, pp. 38-42.

Boisnier, A. and Chatman, J.A. (2002). *The role of subcultures in agile organizations* [online]. [cited 28 January 2006] Available from Internet: URL http://www.hbs.edu/research/facpubs/workingpapers/papers2/0102/02-091.pdf

Brooks, J. (April 1997). *Converging cultures - trends in European corporate governance.* [online]. [cited 12 February 2003]. Available from Internet: URL http://www.tiaa-cref.org/pressroom/corpgov.pdf

Bruce, G. and Dempsey, R. (1997). *Security in distributed computing – did you lock the door?.* Upper Saddle River, New Jersey : Prentice Hall.

Buren, A., van der Meer, B., Shahim, A., Barnhoorn, W. & Roos Lindgreen, E. (1999). Information security at top level. *Information security management & small systems security*, pp.75-76.

Cangemi, M. (March 2000). *A call to action for corporate governance* [online]. [cited 16 July 2002] Available from Internet: URL http://csweb.rau.ac.za/ifip/issa2002/presentations/Basie%20von%20Solms.ppt

Chapman, A. (2001). *Conscious competence learning model.* [online]. [cited 3 October 2004] Available from Internet: URL http://www.businessballs.com/ProcessofchangeJF2003.pdf

Charlton, G. (2000). *Human habits of highly effective organisations.* Pretoria, South Africa : Van Schaik Publishers.

Collis, J. & Hussey, R. (2003). *Business research: a practical guide for undergraduate and postgraduate student – second edition.* London, UK : Palgrave Macmillan Ltd.

Deal, T.E. and Kennedy, A.A. (1982). *Corporate cultures: the rites and rituals of corporate life*. Harmondsworth, Penguin Books.

Deloitte & Touche. (May 2002). *Management briefing – information security*. [online]. [cited 13 January 2003] Available from Internet: URL http://www.deloitte.com/dtt/cda/doc/content/info_security(1).pdf

Dictionary.com. (2003). [online]. [cited 3 July 2003]. Available from Internet: URL http://dictionary.reference.com/search?q=obedience

Drennan, D. (1992). *Transforming company culture.* Berkshire, England : MacGraw-Hill.

Fenton, J.H. & Wolfe, J.M. (2004). *Organizing for success: some human resources issues in information security.* Information security management handbook – fifth edition. Boca Raton, London, New York, Washington D.C. : Auerbach Publishers.

Freeman, E.H. (2004). *Information security and personnel practices.* Information security management handbook – fifth edition. Boca Raton, London, New York, Washington D.C. : Auerbach Publishers.

Galbraith, J.K. (1983). *The anatomy of power*. Boston : Houghton Mifflin.

Gjerstad, E. (2005). *Ethics and Power in Governance: Avoiding totalitarianism, dogmatism and relativism* [online]. [cited 2 February 2006] Available from Internet: URL http://soc.kuleuven.be/io/ethics/paper/Paper%20WS1_pdf/Eevastiina%20Gjerstad.pdf

Gordon, G. (May 12, 2002). Dozens of threats beset your data. *Sunday Times, Business Surveys* [online]. [cited 17 July 2002] Available from Internet: URL http://www.suntimes.co.za/2002/05/12/business/surveys/internet/survey10.asp

Gordon & Glickson LLC. (2001). *Information technology today is fraught with risks, and missteps can be costly.* [online]. [cited 23 March 2003] Available from Internet: URL http://www.ggtech.com/

Hagberg Consulting Group (2002). *Corporate culture/organisational culture: understanding and assessment* [online]. [cited 25 January 2003] Available from Internet: URL http://www.hcgnet.com/html/articles/understanding-Culture.html

Hall, J. (July 25, 2001). *Selling security to management.* [online]. [cited 17 March 2002] Available from Internet: URL http://rr.sans.org/aware/selling_sec.php

Handy, C. (1978). *Gods of management – changing the work of organizations.* New York : Oxford University Press.

Hare, C. (2004). *Policy development.* Information security management handbook – fifth edition. Boca Raton, London, New York, Washington D.C. : Auerbach Publishers.

Harrison, R. (1993). *Diagnosing Organizational Culture – Trainer's Manual.* San Diego : Pfeiffer & Company.

Hellriegel, D., Jackson, S.E., Slocum, J., Staude, G., Amos, T., Klopper, H.B., Louw, L. and Oosthuizen, T. (2004). *Management – second South African edition.* Cape Town, South Africa : Oxford University Press Southern Africa

Hellriegel, D., Jackson, S.E. and Slocum, J.W. (2002). *Management: a competency-based approach.* Cincinnati, Ohio : South-Western Thomson Learning

Henry, K. (2004). *The human side of information security.* Information security management handbook – fifth edition. Boca Raton, London, New York, Washington D.C. : Auerbach Publishers.

Kilmann, R.H. (1985). Corporate culture. *Psychology Today,* pp. 62-69.

Kilmann, R.H., Saxton, M.J., Serpa, R. & Associates (1985). *Gaining control of the corporate culture.* San Francisco, California, United States of America : Jossey-Bass Publishers.

King Report (2001). *King committee on corporate governance - King report on corporate governance for South Africa 2001.* [online]. [cited 3 March 2002] Available from Internet: URL http://www.iodsa.co.za/IoD%20Draft%20King%20Report.pdf

Krige, W. (1999). *The usage of audit logs for effective information security management.* Unpublished master's thesis. Port Elizabeth Technikon, Port Elizabeth, South Africa.

Malekzadeh, A.R. & Nahavandi, A. (1990). Making mergers work by managing cultures. *The Journal of Business Strategy*, May/June, pp. 55-57.

Martin, J. & Siehl, C. (1983). Organizational culture and counterculture: an uneasy symbiosis. *Organizational Dynamics,* Vol 12, No. 2, pp. 52-64.

Martins, A. & Eloff, J. (2002). *Information security culture*. IFIP TC11, 17th International Conference on Information Security (SEC2002), Ain Shams University, Cairo, Egypt, Kluwer Academic Publishers Group, Netherlands.: pp.203-214.

Meek, V.L. (1988). Organizational culture: origins and weaknesses. *Organization Studies*, Vol. 9, No. 4, pp. 453-473.

Miles, R. E. & Snow, C. C. (1978*). Organizational strategy, structure, and process*. New York: McGraw-Hill Book Co

Mitnick, K.D. & Simon, W.L. (2002). *The art of deception – controlling the human element of security.* Indianapolis, Indiana : Wiley Publishing, Inc.

National Institute of Science and Technology Special Publication 800-16 (April, 1998). *Information technology security training requirements: a role- and performance-based model.* Washington D.C. : Superintendent of Documents, U.S. Government Printing Office.

Nonaka, I. (1997, November 11-12). *Organizational knowledge creation.* Knowledge Advantage Conference, San Diego, USA [online]. [cited 25 July 2006] Available from Internet: URL http://www.knowledge-nurture.com/web/bulabdoc.nsf/0/86b566634bc84ea28625662c005c1996/$FILE/nonaka.PDF

Nonaka, I. (1994). A dynamic theory of organizational knowledge creation. *Organization Science*, Vol. 5, No. 1, pp. 14-37.

Oxford Dictionary of Current English (1993). New York City: Oxford University Press.

Planting, S. (2001, March 9). Giving boards a workout - the fish rots from the head. *Future Company* [online]. [cited 27 April 2002] Available from Internet: URL http://www.futurecompany.co.za/2001/03/09/reviewb.htm

PriceWaterhouseCoopers (April, 2006). *Information security breaches survey 2006 executive summary*. [online]. [cited 25 April 2006] Available from Internet: URL http://www.pwc.com/uk/eng/ins-sol/publ/pwc_dti-fullsurveyresults_execsum06.pdf

Quick, J.C. (1992). *Crafting an organizational culture: Herb's hand at Southwest Airlines.* Managing a dynamic organization. New York : American Management Association.

The Quotations Page (2006). Quotation Search [online]. [cited 12 December 2006] Available from Internet: URL http://www.quotationspage.com/search.php3?homesearch=education&startsearch=Search

Robbins, S.P. (1993). *Organizational behavior – concepts controversies and applications*. Englewood Cliffs, New Jersey : Prentice-Hall.

Robiette, A. (February 27, 2001). Why is an information security policy needed? *JISC – Joint Information Systems Committee* [online]. [cited 13 June 2002] Available from Internet: URL http://www.jisc.ac.uk/pub01/security_policy.html#S1

Rowe, A.J., Mason, R.O., Dickel, K.E., Mann, R.B. and Mockler, R.J. (1994). *Strategic management – a methodological approach – fourth edition*. Reading, Massachusetts : Addison-Wesley Publishing Company

Sathe, V. (1983). Implications of corporate culture: A manager's guide to action. *Organizational Dynamics*, pp. 5-25.

Schafer, M. (February 2003). The human-capital balancing act. *Optimize Magazine: issue 16* [online]. [cited 27 February 2003] Available from Internet: URL http://www.optimizemag.com/issue/016/culture.htm

Schein, E.H. (1999). *The corporate culture survival guide.* San Francisco, California, United States of America : Jossey-Bass Publishers.

Schein, E.H. (1992). Organisational leadership and culture. [online]. [cited 12 January 2004] Available from Internet: URL http://www.tnellen.com/ted/tc/schein.html

Schein, E.H. (February, 1990). Organizational culture. *American psychologist*, Vol 45, No. 2, pp. 109-119.

Schwartz, H and Davis, S.M. (1981). Matching corporate culture and business strategy. *Organizational Dynamics*, pp. 30-48.

Sharp, D.E. (2004). *Information security in the enterprise.* Information security management handbook – fifth edition. Boca Raton, London, New York, Washington D.C. : Auerbach Publishers.

Shaurette, K.M. (2004). *The building blocks of information security.* Information security management handbook – fifth edition. Boca Raton, London, New York, Washington D.C. : Auerbach Publishers.

Shorten, B. (2004). *Information security policies from the ground up.* Information security management handbook – fifth edition. Boca Raton, London, New York, Washington D.C. : Auerbach Publishers.

Tan, V.S.L. (2001). *Changing corporate culture* [online]. [cited 4 December 2005] Available from Internet: URL http://adtimes.nstp.com.my/jobstory/2001/sept22c.htm

Thomson, K.L. & von Solms, R. (2005). Information security obedience: a definition. *Computers & Security*, Vol. 24, pp 69-75.

Thomson, K.L. & von Solms, R. (2004). *Towards corporate information security obedience*. IFIP/SEC 2004, Toulouse, France.

von Krogh, G. (1998). Care in knowledge creation. *California Management Review*, Vol 40 No. 3, pp. 133-153.

Whitman, M.E. & Mattord, H.J. (2003). *Principles of Information Security*. Kennesaw State University : Thomson Course Technology.

Zylt (2001). [online]. [cited 4 January 2002] Available from Internet: URL http://www.zylt.com

APPENDICES: Papers Presented and Published

The following papers were presented and published whilst conducting research towards this thesis:

Appendix A:

Paper 1

In 2004, Thomson, K-L, & von Solms, R, *"Towards corporate information security obedience"*, IFIP/SEC 2004, Toulouse, France.

Appendix B:

Paper 2

In 2004, Thomson, K-L, & von Solms, R, *"Cultivating corporate information security obedience"*, Information Security of South Africa (ISSA) 2004, Johannesburg, South Africa.

Appendix C:

Paper 3

In 2005, Thomson, K-L & von Solms, R, *"Information security obedience: a definition"*, was published in *Computers & Security*, Volume 24, pages 69-75.

Appendix D:

Paper 4

In 2006, Thomson, K-L & von Solms, R, "*Towards an information security competence maturity model*", was published in *Computer Fraud & Security*, Volume 2006, Issue 5, pages 11-15.

Appendix E:

Paper 5

In 2006, Thomson, K-L, von Solms, R & Louw, L, *"Cultivating an organisational information security culture"*, published in *Computer Fraud & Security*, Volume 2006, Issue 10, pages 7 – 11.

Appendix A

TOWARDS CORPORATE INFORMATION SECURITY OBEDIENCE

Kerry-Lynn Thomson and Rossouw von Solms
Port Elizabeth Technikon, South Africa; kthomson@petech.ac.za;
rossouw@petech.ac.za

Abstract: All organisations possess a corporate culture, whether they are aware of it or not. This culture determines, to a large extent, the effectiveness of an organisation and the behaviour of employees within an organisation. As part of its corporate governance duties, senior management is responsible for the protection of the assets of its organisation. And as information is a vital asset to most organisations, senior management is ultimately responsible for the protection of information assets. An ideal corporate culture, in terms of information security, would be one where the second-nature behaviour of employees, determined by the culture, is to protect information assets. This paper will provide initial guidelines as to how to establish this culture by examining Schein's model and by investigating how to start implementing Corporate Information Security Obedience.

Key words: Information Security; Corporate Governance; Corporate Culture; Goal Consensus; Corporate Information Security Obedience.

Appendix A

1. Introduction

Information is a vital asset and it is often described as the lifeblood of organisations (Gordon, 2002, online). It is, however, difficult to measure the exact value of the information that an organisation possesses. Still, it is evident that any breach in the confidentiality, integrity or availability of information could result in devastating consequences for an organisation (Gordon and Glickson LLC, 2001, online). Information security practices, together with other physical and technological means, therefore, need to be implemented and managed within the organisation to ensure that the information is kept safe and secure (Krige, 1999, p 7).

As information is a fundamental organisational asset, its security must be integrated into the organisation's overall management plan (Lane, 1985, pp 2-3; Smith, 1989, p 193). This plan should be guided by good corporate governance practices. Corporate governance is one of the significant issues in business at present. Corporate governance is there to endorse the competent use of resources and to involve accountability for the management of those resources (Gaines, 2002, online; World Bank Group, 1999, online).

Senior management, as part of its corporate governance duties, should encourage employees to adhere to the behaviour specified by senior management to contribute towards a successful organisation. Senior management should preferably not autocratically enforce this behaviour, but encourage it as naturally as possible, resulting in the correct behaviour becoming part of the corporate culture. Corporate culture is the outcome of all the collective, taken-for-granted assumptions that a group has learned throughout history. It is the residue of success (Schein, 1999, p 29).

The purpose of this paper is to detail the ideal corporate culture that should exist for it to be effective in protecting information. The paper initially investigates the role senior management should play in protecting information assets and how the creation and execution of the Corporate Information Security Policy could play a part in cultivating an information security conscious culture. The emphasis of this paper is to start investigating how to implement Corporate Information Security Obedience through expanding Schein's model of corporate culture into a two-dimensional model representing both management and employee dimensions.

2. Managing an organisation

Corporate governance is extremely important for managing the operation of organisations. Senior management, through effective corporate governance practices, must lead its organisation through 'direction giving' and strategy implementation (Planting, 2001, online). In order to implement this management strategy, the King Report recommends that four central pillars of corporate governance are visible in an

organisation, namely; accountability, responsibility, fairness and transparency (2001, p 17).

Accountability provides assurance that individuals and groups in an organisation are accountable for the decisions and actions that they take (King Report, 2001, p 14). The pillar of *responsibility* indicates that corrective action should be taken against negligence and misconduct (King Report, 2001, p 14). The third pillar, *fairness*, attempts to ensure that there is a balance in an organisation, in terms of the recognition various parties should receive. The final pillar, *transparency*, is the measure of how effective management is at making necessary information available in an open, precise and timely manner (King Report, 2001, pp. 13-14). These four pillars contribute to the overall goal of proper corporate governance.

Through effective corporate governance, senior management is accountable and responsible for the wellbeing of its organisation and must ensure that the assets of its organisation are well protected. One such asset is information, and, therefore, it is the responsibility of senior management to protect the information assets of its organisation (King Report, 2001, p 17; Deloitte & Touche, 2002, online). Another responsibility of senior management is to cultivate and shape the corporate culture of its organisation.

3. Corporate culture

Organisations develop cultures whether they want to or not. The culture of an organisation operates at both a conscious and unconscious level and if management does not understand the culture in its organisation, it could prove to be fatal in today's business world (Hagberg Consulting Group, 2002, online). Edgar H. Schein defines three levels of culture.

The three levels of corporate culture

One of the problems when trying to understand culture is to oversimplify this complex field. Culture exists at several levels, which range from the very visible to the tacit and invisible. Furthermore, it is imperative that these levels are managed and understood (Schein, 1999, p 15).

The first level of corporate culture is the *Artifacts Level.* This is probably the easiest level to observe as it consists of the visible behaviour of individuals (Hagberg Consulting Group, 2002, online; Schein, 1999, p 15). At this level, it is still not clear as to why employees of an organisation behave in this way and why each organisation is constructed as it is (Schein, 1999, p 16). This leads to an investigation of the second level of culture. The *Espoused Values Level* of corporate culture is the level where the values an organisation is promoting are outlined in the organisation's policies (Schein, 1999, p 17).

There could be a few noticeable inconsistencies between some of the *Espoused Values* or goals of an organisation and the visible behaviour of individuals as seen at the *Artifacts Level*. These inconsistencies indicate that a deeper level of thought is driving the obvious behaviour of the employees (Schein, 1999, p 18). To truly understand the visible behaviour and culture of an organisation, the *Shared Tacit Assumptions Level* of culture must be understood (Schein, 1999, pp 18-19).

This *Shared Tacit Assumptions Level* represents the core of corporate culture. This core is the mutually learned beliefs and assumptions that become taken for granted as the organisation continues to be successful. The beliefs and values found at this level are second-nature to employees and influence the decisions and actions that they take (Schein, 1999, p 21). The corporate culture of an organisation should assist senior management in enforcing and ensuring good information security practices. Together with corporate culture, good corporate governance practices are essential for successful information security.

4. Information security and corporate governance

Information security transcends many facets of an organisation and is one of the most significant policy and structure decisions in an organisation (Spafford, 1998, online). It is becoming progressively more obvious that access to correct information at the right time is imperative to gaining competitive advantage or simply remaining in business (PriceWaterhouseCoopers, 2002, p 1). Policies and procedures are the responsibility of senior management as part of their corporate governance duties. Therefore, it follows that senior management should be responsible for setting strategic direction regarding the protection of information. One of the ways for management to express its commitment to information security in its organisation is to provide support towards a documented Corporate Information Security Policy, as it is one of the controls considered common best practice in terms of information security (BS 7799-1, 1999, p 4).

5. Corporate information security policy

The Corporate Information Security Policy is a direction-giving document and should define the objectives and boundaries of the information security program. The main aim of any policy is to influence and determine decisions, actions and other issues, by specifying what behaviour is acceptable and what behaviour is unacceptable. The behaviour and actions of employees often represents the weakest link in the information security process (Martins & Eloff, 2002, p 203). Policies and procedures are, therefore, organisational laws that determine acceptable and unacceptable conduct within the context of corporate culture (Whitman & Mattord, 2003, p 194). Additionally, it should indicate management's commitment and support for information security and should describe the role that the policy plays in reaching the organisation's vision (Höne, 2003, CD-ROM; BS 7799-1, 1999, p 5). The correct behaviour, as envisioned in the Corporate

Information Security Policy, should become second-nature to employees and the corporate culture should adapt to reflect this.

6. The need to change the corporate culture

The acceptable actions and behaviour of employees towards information as outlined in the Corporate Information Security Policy should become the behaviour that employees demonstrate in their daily activities. Physical and technical controls are tangible controls that attempt to enforce compliance with information security practices and procedures in an organisation, but it is really operational controls and the resulting behaviour and actions of the employees and the processes they use that can sustain information security practices (Deloitte & Touche, 2002, online). As seen previously, the corporate culture of an organisation largely determines the behaviour of employees. Therefore, for the acceptable behaviour to become the *de facto* behaviour of employees, the corporate culture must be changed.

Apprehension arises when there is the prospect of a big change in the environment that employees know so well (Drennan, 1992, p 9). The power to change corporate culture lies principally in the hands of senior management and transforming the culture takes vision, commitment and determination. Without this combination it will not happen, and it certainly will not last (Drennan, 1992, p 3-4). Employees of an organisation may be coerced into changing their obvious behaviour, but this behavioural change will not become established until the deepest level of culture, the *Shared Tacit Assumptions Level*, experiences a transformation (Schein, 1999, p 26).

A new corporate culture cannot simply be 'created'. Senior management can demand or encourage a new way of working and thinking, management can monitor the changes to make sure that they are done, but employees of the organisation will not internalise the changes and make it part of the new culture unless they understand the benefit of these changes. It is senior management's responsibility to highlight that the changes needed in the current culture are worthwhile and important (Schein, 1999, p 187). Senior management, through effective corporate governance practices, must ensure that the policies of the organisation are in line with the vision for the organisation. Senior management should then enforce these policies so that they become part of the way things are done in the organisation and ensure that employees understand the benefits to their organisation. However, it is not enough for senior management to only enforce its policies - it is important for the attitudes of senior management to encourage this change in the corporate culture. If nothing changes in the procedures of the organisation or the attitudes of its management, employee attitudes will not change either (Drennan, 1992, p 3).

7. Organisational environments

There are three key environments that could exist in organisations. These environments dictate how the organisation is run and how employees react in certain circumstances. These environments are Coercive, Utilitarian and Goal Consensus (Schein, 1992, online).

The Coercive Environment is one where employees feel alienated in their environment and seek to leave this environment if possible. Peer relationships in this environment develop in defence of the authority in the organisation, in other words, senior management. These employees perform tasks because they must, rather than because they agree with the actions and decisions of senior management (Schein, 1992, online). The Utilitarian Environment is one where employees participate in their organisation by evolving workgroups based on an incentive system. In this environment employees will do as senior management wishes because of the rewards that they will receive. They still do not necessarily agree with senior management (Schein, 1992, online).

Figure 1 illustrates the Coercive and Utilitarian Environments mapped onto Schein's model of corporate culture. It shows that, in the Coercive and Utilitarian Environments, the *Artifacts Level* of both management and employees are in concurrence with one another. In the Coercive Environment this indicates that there is stringent management control and employees adhere to the behaviour specified by management, or else harsh corrective action will be taken against them. In the Utilitarian Environment this concurrence indicates that employees will do as management wishes in return for a reward. As indicated in the Figure, the *Shared Tacit Assumptions Level* in both environments is not in line at all – the beliefs and values of management and employees are not the same. Without either strict management or incentives, the correct behaviour of employees would fade.

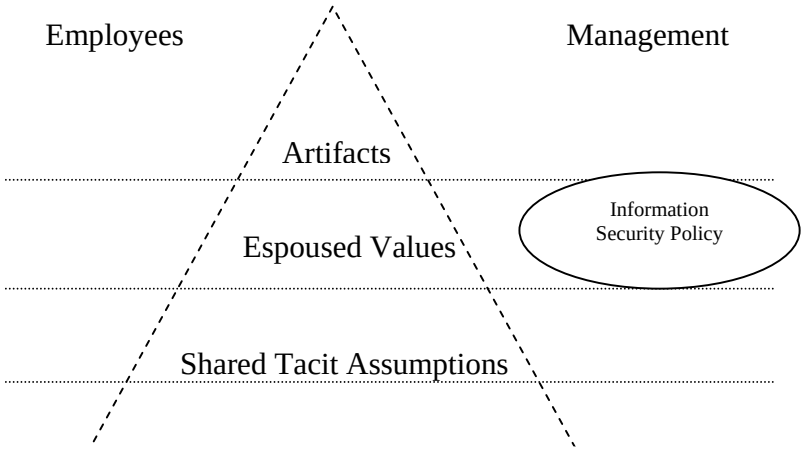

Figure 1. **The coercive and utilitarian environments and Schein's model**

Appendix A

In Figure 1 the Information Security Policy is found at the *Espoused Values Level* of Schein's model and found on the Management side. This indicates that the contents of the policy are in agreement with what management wishes, but not at all in line with the beliefs and values of the employees. It is vital that employees are in agreement with their work policies, as it is indicated that productivity and performance will increase by 30% to 40% if employees are satisfied with the policies (Schafer, 2003, online). Consequently, employees should be satisfied with the Corporate Information Security Policy. If the Information Security Policy is not discussed, supported and evaluated by management and employees, the Policy may remain a 'piece of paper' (Canadian Labour Program, 2003, online).

The third organisational environment, the Goal Consensus Environment, is one where employees are morally involved with the organisation. They identify with the organisation and share the same beliefs and values of senior management and they are striving towards the vision of senior management. In this environment, employees' actions are not as a result of being forced to do so or because of a reward, but because they are in agreement with the way things are done in the organisation (Schein, 1992, online). This Goal Consensus Environment could be seen as a corporate culture which is in line with the vision of senior management. This would mean that 'right' decisions and actions of employees become second-nature and part of their culture (Schein, 1999, p 15-17).

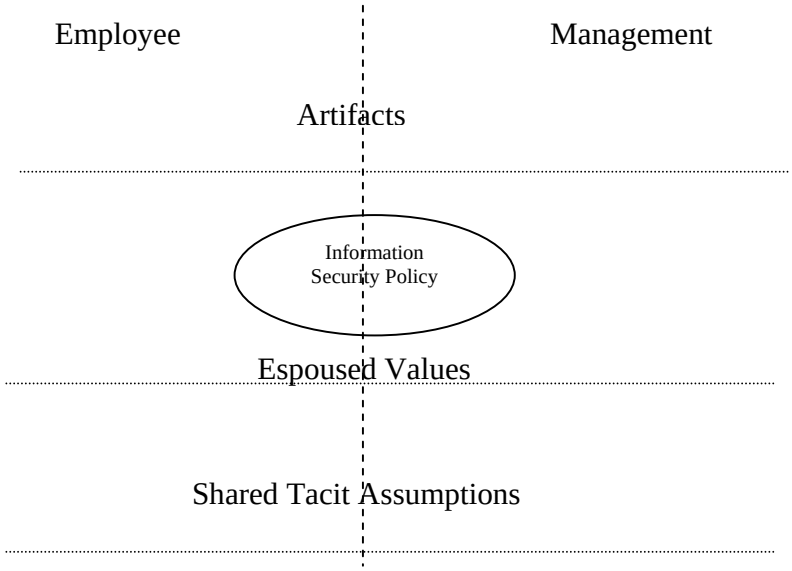

Figure 2. **The goal consensus environment and Schein's model**

Figure 2 illustrates that in the Goal Consensus Environment, all three levels of corporate culture in Schein's model are in agreement. This is an ideal corporate culture, in terms of information security, as the information security vision expressed at the *Espoused Values*

Level by senior management is supported by the actions and behaviour of employees at the *Artifacts Level*. This level is determined by the *Shared Tacit Assumptions Level* of corporate culture. In the Figure, the Corporate Information Security Policy is found at the intersection of management and employees. This indicates that the beliefs and values of the employees are in agreement with senior management's vision for information security. This would indicate that Corporate Information Security Obedience has been implemented in this organisational environment (Thomson & von Solms, 2003, p 107).

8. Implementing corporate information security obedience

As seen previously, corporate culture is the residue of success. In other words, it is the set of procedures that senior management and employees of an organisation follow in order to be successful. For information security practices to be successful, it is important for Corporate Information Security Obedience to be implemented in an organisation.

By implementing Information Security Obedience, the *de facto* behaviour of employees towards information security should be the correct behaviour outlined in the Information Security Policy. In order to do this, the *Espoused Values* and *Shared Tacit Assumptions Level* of Schein's model must be addressed. Senior management must have a very clear vision as to what correct behaviour is in terms of information security. Management should then analyse its current corporate culture and identify the cultural elements that need to change (Spotlight, 2002, online). The *Espoused Values Level* is where the organisational policies, including the Corporate Information Security Policy, of an organisation are created by senior management. In order for Information Security Obedience to be implemented, the Information Security Policy contents must be drafted and communicated in a way that is acceptable in terms of the employees' beliefs and values. One way to do this is to involve employees in decision-making processes, taking into account employee welfare. If employees do not agree with the Corporate Information Security Policy or do not understand the benefits of the change in behaviour they will not adhere to the correct behaviour (Goal/QPC, 2003, online).

Correct behaviour should be encouraged and displayed by senior management, which will, to a large extent, shape the corporate culture (Hagberg Consulting Group, 2002, online). If this new, correct behaviour is an improvement on the current behaviour it should begin to influence the beliefs and values of employees found at the *Shared Tacit Assumptions Level*. This in turn should begin to shape the corporate culture (Schein, 1999, p 23). This would mean that the *Espoused Values Level* and the associated Information Security Policy is in line with the *Shared Tacit Assumptions Level* of employees and Corporate Information Security Obedience has been achieved.

9. Conclusion

Information is a vital asset in most organisations and as such should be well protected through effective information security practices. One of the problems facing the protection of information is the actions and behaviour of the employees in an organisation. If correct information security practices could become second-nature to employees and part of the way they conduct their daily activities, it would, to a large extent, eliminate this problem. This would assist in the creation of an environment of Corporate Information Security Obedience, where the information security procedures outlined by senior management in the Corporate Information Security Policy is the behaviour displayed by employees.

In order to implement Information Security Obedience the beliefs and values of employees, in terms of information security, must be addressed at the root level of *Shared Tacit Assumptions*. This level must be aligned with the contents of the Corporate Information Security Policy found at the *Espoused Values Level*. If these two levels are in concurrence with one another, it will mean that the information security practices employed by employees is the same as the correct information security practices outlined at the *Espoused Values Level*. This paper has outlined the reason that Corporate Information Security Obedience is necessary for employees to fully understand the role they must play in information security in their organisation. This should, to a large extent, eradicate the incorrect information security practices performed by employees and further research will continue to investigate the action that should be taken to firmly entrench correct information security practices in an organisation through Corporate Information Security Obedience.

At present, the concept of implementing Corporate Information Security Obedience is being researched. Therefore, there are no further recommendations on how to accomplish this implementation included in this paper. These recommendations will form part of further research.

References

BS 7799-1. (1999). *Code of practice for information security management (CoP).* DISC PD 0007. UK.

Canadian Labour Program. (2003). Work-life balance in Canadian workplaces. *[online]. [cited 20 February 2004] Available from Internet: URL http://labour.hrdc-drhc.gc.ca/worklife/moving-beyond-policies-en.cfm*

Deloitte & Touche. (May, 2002). *Management briefing – information security*. [online]. [cited 13 January 2003] Available from Internet: URL http://www.deloitte.com/dtt/cda/doc/content/info_security(1).pdf

Drennan, D. (1992). *Transforming company culture.* Berkshire, England : MacGraw-Hill.

Gaines, C. (2002, April 22). The benefits of the BS7799 certification with particular reference to e-commerce applications. *IT Security* [online]. [cited 4 August 2002] Available from Internet: URL http://www.itsecurity.com/papers/insight1.htm

Goal/QPC (2003). Journal of innovative management [online]. [cited 4 February 2004] Available from Internet: URL http://www.goalqpc.com/2003/Journalfiles/currentissue.htm

Gordon, G. (May 12, 2002). Dozens of threats beset your data. *Sunday Times, Business Surveys* [online]. [cited 17 July 2002] Available from Internet: URL http://www.suntimes.co.za/2002/05/12/business/surveys/internet/survey10.asp

Gordon and Glickson LLC. (2001). *Comprehensive information security policies: meeting an organisation's privacy and security needs.* [online]. [cited 23 March 2003] Available from Internet: http://www.ggtech.com/

Hagberg Consulting Group (2002). *Corporate culture/organisational culture: understanding and assessment* [online]. [cited 25 January 2003] Available from Internet: URL http://www.hcgnet.com/html/articles/understanding-Culture.html

Höne, K. (2003). *Abstract of 'effective information security policies – the why, what and how'.* [CD-ROM]. South Africa: ISSA 2003.

King Committee on Corporate Governance. (2001). *King report on corporate governance for South Africa 2001.* [online]. [cited 3 March 2002] Available from Internet: URL http://www.iodsa.co.za/IoD%20Draft%20King%20Report.pdf

Krige, W. (1999). *The usage of audit logs for effective information security management.* Unpublished master's thesis. Port Elizabeth Technikon, Port Elizabeth, South Africa.

Lane, V.P. (1985). *Security of computer based information systems.* London: Macmillan.

Martins, A. & Eloff, J. (2002). *Information Security Culture.* IFIP TC11, 17th International Conference on Information Security, Ain Shams University, Cairo, Egypt, Kluwer Academic Publishers Group.

Planting, S. (2001, March 9). Giving boards a workout - the fish rots from the head. *Future Organisation* [online]. [cited 27 April 2002] Available from Internet: URL http://www.futureorganisation.co.za/2001/03/09/reviewb.htm

PriceWaterhouseCoopers (2002). *Information security breaches survey technical report.* [online]. [cited 5 January 2003] Available from Internet: URL http://www.security-survey.co.uk

Schafer, M. (February 2003). The human-capital balancing act. *Optimize Magazine: issue 16* [online]. [cited 13 February 2003] Available from Internet: URL http://www.optimizemag.com/issue/016/culture.htm

Schein, E.H. (1999). *The corporate culture survival guide.* San Francisco, California, United States of America : Jossey-Bass Publishers.

Schein, E.H. (1992). Organisational leadership and culture. [online]. [cited 12 January 2004] Available from Internet: URL http://www.tnellen.com/ted/tc/schein.html

Smith, M.R. (1989). *Commonsense computer security*. London: McGraw-Hill.

Spafford, E.H. (1998). It's about more than computers. *CERIAS* [online]. [cited 12 February 2003] Available from Internet: URL http://www.cerias.purdue.edu/training_and_awarness/products/brochure_001.pdf

Spotlight (2002). *Schein interview.* [online]. [cited on 12 February 2004] Available from Internet: URL http://www.boys-camp-southafrica.de/files/Edgar%20Schein.pdf

Thomson, K-L & von Solms, R. (2003). *Integrating information security into corporate culture.* Unpublished master's thesis. Port Elizabeth Technikon, Port Elizabeth, South Africa.

Whitman, M.E. & Mattord, H.J. (2003). *Principles of Information Security*. Kennesaw State University : Thomson Course Technology.

World Bank Group. (September 20, 1999). *Corporate governance: a framework for implementation – overview*. [online]. [cited 23 December 2002] Available from Internet: URL http://www.worldbank.org/html/fpd/privatesector/cg/docs/gcgfbooklet.pdf

Appendix B

CULTIVATING CORPORATE INFORMATION SECURITY OBEDIENCE

Kerry-Lynn Thomson[a] and Rossouw von Solms[b]

[a]Port Elizabeth Technikon, South Africa

[b]Port Elizabeth Technikon, South Africa

[a]kthomson@petech.ac.za, (041) 504 3408, Department of Information Technology, PE Technikon, Private Bag X6011, Port Elizabeth 6000

[b]rossouw@petech.ac.za, (041) 504 3604, Department of Information Technology, PE Technikon, Private Bag X6011, Port Elizabeth 6000

ABSTRACT

One of the most prevalent problems with regard to protecting information assets is the behaviour of employees. Moreover, the behaviour of employees is, to a large extent, determined by the corporate culture of an organisation. Senior management, as part of its corporate governance responsibilities, must define a vision for information security in its organisation. An ideal corporate culture, in terms of information security, would be one where the *de facto* behaviour of employees is to satisfactorily protect information assets. This paper will expand Schein's corporate culture model into two dimensions, detailing both management and employee's behaviour in terms of information security and the three levels of corporate culture. A diagram detailing the Driving and Restraining Forces involved in the process of culture change will be detailed and the paper will conclude by investigating the Force Field Analysis process.

KEY WORDS

Corporate Information Security Obedience; Information Security; Corporate Culture; Force Field Analysis

Appendix B

CULTIVATING CORPORATE INFORMATION SECURITY OBEDIENCE

1. Introduction

In order to adequately protect the information assets of an organisation it is vital for Corporate Information Security Obedience to be implemented in the organisation. As part of Information Security Obedience, senior management must define the vision for information security in their organisation. In addition, the *de facto*, or second-nature, behaviour of employees must adhere to the behaviour necessary to adequately protect the information assets of an organisation.

This paper will outline the importance of corporate culture and the Corporate Information Security Policy, which should influence it. Edgar Schein's corporate culture model will be examined and it will be investigated how to expand this into a two-dimensional model to create an environment in which Information Security Obedience can be implemented. The paper will conclude by investigating Force Field Analysis and the Force Field Diagram, in an attempt to begin the transformation of the corporate culture.

2. Corporate culture

Every organisation has a corporate culture which, to a large extent, determines the behaviour of employees. Employees' behaviour is affected by culture as it defines what behaviour is acceptable and what is unacceptable (Beach, 1993, p 17). And, very often, the behaviour and actions of employees and the information security processes they use in their daily work represents the weakest link in the information security process. A disturbing fact, though, is that it is estimated that only 5% of organisations have a definable culture, where the senior management takes an active role in the shaping of the corporate culture (Atkinson, 1997, p 17). Therefore, only in a minority of organisations is senior management active in positively influencing the behaviour of employees.

Corporate culture effects organisations in two crucial ways. The first is through legislation and, second, through its own decision making. The effects of legislation on an organisation are direct and can be identified. Legislation represents the culture of a country, by defining what can and what cannot be done. Consequently, an organisation must adhere to the legislation that affects it; otherwise legal action could be taken against it. Not adhering to this legislation would have a direct and visible consequence for the organisation. However, the effects of corporate culture on an organisation's decision making are indirect and invisible and can be difficult to assess. Matters of culture are elusive and difficult to pin down, but no less important than legislation issues (Policy Studies Institute, 1999, online).

Edgar Schein defines three levels of culture to describe this complex field and it is vital for these levels to be managed and understood by senior management (1999, p 15). The first level of corporate culture is the Artifacts level and consists of the visible and obvious behaviour of individuals (Hagberg Consulting Group, 2002, online; Schein, 1999, p 15). At this level, it is still not clear as to why employees of an organisation behave in this way. Therefore, it is necessary to investigate the second level of culture; the Espoused Values level (Schein, 1999, p 16). The Espoused Values level of corporate culture is the level where the vision and values an organisation is promoting are found. The vision and values and the resulting necessary behaviour of employees to achieve this vision, are outlined in management's policies at this level (Schein, 1999, p 17).

Therefore, the first two levels of culture describe what can be seen through the visible behaviour and actions of employees, described at the Artifacts level, and what should be seen as a result of the behaviour and actions outlined at the Espoused Values level. There could, however, be a few obvious discrepancies between some of the Espoused Values or goals of an organisation and the visible behaviour of individuals as seen at the Artifacts level. Therefore, in many cases, it is not the contents of management policies that dictate employee behaviour, but it is a deeper level of thought that is driving the obvious behaviour of the employees. To fully understand what is driving the visible behaviour of employees, the Shared Tacit Assumptions level of culture must be understood and appreciated (Schein, 1999, pp 18-19).

This third level of culture, the Shared Tacit Assumptions level, is the heart of corporate culture as it represents the commonly learned values and assumptions of employees that become taken for granted in an organisation. The beliefs and values found at this level are innate to employees and their behaviour in their work environment is directly influenced by these beliefs (Schein, 1999, p 21).

Therefore, in order to change corporate culture, the beliefs found at the Shared Tacit Assumptions level needs to be changed, as these beliefs influence the actions and behaviour of employees. These beliefs would include those that influence employees with regard to information security. One of the key components of an organisation, with regard to information security, is a Corporate Information Security Policy.

3. Corporate information security policy

According to its corporate governance duties, senior management must lead its organisation through 'direction-giving' and strategy implementation. This 'direction-giving' is achieved through the creation and implementation of management policies (Planting, 2001, online; King Report, 2001, p 46). In addition, senior management, as part of their corporate governance duties, is both accountable and responsible for the protection of the assets and reputation of its organisation (King Report, 2001, pp. 45-47). Therefore, one of the main functions of senior management in terms of good corporate governance is to guarantee that policies and procedures are in place in the organisation to

protect its assets. And, as one of the most important assets of any organisation is information, it follows that senior management should be accountable and responsible for information security practices in its organisation.

One of the ways to implement good information security practices in an organisation is to ensure that a detailed Corporate Information Security Policy is in place. The content of the Corporate Information Security Policy is particularly significant as it should outline the behaviour employees should adhere to in order to adequately protect information assets. However, it is extremely important for senior management to realise that the culture of an organisation is not formed by what it, as senior management, preaches or publishes in policies, but what it accepts in practice (Drennan, 1992, p 3). Therefore, if the behaviour of employees is not in line with the behaviour outlined in management policies, but is not corrected by senior management, the 'incorrect' behaviour will continue.

A Corporate Information Security Policy must outline the vision senior management has for the organisation in terms of information security. The Information Security Policy would be found at the Espoused Values level of culture, as it is at this level that the vision and goals are expressed. The Corporate Information Security Policy must work within the organisation where this culture exists and must address the security needs of the specific organisation (Deloitte & Touche, 2002, online). Therefore, each policy must be tailored for each organisation and, although no organisation can guard against all the possible risks related to protecting information, a carefully constructed Information Security Policy can establish the foundation of a corporate culture that is able to lessen many of the threats to information (Gordon and Glickson LLC, 1997, online).

Therefore, the Information Security Policy assists in the creation of an information security conscious corporate culture by specifying what behaviour is acceptable and what behaviour is unacceptable in terms of information security. If the policy is implemented properly in an organisation, it should begin to change the behaviour of employees and consequently the culture and would lead to a state of Corporate Information Security Obedience. However, changing the corporate culture is not an easy task.

4. Changing corporate culture

A new corporate culture cannot be created overnight. Corporate culture is one of the most stable aspects of an organisation as many of the most important facets of culture are essentially invisible, which makes transforming culture very difficult (Schein, 1999, pp. 21-26). Any prospective change in an environment in which employees are comfortable could lead to massive amounts of anxiety and resistance to change. For an organisation's corporate culture to change, it involves the unlearning of beliefs, values and assumptions and a change in attitude (Schein, 1999, p 26). Employees prefer stability in their environment and the traditions that are inherent in this environment are difficult to change. These traditions play a large part in shaping the corporate culture of an organisation (Drennan, 1992, p 9).

Senior management can demand a new way of working and can monitor these coerced modifications to make sure that they are done. However, the power behind any successful culture change is the degree to which the people who have to implement the changes are engaged in the change process (Maset, 2001, online). In an organisation, the people who must implement the changes are both senior management and employees.

Therefore, it is vitally important for both management and employees to be involved with the change process from the beginning. All parties should have input as employees of an organisation will not internalise the changes and make it part of the new culture unless they understand the benefit of these changes, hence the need for them to be involved in creating the change process. It is senior management's responsibility to highlight that the changes needed in the current culture are worthwhile and important and needed to obtain the vision for information security in the organisation (Schein, 1999, p 187).

Vision defines the ideal future. This vision might imply that the current culture be kept the way it is or it might imply the need for change in the organisation. This means that the vision might need nothing more than the natural evolution of the present culture, or it may require drastic changes in what the organisation is doing – and perhaps, therefore, in the organisation's culture (Beach, 1993, p 17). As seen previously, the vision for information security is found at the Espoused Values level of culture.

The behaviour of employees towards information security is influenced by their beliefs and values regarding information, which is found at the Shared Tacit Assumptions level of culture. Employees of an organisation may be coerced into changing their obvious behaviour, but this behavioural change will not become established until this deepest level of culture, the Shared Tacit Assumptions level, experiences a transformation (Schein, 1999, p 26). Therefore, to achieve the vision for information security, the Espoused Values level and the Shared Tacit Assumptions level of culture should be aligned, so that the employees' behaviour at the Artifacts level will support the vision for information security. The following section will show this graphically by expanding Schein's culture model into two dimensions.

5. Expanding Schein's model

There are three types of environments that could be found in organisations. These environments are Coercive, Utilitarian and Goal Consensus. These environments determine how the organisation operates and how employees will react in certain circumstances (Schein, 1992, online).

The Coercive Environment is one where employees perform tasks because they must, rather than because they agree with the actions and decisions of senior management. Peer relationships in this environment develop to protect the employees from the authority in the organisation, namely; senior management (Schein, 1992, online). In the Utilitarian Environment employees will do as senior management wishes

because of an incentive system and not because they necessarily agree with senior management (Schein, 1992, online).

In the Goal Consensus Environment employees identify with the organisation and share the same beliefs and values of senior management and they are willingly striving towards the vision senior management has for information security in the organisation. The employees' actions are not as a result of being forced to do so or because of remuneration, but because they are in agreement with the way things are done in the organisation and their behaviour is second-nature to them (Schein, 1992, online).

Figure 1 illustrates the progression from a Coercive or Utilitarian Environment in 'Culture 1' to a Goal Consensus Environment in 'Culture 3'. The Corporate Information Security Policy is represented by 'A'.

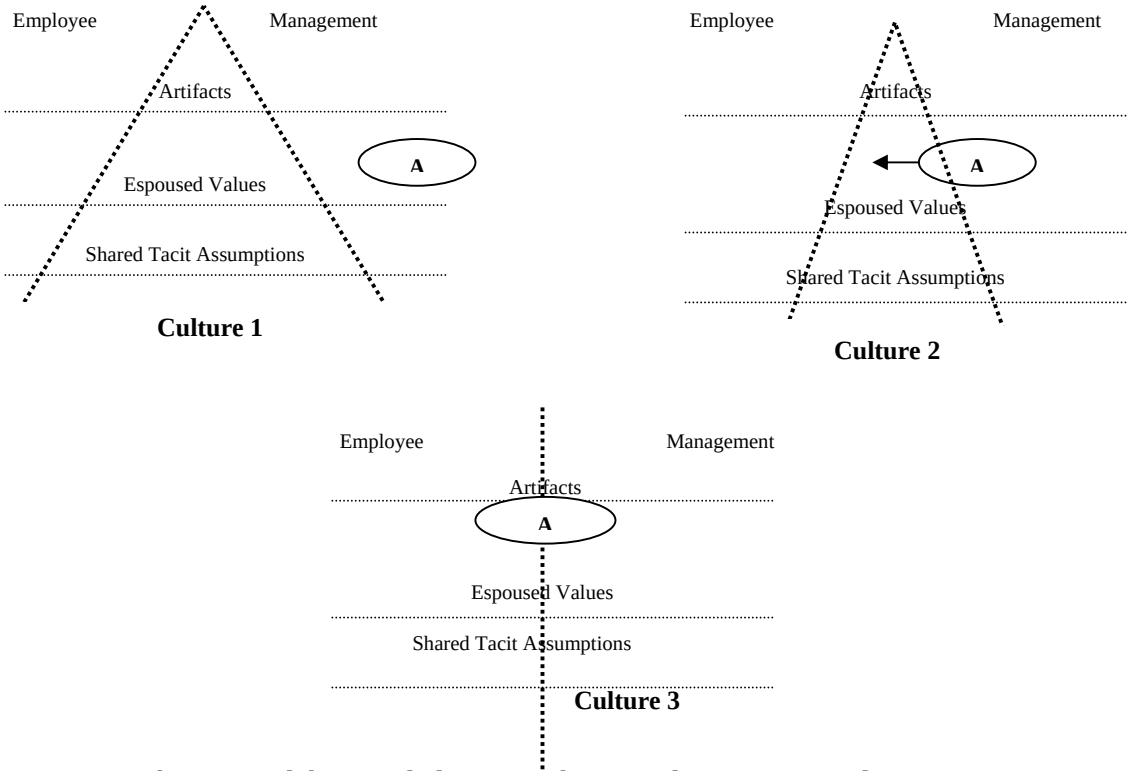

Figure 1: Schein's model expanded into employee and management dimensions

'Culture 1' illustrates that the beliefs and values of employees and management, at the Shared Tacit Assumptions level, are widely varied and not in line with one another. This means that the information security beliefs of employees are not those shared by senior management. However, in 'Culture 1', the information security practices used by employees, visible at the Artifacts level, are in line with the information security

practices used and approved by senior management. This is as a result of the fact that, in both the Coercive and Utilitarian Environments, the Artifacts level of employees and senior management is in line, not as a result of employees agreeing with the policies of senior management, but rather because they are being forced to do so.

In addition, the Information Security Policy in 'Culture 1' is found completely in management's dimension of the culture. This illustrates that the information security beliefs and values of employees are not the same as the information security vision of senior management, as expressed in the Information Security Policy. The alignment of the behaviour of employees and management, with regard to information security practices, would not be possible in the Coercive Environment without stringent management control, or an incentive system in the Utilitarian Environment. Therefore, in order for senior management to ensure that the Artifacts level remains in line with their policies, they must stringently enforce these policies on their reluctant employees. This leads to increasing tension in an organisation.

'Culture 2' illustrates that, as the Corporate Information Security Policy is shifted towards the employee dimension, the 'arms' of the employee and management dimensions move closer together. This represents the fact that the beliefs of employees and management, with regard to information security, are beginning to correlate. In order to shift the Information Security Policy, it is necessary for employees to start understanding the vision senior management has for information security. Employees should now begin to realise the advantage of adequately protecting information security assets and, as a result, their actions do not have to be enforced to such a large extent. This would decrease the tension in the organisation, as employees are beginning to understand the benefit that good information security practices would have for their organisation.

In 'Culture 3' an ideal culture has been achieved. This is where all three levels of Schein's model are in line with one another. The Corporate Information Security Policy has successfully been shifted to be part of both the employee and management dimension in the diagram. In this culture, employees do not need incentives, or are not under threat of severe consequences, to implement correct information security practices. Employees are in agreement with the way things are done in the organisation and acceptable information security practices are second-nature to them (Schein, 1992, online). This is referred to by Schein as a Goal Consensus Environment, as the environment represents a corporate culture where senior management's vision for information security is shared by everyone in the organisation. Everyone is striving towards the same goals. The *de facto* behaviour of employees is, consequently, the behaviour necessary for the organisation to be successful (Schein, 1999, p 15-17).

When all the levels of corporate culture are in line with one another, with regard to information security, as in 'Culture 3', it indicates that Corporate Information Security Obedience has been implemented in this organisational environment (Thomson & von Solms, 2003, p 107). This section described the ideal corporate culture that should exist to adequately protect information assets. A method to begin transformation of the

corporate culture into this ideal culture, adhering to Corporate Information Security Obedience, is described in the subsequent section.

6. Force field analysis

Organisations frequently are unsuccessful in the implementation of change. This implementation is most often hindered by the fact that change initiatives are treated as 'top-down' processes. Senior management attempts to impose change on employees, instead of taking their actions and attitudes into consideration. This 'top-down' approach lacks understanding and the motivation of the employees (Maset, 2001, online). As seen previously, employees will not internalise culture change unless they understand the benefit of this change to their organisation. Therefore, it is extremely important, when implementing culture change, that employees are involved in and understand the process.

One method of change, the Force Field Analysis approach, developed by Kurt Lewin in 1947, would ensure that employees are involved in the implementation of culture change. According to Lewin, any change (whether cultural or not) can be viewed as the effect of Driving and Restraining Forces. In terms of culture, the current corporate culture is the status quo in an organisation. The Driving Forces seek to upset the status quo, while Restraining Forces attempt to preserve the status quo (Pojasek, 2001, p 74).

Senior management must be held accountable for developing and communicating a clear vision of the future. This vision is the reason for change, or the Driving Forces. At the same time, senior management must be aware of the current reality, or Restraining Forces, that inhibits the realisation of the vision (Charlton, 2000, p 42). The Driving Forces are moving the organisation towards change and the Restraining Forces are pushing against change. The actual, resulting change is a consequence of the interaction of these two sets of forces. A Force Field Analysis should result in a Force Field Diagram illustrated in Figure 2.

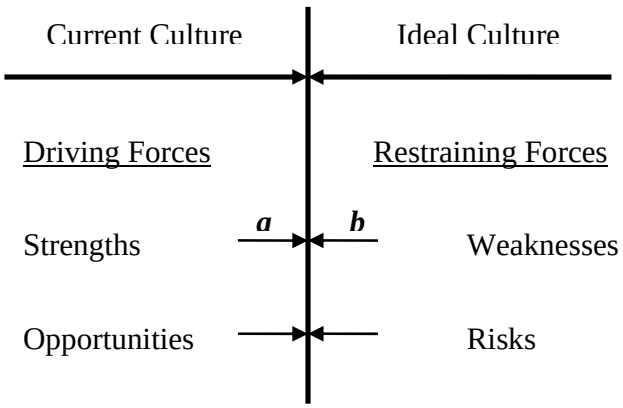

Figure 2: Template for a Force Field Diagram

Appendix B

A Force Field Diagram represents Driving Forces on one side of the diagram, pushing towards the 'Ideal Culture' and the Restraining Forces pushing towards the 'Current Culture'. Each Driving or Restraining Force is represented by a vector or arrow and the length of the vector is equivalent to the strength of the force. Therefore, if two opposing vectors are of equal length, there will be no change. If the Driving Force vector is stronger than the Restraining Force vector, the culture will shift towards the ideal. However, if the Restraining Force vector is stronger than the Driving Force vector, the culture will not change and achieving a culture change will be very difficult. Therefore, by referring to Figure 2, we can conclude the following:

If	a = b	:	Status quo maintained
If	a > b	:	Change towards ideal culture
If	a < b	:	Status quo maintained

Increasing one set of vectors without decreasing the other will, as in physics, increase the tension and conflict in an organisation. It is, therefore, preferable to decrease the Restraining Forces instead of applying greater pressure to the Driving Forces when attempting to change culture in an organisation (Pojasek, 2001, p 75).

a. The process of force field analysis

Force Field Analysis for culture change should begin by describing the current culture, followed by a detailed description of the ideal culture for that organisation. The 'gap' that is identified should be breached by the process of Force Field Analysis. It should also be identified what the impact will be for an organisation if their current culture is not changed (Saferpak, 2000, online).

The next step is for the Restraining Forces, represented diagrammatically by vectors, to be identified and placed on one side of the diagram. Each Restraining Force should then be considered and possible solutions to overcome the effect of the force must be developed. These are the Driving Forces, also represented by vectors, and must be placed on other side of the Force Field Diagram (ACIG, 2000, p 1; Pojasek, 2001, p 75). A numerical value should be assigned to each vector according to its strength.

A Force Field Diagram is a very simple, but powerful, tool that could be used to simplify the complex problem of culture change. In terms of information security, the 'Ideal Culture' to represent in a Force Field Diagram would be one where Corporate Information Security Obedience has been achieved. Those Restraining Forces acting as a barrier to Corporate Information Security Obedience must be identified and the Driving Forces necessary for change must also be identified.

If a Driving Force is imposed on employees by senior management without decreasing or eliminating the opposing Restraining Force, a great deal of tension will

exist between employees and senior management. This could result in a Coercive Environment where it is necessary to compel employees to behave in accordance with correct information security practices, instead of these information security practices becoming part of their intrinsic behaviour. Therefore, the Restraining Forces must be decreased through awareness and understanding to bring about a change that is not forced on employees, which should bring about an environment that would facilitate the change to the 'Ideal Culture'.

7. Conclusion

Protecting information assets is crucial for the successful operation of most organisations. However, one of the major problems facing the protection of information assets, through information security, is the behaviour and actions of employees. Often it is the lack of understanding the importance of the information security processes that lead to 'incorrect' behaviour and actions of employees.

The corporate culture of an organisation largely influences the behaviour of employees within the organisation by defining what behaviour is 'acceptable' and 'unacceptable'. The behaviour of employees, visible at the Artifacts level of culture, is directly influenced by the Shared Tacit Assumptions level of culture. The vision for information security and the resulting 'correct' behaviour necessary to protect information assets should be expressed at the Espoused Values level of culture in the contents of the Corporate Information Security Policy.

If the 'correct' behaviour, outlined in the Information Security Policy, and the actual behaviour of employees does not match, it indicates that the corporate culture of the organisation will have to be changed. To change the corporate culture into one that incorporates Corporate Information Security Obedience, the beliefs and values, found at the Shared Tacit Assumptions level, must be adapted to be in line with the principles found in the Information Security Policy at the Espoused Values level.

One of the methods currently being researched for culture change is Force Field Analysis, resulting in a Force Field Diagram. This diagram simplifies complex change problems into sets of vectors representing Driving and Restraining Forces. By identifying Restraining Forces, and the associated Driving Forces, it clarifies what the exact barriers are for culture change. At present, there is no technique to assign specific values to the vectors in the Force Field Diagram. This, and the adaptation of the Force Field Diagram into one that can be used to facilitate the implementation of Corporate Information Security Obedience, will form part of future research.

8. REFERENCES

ACIG – Australian Continuous Improvement Group (2000). *Force field analysis.* [online]. [cited 24 February 2004] Available from Internet: URL http://www.acig.com.au/library/forcefield.PDF

Atkinson, P. (1997). *Creating culture change – strategies for success*. Bedfordshire, England : Rushmere Wynne.

Beach, L.R. (1993). Making the right decision. Organizational culture, vision and planning. Eaglewood Cliffs, New Jersey : Prentice Hall.

Canadian Labour Program. (2003). Work-life balance in Canadian workplaces. *[online]. [cited 20 February 2004] Available from Internet: URL http://labour.hrdc-drhc.gc.ca/worklife/moving-beyond-policies-en.cfm*

Charlton, G. (2000). *Human habits of highly effective organisations.* Pretoria, South Africa : Van Schaik Publishers.

Deloitte & Touche. (May, 2002). *Management briefing – information security*. [online]. [cited 13 January 2003] Available from Internet: URL http://www.deloitte.com/dtt/cda/doc/content/info_security(1).pdf

Drennan, D. (1992). *Transforming company culture.* Berkshire, England : MacGraw-Hill.

Gordon and Glickson LLC. (1997). *Information technology today is fraught with risks, and missteps can be costly.* [online]. [cited 23 March 2003] Available from Internet: URL http://www.ggtech.com/

King Committee on Corporate Governance. (2001). *King report on corporate governance for South Africa 2001*. [online]. [cited 3 March 2002] Available from Internet: URL http://www.iodsa.co.za/IoD%20Draft%20King%20Report.pdf

Maset (2001). *Change the culture – by engaging the workforce*. [online]. [cited 17 February 2004] Available from Internet: URL http://www.masetllc.com/products/425.shtml

Planting, S. (2001, March 9). Giving boards a workout - the fish rots from the head. *Future Organisation* [online]. [cited 27 April 2002] Available from Internet: URL http://www.futureorganisation.co.za/2001/03/09/reviewb.htm

Pojasek, R.B. (2001). *To change the culture, you must first master the force.* [online]. [cited 22 January 2004] Available from Internet: URL http://www.pojasek-associates.com/Reprints/Master_the_Force.pdf

Policy Studies Institute (1999). *Industrial and financial culture.* [online]. [cited 23 March 2003] Available from Internet: URL http://www.psi.org.uk/publications/archivepdfs/Innovation%20and%20Indust/IISB2.pdf

Saferpak (2000). To carry out force field analysis. [online]. [cited 23 March 2004] Available from Internet: URL http://www.saferpak.com/force_field.htm

Schafer, M. (February 2003). The human-capital balancing act. *Optimize Magazine: issue 16* [online]. [cited 27 February 2003] Available from Internet: URL http://www.optimizemag.com/issue/016/culture.htm

Schein, E.H. (1999). *The corporate culture survival guide.* San Francisco, California, United States of America : Jossey-Bass Publishers.

Schein, E.H. (1992). Organisational leadership and culture. [online]. [cited 12 January 2004] Available from Internet: URL http://www.tnellen.com/ted/tc/schein.html

Thomson, K-L & von Solms, R. (2003). *Integrating information security into corporate culture.* Unpublished master's thesis. Port Elizabeth Technikon, Port Elizabeth, South Africa.

Appendix C

INFORMATION SECURITY OBEDIENCE: A DEFINITION

Kerry-Lynn Thomson[a] and Rossouw von Solms[b]

[a]Port Elizabeth Technikon, South Africa
[b]Port Elizabeth Technikon, South Africa

[a]kthomson@petech.ac.za, Department of Information Technology, PE Technikon, Private Bag X6011, Port Elizabeth 6000
[b]rossouw@petech.ac.za, Department of Information Technology, PE Technikon, Private Bag X6011, Port Elizabeth 6000

Abstract

Information is a fundamental asset within any organisation and the protection of this asset, through a process of information security, is of equal importance. This paper examines the relationships that exist between the fields of corporate governance, information security and corporate culture. It highlights the role that senior management should play in cultivating an information security conscious culture in their organisation, for the benefit of the organisation, senior management and the users of information.

Key Words

Corporate Governance, Information Security, Corporate Culture, Information Security Obedience

Appendix C

INFORMATION SECURITY OBEDIENCE: A DEFINITION

1. INTRODUCTION

Information is important. It is often depicted as the lifeblood of the growing electronic economy (Gordon, 2002, online). Commercial organisations and governments rely heavily on information to conduct their daily activities. Therefore, the security of information needs to be managed and controlled properly (Lane, 1985, pp 2-3; Smith, 1989, p 193). No matter what the information involves; whether it is customer records or confidential documentation, there are many threats that make information vulnerable (Gordon, 2002, online). Information security, therefore, needs to be implemented and managed within the organisation to ensure that the information is kept safe and secure (Krige, 1999, p 7).

Information is an organisational asset, and consequently the security thereof needs to be integrated into the organisation's overall management plan (Lane, 1985, pp 2-3; Smith, 1989, p 193). Effective corporate governance should dictate this overall management plan. Sir Adrian Cadbury, in the foreword of *Corporate Governance: A Framework for Implementation* has the following description of corporate governance. He states that corporate governance deals with establishing a balance between economic and social goals and between individual and mutual goals. The framework for governance is there to promote the competent use of resources and, in the same way, to involve accountability for the stewardship of those resources (World Bank Group, 1999, online).

It is inevitable that these organisations that should deploy effective corporate governance develop a corporate culture. Cultural assumptions in organisations develop around how people in the organisation relate to one another, but that is only a tiny portion of what culture covers (Schein, 1999, p 28). Corporate culture is generally defined as values that are shared by everyone in an organisation, including fundamental beliefs, principles and practices (Beveridge, 1997, online). These fundamental beliefs, principles and practices have a direct influence on the behaviour patterns of employees as far as information security is concerned.

The purpose of this paper is to investigate to what extent the senior management of an organisation should be involved in changing the beliefs, principles and practices of their employees towards information security, thereby influencing their behaviour favourably towards the protection of information. The paper will initially investigate the field of corporate governance, followed by the challenges facing corporate governance and information security. Corporate culture and its importance to an organisation will then be explored and the paper will conclude by investigating the relationships between corporate governance, corporate culture and information security. Based on this investigation, the term 'Information Security Obedience' will be defined.

2. CORPORATE GOVERNANCE

Corporate governance is a contemporary term for an issue which has been challenging organisations for decades – that of 'accountability'. Corporate governance is defined as the exercise of power over and responsibility for corporate entities (Blackwell Publishers, 2000, online). At its most fundamental level, corporate governance provides assurance that an organisation has the necessary corporate structures to support accountability (Brooks, 1997, online).

Accountability, however, is only one of the four pillars of corporate governance. The remaining pillars are responsibility, fairness and transparency (King Report, 2001, p 17; World Bank Group, 1999, online). The pillar of *accountability* ensures that individuals or groups in an organisation are accountable for their decisions and actions (King Report, 2001, p 14). The second pillar, *responsibility*, indicates that corrective action can be taken against mismanagement and misconduct (King Report, 2001, p 14). *Fairness*, the third pillar of corporate governance, attempts to ensure that there is a balance in an organisation. The rights of various groups should be recognised and valued (King Report, 2001, p 14). The final pillar, *transparency*, is the ease with which outsiders can see what is transpiring inside an organisation (King Report, 2001, p 13).

Through these corporate governance pillars, the Board of Directors is both accountable and responsible to their organisation and their shareholders for the wellbeing of their organisation (King Report, 2001, p 17). Information is a vital asset to most organisations, and because the Board of Directors is both accountable and responsible for the welfare of their organisation they should ensure that the organisational asset of information is protected to ensure the well-being of the organisation (Deloitte & Touche, 2002, online).

3. CHALLENGES FACING CORPORATE GOVERNANCE AND INFORMATION SECURITY

There are many challenges facing the convergence of corporate governance and information security – one of which is to convince the senior management of an organisation that they should be ultimately accountable and responsible for the protection of their organisation's information. PriceWaterhouseCoopers highlights the lack of support there is for information security, in their 2002 Information Security Breaches Survey, by stating that "The root cause is that security is treated as an overhead rather than an investment" (PriceWaterhouseCoopers, 2002, p 3).

Furthermore, according to PriceWaterhouseCoopers, only 27% of organisations in the United Kingdom spend more than 1% of their Information Technology budget on protecting their information and only 5% of organisations spend more than 10% of their IT budget on information security (PriceWaterhouseCoopers, 2002, p 3). This lack of attention to information security could be as a result of the fact that managers can normally only allocate a limited amount of time and consideration to information

security. As a consequence, management's attention is often limited to a small group of acute threats and countermeasures that happen to relate to the issues of the day (Buren, van der Meer, Shahim, Barnhoorn & Roos Lindgreen, 1999, p 76).

However, the successful operation of organisations today relies on information, and the exchange of information. Further, the protection of information, through information security, is important for the impact it can have on business (Deloitte & Touche, 2002, online). Therefore, management should be concerned with information security as information is vital for the success of the organisation. In fact, they are accountable and responsible for the well-being of the organisation that depends heavily on information, as highlighted earlier.

One of the ways for management to demonstrate their dedication to information security in their organisation is to provide their support and commitment towards a formally agreed upon and documented corporate information security policy, as it is one of the controls that is considered common best practice in terms of information security (BS 7799-1, 1999, p 4).

Quality information security begins and ends with quality corporate policies (Whitman & Mattord, 2003, p 194). An overriding duty of the Board of Directors is to ensure the long-term feasibility of an organisation. To do this, it is essential that the assets of an organisation are protected (World Bank Group, 1999, online).

Therefore, it follows that the Board of Directors should be involved in the protection of information, an important organisational asset. The level of information security that the Board of an organisation is prepared to propose and put into operation, and the level of information security that is acceptable to the shareholders should be consolidated and result in the corporate information security policy (King Report, 2001, p 96). The information security policy should be based on the approved corporate security objectives and strategy and is there to provide management direction and support for information security (British Standards Institute, 1993, p 17).

The main aim of any policy, whether for information security or not, is to influence and determine decisions, actions and other issues, by specifying what behaviour is acceptable and what behaviour is unacceptable. Policies and procedures are, therefore, organisational laws that determine acceptable and unacceptable conduct within the context of corporate culture (Whitman & Mattord, 2003, p 194).

4. CORPORATE CULTURE

Every organisation has a culture and this culture exists at both a conscious and unconscious level (Hagberg Consulting Group, 2002, online). This culture could be operating with authoritative principles and driven by top management. However, many

organisations have a culture that exists by default. This culture changes by accident and is influenced by a few key people in the organisation (Atkinson, 1997, p 16). A disturbing fact is that it is estimated that only 5% of organisations have a definable culture, where the senior management takes an active role in the shaping of the culture (Atkinson, 1997, p 17). If management does not understand the culture in their organisation, it could prove to be fatal in today's business world (Hagberg Consulting Group, 2002, online).

Culture is the overall, taken-for-granted assumptions that a group has learned throughout history (Schein, 1999, p 29). Corporate culture is an extensive issue and because the shared beliefs of an organisation include values about what is desirable and undesirable – how things should and should not be – these beliefs dictate the kinds of activities that are 'legal' and the kinds that are 'illegal' for the employees in an organisation (Beyer, 1981, p 21).

Since corporate culture plays a major role in the actions of employees in an organisation, it is an important aspect in an organisation, as it is central to restraining or enhancing the performance of an organisation (Atkinson, 1997, pp 16-17). Culture is imperative because it is a powerful, underlying and often unconscious set of forces that establishes individual and group behaviour. Corporate culture is especially important because cultural elements determine the strategy and goals of an organisation (Schein, 1999, p 14).

One of the difficulties in trying to understand culture is that it is a very complex discipline, which should not be oversimplified. It is very simple to say that culture "is the way things are done around here", but a much better way of thinking is to appreciate that culture exists at numerous levels. These levels range from the visible to the tacit and invisible. Furthermore, it is imperative that these levels are managed and understood (Schein, 1999, p 15).

Levels of Corporate Culture

The corporate culture and behaviour of people in organisations has been extensively researched by Edgar H. Schein. Schein states that, "A better way to think of culture is to realise that it exists at several 'levels', and that we must understand and manage the deeper levels" (1999, p 15).

The first level of corporate culture and probably the simplest level to examine in an organisation is that of *artifacts*. Some of the most visible expressions of culture are these artifacts (Hagberg Consulting Group, 2002, online). Artifacts can be described as what an individual can see, hear and feel when they walk into an organisation. Examples of artifacts could range from the design and décor of the organisation to how people behave towards each other and customers (Schein, 1999, p 16).

Espoused values are the second level of culture in an organisation. These are the values expressed and published in an organisation's policies and are those values that an organisation is said to be promoting. Examples of espoused values are teamwork and good communication (Schein, 1999, p 17).

When it comes to the first two levels of corporate culture, there could be a few obvious contradictions between some of the *espoused values* or goals of an organisation and the visible behaviour of an organisation as seen at the *artifacts* level. What these contradictions between the two levels indicate is that a deeper level of thought and insight is driving the evident behaviour of the employees (Schein, 1999, p 18). What an organisation strives to do and the values it wishes to endorse may be different from the values, beliefs, and norms expressed in the actual practices and behaviour of the organisation (Hagberg Consulting Group, 2002, online). Therefore, the deeper level that drives the visible behaviour may or may not be consistent with the values and principles that are espoused by the organisation. So, to truly understand the culture of an organisation the deepest level of corporate culture must be understood (Schein, 1999, pp 18-19).

Schein refers to this deepest level as the *shared tacit assumptions* level. The heart of corporate culture is the mutually learned values, beliefs and assumptions that have become taken for granted as the organisation continues to be successful. These tacit assumptions involve the nature of the organisation's environment and how to succeed in it. Examples of shared tacit assumptions are unique to a particular organisation, but generally are decisions and actions that are second-nature to an employee (Schein, 1999, p 19).

Therefore, the decision and actions of employees are determined through the three levels of corporate culture. And these three levels emphasise that culture is extremely stable, as it represents the accumulated learning of a group (Schein, 1999, p 21).

As has been highlighted earlier, the Board of Directors should be both accountable and responsible for the well-being of an organisation which depends on information and information resources. To protect this information, the behaviour patterns of employees must assist in ensuring information security. Since, the corporate culture of an organisation determines the behaviour of employees in an organisation; it should be used to influence these behaviour patterns of employees towards the protection of information as envisioned by the Board of Directors.

5. RELATIONSHIPS BETWEEN THE THREE FIELDS

The three fields of information security, corporate governance and corporate culture have been highlighted individually in the earlier part of the paper. The following section will investigate the relationships that should exist between these three fields. The relationships between the fields can be depicted diagrammatically, as shown in Figure 1.

Appendix C

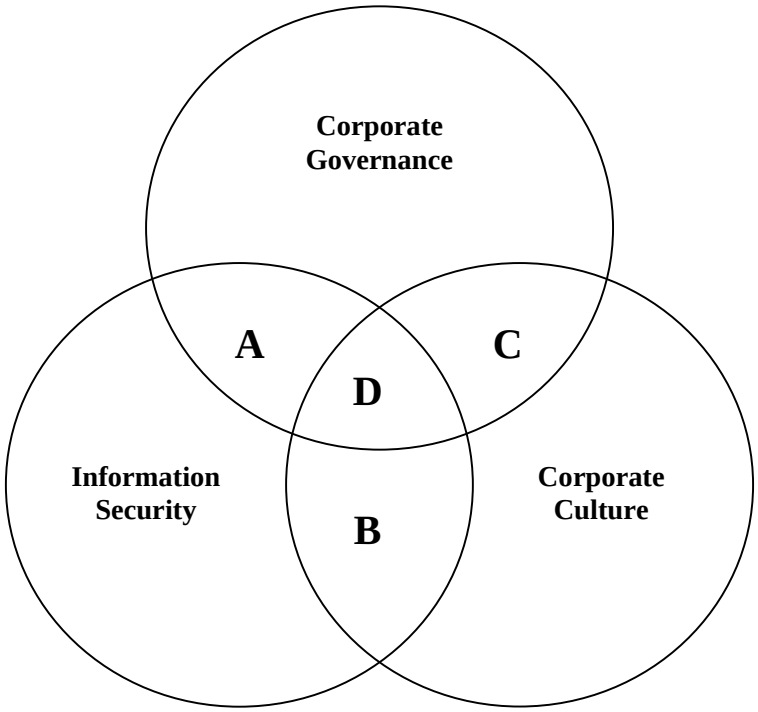

Figure 1. The relationships between information security, corporate governance and corporate culture

The relationship that should exist between information security and corporate governance, represented by 'A' in the diagram, is highlighted with the following quote from Michael Cangemi, President and COO of the Etienne Aigner Group Inc. He states that, "The information possessed by an organisation is among its most valuable assets and is critical to its success. The Board of Directors, which is ultimately accountable for the organisation's success, is therefore responsible for the protection of its information. The protection of this information can be achieved only through effective management and assured only through effective board oversight" (IIA, AICPA, ISACA, NACD, March 2000, online). This highlights the fact that there is a very strong relationship between the fields of information security and corporate governance.

As seen in previous sections of the paper, information security is currently being seen as an overhead, rather than as an investment. The senior management of organisations tends to view information security as a technical problem that the IT department should be concerned with. However, the information that resides on an organisation's systems is owned by the business as a whole, not the IT manager. Information and information systems play critical roles in business processes. Therefore, it is the senior management of organisations that needs to direct the approach to protecting their information (Deloitte

& Touche, 2002, online). Proactively addressing an organisation's information security issues in the digital era is not only good business practice; it is a necessity (Gordon and Glickson, 2001, online). One of the ways to enhance the relationship between information security and corporate governance is for senior management to support and direct the creation and implementation of a corporate information security policy. Therefore, the corporate information security policy should play a critical role in the way that senior management governs the security of information.

The relationship, represented by 'B' in the diagram, represents the relationship between information security and corporate culture. When investigating information security, it is often seen that the procedures employees use in their daily work and their behaviour could symbolise the weakest link in information security (Martins and Eloff, 2002, p 203). In addition, it has been pointed out that the corporate culture of an organisation, to a large extent, determines the decisions and actions of employees (Schein, 1999, p 17). Therefore, the corporate culture in an organisation should be used to influence the behaviour of the employees towards information security in a positive way. In order to do this, the *shared tacit assumptions* level of corporate culture must be addressed. The collective beliefs and values of employees are found at this level of corporate culture. This *shared tacit assumptions* level directly influences the *artifacts* level of culture, which displays the visible behaviour of employees. Therefore, for employee behaviour to change; their beliefs must be altered positively towards information security. Understanding the corporate culture around information security is crucial, and assessing employees' awareness, competence and commitment determines the best method for the implementation and distribution of the corporate information security policy so that it will be effective (Deloitte & Touche, 2002, online). An encompassing information security policy should assist in cultivating a corporate culture that takes advantage of the benefits of information security practices (Gordon and Glickson, 1997, online). Therefore, as information security is highly dependent on the behaviour of the users of information, the behaviour should preferably be instilled through corporate culture to ensure that acceptable behaviour becomes the de facto behaviour.

The relationship between corporate governance and corporate culture is represented by 'C' in the diagram. The behaviour of employees is, to a large extent, shaped by the beliefs and values the employees have at the *shared tacit assumptions* level of corporate culture. Therefore, senior management should make a resolute attempt to shape the s*hared tacit assumptions* level, and, consequently, the corporate culture into one that will help in the achievement of the organisation's goals.

As part of good corporate governance practices, one of the responsibilities of senior management is that they must outline the goals and vision for their organisation. These goals and vision of an organisation should be what is expressed by senior management at the *espoused* v*alues* level of corporate culture. It is also senior management's responsibility to guide their organisation in achieving these goals. Therefore, senior management, as part of their corporate governance duties, should ensure that the

necessary elements of corporate culture are in place to support the organisation in achieving its goals.

The desired corporate culture would be one where the vision expressed at the *espoused values* level of culture by senior management is supported by the actions and behaviour of employees determined by the *shared tacit assumptions* level of corporate culture.

The behaviour displayed by senior management, in terms of information security practices, helps shape the attitude of employees towards information security. In addition, it is also the behaviour senior management accepts from their employees that influences the corporate culture. Management policies describe what behaviour is acceptable and unacceptable. Senior management must ensure that the policies are implemented in their organisation in such a way that the behaviour of the employees change, which would ultimately lead to a change in the corporate culture. Therefore, as information security is a management responsibility, the information security policy should guide employees to function in a manner that adds to the protection of information (Whitman & Mattord, 2003, p 194). As detailed previously, for senior management to transform the corporate culture in their organisation they must address the beliefs and values found at the *shared tacit assumptions* level of corporate culture. Senior management must ensure that their employees' beliefs will support all *espoused values* of their organisation, including their vision for information security.

The relationship represented by 'D' in the diagram is the relationship between the three fields of information security, corporate governance and corporate culture. To be genuinely valuable, information security needs to become part of the way everyone conducts their daily tasks, from senior management, throughout the entire organisation (Deloitte & Touche, 2002, online). Therefore, information security should become an intricate part of the corporate culture of the organisation, as it is the culture that determines how employees conduct their daily tasks (Beach, 1993, p 11). This relationship should represent the situation whereby senior management's vision for the protection of information in the organisation is conveyed through the corporate information security policy. This policy should be drafted, advocated and implemented in such a way that it positively influences the corporate culture with regard to information security. Further, as information security is highly dependent on the behaviour of users, the corporate culture should contribute towards the fact that the de facto behaviour of users is indeed what senior management envisaged as acceptable behaviour. This relationship can be encompassed by the term 'Information Security Obedience'. Obedience is defined as "compliance with that which is required by authority" (Dictionary.com, 2003, online). The authority in this case is the senior management of organisations, striving towards effective corporate governance. Another definition is, "words or actions denoting submission to authority" (Dictionary.com, 2003, online). As has been said, the words or actions of employees are, to a large extent, determined by the corporate culture in an organisation.

Therefore, by using the term Information Security Obedience, it binds together all three fields of information security, corporate governance and corporate culture. The term does this by stating that the actions of the employees must comply with that which is required by senior management in terms of information security. Therefore, 'Information Security Obedience' is defined, for the purposes of this paper, as 'de facto user behaviour complying with the vision of senior management as defined in the corporate information security policy'.

6. CONCLUSION

Information is important to any organisation. However, the protection of this information through information security still forms a very small part in the overall corporate governance strategy. Senior management must be made aware that the protection of information should be their responsibility and they should create the policy necessary to ensure information security in their organisation. One of the problems facing information security is the behaviour of employees. Most employees do not understand the importance of protecting information, and this lack of understanding is reflected in their negligent information security practices. The corporate information security policy should describe the vision and goals of senior management in relation to information security. This policy should then be implemented in the organisation in such a way that it affects the behaviour of the users. To ensure the behaviour of employees change favourably towards information security practices, it should become second-nature behaviour in the daily activities. Information Security Obedience is the solution to ensuring proper information security behaviour.

This paper defined the term 'Information Security Obedience'. It explored the relationships between the three fields of corporate governance, corporate culture and information security, and highlighted the importance of binding these fields together. Further research will be conducted to investigate how current information security practices should be modified to have an effect on corporate culture. The manner in which the corporate information security policy is drafted and implemented in an organisation will be investigated. A further paper will highlight how 'Information Security Obedience' can be used to integrate the three fields and what actions must be taken to do so.

7. REFERENCES

Atkinson, P. (1997). *Creating culture change – strategies for success.* Bedfordshire, England : Rushmere Wynne.

Beach, L.R. (1993). *Making the right decision. Organizational culture, vision and planning.* Eaglewood Cliffs, New Jersey : Prentice Hall.

Beveridge, C.A.R. (December, 1997). *Behaviour in organisations*. [online]. [cited 23 January 2003] Available from Internet: URL http://www.carb.fsnet.co.uk/bio97.pdf

Beyer, J.M. (1981). *Handbook of organizational design.* New York : Oxford.

Blackwell Publishers. (2000). [online]. [cited 12 January 2002]. Available from Internet: URL http://www.blackwellpublishers.co.uk/journals/corg

British Standards Institute. (1993). *Code of practice for information security management (CoP).* DISC PD 0003. UK.

Brooks, J. (April 1997). *Converging cultures - trends in European corporate governance.* [online]. [cited 12 February 2003]. Available from Internet: URL http://www.tiaa-cref.org/pressroom/corpgov.pdf

Bruce, G. & Dempsey, R. (1997). *Security in distributed computing – did you lock the door?*. Upper Saddle River, New Jersey : Prentice Hall.

BS 7799-1. (1999). *Code of practice for information security management (CoP).* DISC PD 0007. UK.

Buren, A., van der Meer, B., Shahim, A., Barnhoorn, W. & Roos Lindgreen, E. (1999). Information security at top level. *Information security management & small systems security*, pp.75-76.

Deloitte & Touche. (May 2002). *Management briefing – information security*. [online]. [cited 13 January 2003] Available from Internet: URL http://www.deloitte.com/dtt/cda/doc/content/info_security(1).pdf

Dictionary.com. (2003). [online]. [cited 3 July 2003]. Available from Internet: URL http://dictionary.reference.com/search?q=obedience

Drennan, D. (1992). *Transforming company culture.* Berkshire, England : MacGraw-Hill.

Gordon, G. (2002, May 12). Dozens of threats beset your data. *Sunday Times, Business Surveys* [online]. [cited 17 July 2002] Available from Internet: URL http://www.suntimes.co.za/2002/05/12/business/surveys/internet/survey10.asp

Gordon and Glickson LLC. (2001). *Comprehensive information security policies: meeting an organisation's privacy and security needs.* [online]. [cited 23 March 2003] Available from Internet: http://www.ggtech.com/

Hagberg Consulting Group (2002). *Corporate Culture/Organisational Culture: Understanding and Assessment* [online]. [cited 25 January 2003] Available from Internet: URL http://www.hcgnet.com/html/articles/understanding-Culture.html

IIA, AICPA, ISACA, NACD (March 2000). A call to action for corporate governance [online]. [cited 16 July 2002] Available from Internet: URL http://csweb.rau.ac.za/ifip/issa2002/presentations/Basie%20von%20Solms.ppt

King Committee on Corporate Governance. (2001). *King report on corporate governance for South Africa 2001*. [online]. [cited 3 March 2002] Available from Internet: URL http://www.iodsa.co.za/IoD%20Draft%20King%20Report.pdf

Krige, W. (1999). *The usage of audit logs for effective information security management.* Unpublished master's thesis. Port Elizabeth Technikon, Port Elizabeth, South Africa.

Lane, V.P. (1985). *Security of computer based information systems.* London: Macmillan.

Martins, A. and Eloff, J. (2002). Information Security Culture. *IFIP TC11, 17th International Conference on Information Security (SEC2002), Cairo, Egypt*. Kluwer Academic Publishers Group, Netherlands : pp. 203-214.

PriceWaterhouseCoopers (2002). *Information security breaches survey technical report.* [online]. [cited 5 January 2003] Available from Internet: URL http://www.security-survey.co.uk

Schein, E.H. (1999). *The corporate culture survival guide*. San Francisco, California, United States of America : Jossey-Bass Publishers.

Smith, M.R. (1989). *Commonsense computer security*. London: McGraw-Hill.

Whitman, M.E. & Mattord, H.J. (2003). *Principles of Information Security*. Kennesaw State University : Thomson Course Technology.

World Bank Group. (1999, September 20). *Corporate governance: a framework for implementation – overview*. [online]. [cited 23 December 2002] Available from Internet: URL http://www.worldbank.org/html/fpd/privatesector/cg/docs/gcgfbooklet.pdf

Appendix D

Towards an Information Security Competence Maturity Model

Kerry-Lynn Thomson[a] and Rossouw von Solms[b]

[a]Port Elizabeth Technikon, South Africa

[b]Port Elizabeth Technikon, South Africa

[a]kerry-lynn.thomson@nmmu.ac.za, (041) 504 3408, Department of Information Technology, NMMU, Private Bag X6011, Port Elizabeth 6000

[b]rossouw.vonsolms@nmmu.ac.za, (041) 504 3604, Department of Information Technology, NMMU, Private Bag X6011, Port Elizabeth 6000

1. Introduction

"If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology." This quote by Bruce Schneier highlights that technical controls alone will not ensure the safety of the information assets of an organisation and will not solve information security related problems. Just as important to the protection of information, if not more so, are the operational controls necessary to ensure the success of information security practices, as information security is people-based (Shorten, 2004, p 1374).

It is important for the senior management in organisations to realise that information security is not solely concerned with technical and physical controls. Most technical and physical controls have operational issues associated with them, dependent on human behaviour. In addition, employee behaviour, to a large extent is dependent on the corporate culture in an organisation. Therefore, any attempt in an organisation to implement technical and physical controls without considering the culture in the organisation could have disastrous consequences (Shaurette, 2004, p 1080). Corporate culture is a strong driving force in organisations which largely affects the behaviour of employees and, consequently, the success of the information security practices (Beach, 1993, p 17).

The vision of senior management with regard to information security must be outlined in the Corporate Information Security Policy of the organisation. The Policy should be 'translated' into procedures that will positively affect the attitude and behaviour of employees. Eventually the *de facto*, or second-nature, behaviour of employees should

adhere to the behaviour necessary to adequately protect the information assets of an organisation, as outlined by the vision of senior management in the Corporate Information Security Policy. Thomson and von Solms define this natural behaviour of employees, in line with the information security vision of senior management, as Information Security Obedience (2003, p 107).

This paper will highlight the effect that employee behaviour has on the success of information security practices. The paper will examine the Conscious Competence Learning Matrix and will introduce an Information Security Competence Maturity Model that could assist the senior management of an organisation in positively adapting the behaviour of the employees.

2. The Significance of Corporate Culture

Culture is generally defined as those beliefs, values and assumptions that a group has learned over time. Corporate culture is the set of procedures and practices that both senior management and employees follow in order to be successful in their environment (Schein, 1999, p 29).

This set of procedures and practices should be supported in the policies of an organisation. Further, it is the responsibility of senior management to give effect to the policies in an organisation (Leveson, 1970, p 52). It is essential that a Corporate Information Security Policy is created in an organisation, as it implies what behaviour is acceptable and what behaviour is unacceptable in terms of information security practices (Beach, 1993, p 17). The Corporate Information Security Policy must work within the organisation, where the corporate culture exists, and must address the security needs of the specific organisation (Deloitte & Touche, 2002, online).

Therefore, if the corporate culture is not taken into consideration when enforcing the Information Security Policy in an organisation, the behaviour of employees will not change to reflect the 'wishes' embedded in the Information Security Policy. This results in the fact that employee behaviour is often the principal obstacle in ensuring that information assets are kept secure (Martins and Eloff, 2002, p 203).

However, diligent and well trained employees can become the strongest link in terms of information security in an organisation (Henry, 2004, p 1100). It is, therefore, critical to understand how to get employees dedicated to and knowledgeable about their roles and responsibilities towards information security. It is also of vital importance that employees commit to an information security program and adapt their behaviour positively towards information security. The information security program should be created, enforced and encouraged by the senior management of an organisation through the Corporate Information Security Policy (Henry, 2004, p 1100).

3. Conscious Competence Learning Matrix

The Conscious Competence Learning Matrix explains the process and stages that people must move through to learn a new skill, behaviour or technique. This Matrix is generic and could cover a wide variety of skills. It is clear, however, that people only respond to training when they are aware of their need for it (Chapman, 2001, online).

The first stage of the Conscious Competence Learning Matrix is *Unconscious Incompetence*. At this stage the employee is not aware of the tasks that must be performed and the employee is not aware that there is a deficiency in the skills needed to perform the particular task. The employee does not understand the relevance and significance of the new task and must become conscious of his/her incompetence before learning can begin (Chapman, 2001, online). Employees do not know what is 'right' or 'wrong' and their behaviour is consequently out of line.

At stage two of the Matrix, *Conscious Incompetence*, the employee becomes aware of the existence and relevance of the task to be performed. The employee now becomes aware of his/her role in this task and that by learning the skills required for this task, he/she improves his/her ability and effectiveness in the organisation. Employees at this stage know what actions and behaviour are 'right' and which are 'wrong', and the relevant tasks that must be performed. However, they still do not know exactly how to perform these tasks. Ideally at this stage, the employee has a measure of his/her level of deficiency in the particular task and a measure of the stage of skill that is needed to perform the task (Chapman, 2001, online).

The third stage of the Conscious Competence Learning Matrix is *Conscious Competence*. At this stage, the employee will need to concentrate and think to be able to perform the task. The employee will not be able to perform the task unless thinking about it and making a mental effort, as the task has not become 'second nature' or part of the culture.

The most effective means of progressing to the fourth stage in the Learning Matrix is practice. The employees must practice the new task and commit to becoming Unconsciously Competent at the task (Chapman, 2001, online).

At the *Unconscious Competent* stage, the task becomes so practiced that it enters the subconscious thinking of the employee and becomes 'second nature' or part of the culture. The Unconsciously Competent employee may even have difficulty in explaining how a task is done as the task has become mostly instinctual (Chapman, 2001, online).

The progression through the various stages of the Conscious Competence Learning Matrix can be demonstrated through an everyday example. When a person first begins typing on a keyboard it is usually with one or two fingers (Stage 1). As the need to type faster increases, more fingers will be used and the person may wish to take a typing

course to improve his/her skill (Stage 2). Initially, when the person achieves typing using both hands the typing is a conscious effort, with the person frequently looking at his/her hands to check that the correct keys are being hit (Stage 3). Eventually, the typing becomes an unconscious process, where the person is able to look at the computer monitor while typing (Stage 4). However, if the standard QWERTY keyboard were to be replaced with a new keyboard that has a completely different layout, the learning would have to begin again and the person would once again have to progress through the Conscious Competence Learning Matrix.

Senior management would like employees in its organisation to be at stage four of the Conscious Competence Learning Matrix for the daily tasks that employees should perform. This would signify that the correct practices would be part of the natural behaviour of employees. In the following section, the Conscious Competence Learning Matrix will be used to define the Information Security Competence Maturity Model as a way for employees to become skilled in information security practices.

4. Information Security Competence Maturity Model

Employees of an organisation are very often unconsciously incompetent when it comes to information security practices. They are not aware that they are unskilled in terms of information security. Therefore, they are at Stage 1 of the Information Security Competence Maturity Model. At Stage 1, employees are at the *Unconscious Incompetent* stage and unaware of the role they should be playing in terms of information security. At this stage employees are not aware of their ineffectiveness in information security practices. Any attempt to change behaviour at this stage will not be advisable, as employees of an organisation will not internalise the changes and make it part of their new culture unless they understand the benefit of these changes (Schein, 1999, p 187). Therefore, if employees view information security as a hindrance to their work and do not fully understand the benefit, they will not accept the appropriate responsibility for their role in information security, and may go out of their way to find a "work-around" to any information security measure they do not consider necessary (Shorten, 2004, p 1381).

In order for employees to progress form Stage 1 to Stage 2 an effective Information Security Awareness Program should be run in the organisation. The purpose of the Information Security Awareness Program is to focus attention on information security. Employees taking part in the program are recipients of information and do not take an active role in the program (National Institute of Science and Technology Special Publication 800-16, 1998, p 15). An effective Information Security Awareness Program should help employees understand why they must take information security seriously and what they will gain from its proper implementation (Peltier, 2004, p 1494). Ideally, an Information Security Awareness Program should prepare employees for Information Security Training by encouraging a change in employee attitude towards information security. Examples of Information Security Awareness components are awareness

presentations, videos, posters and inspirational information security slogans (National Institute of Science and Technology Special Publication 800-16, 1998, p 15). Once employees have participated in the Information Security Awareness Program, and they have been made aware of all the potential threats to information assets, they progress to Stage 2.

Stage 2 is *Conscious Incompetence*. At this stage employees are already aware of their information security roles and responsibilities. Employees at this stage understand the benefit of protecting information assets and the responsibilities that they have with regard to information security. Employees realise that protecting information assets not only protects themselves, but their organisation as well and employees realise what action is required from them to progress to Stage 3.

For employees to move from Stage 2 to Stage 3, they must participate in Information Security Training. Through Information Security Training, employees will learn "how" information assets must be protected and employees will learn vital skills enabling them to perform information security practices (National Institute of Science and Technology Special Publication 800-16, 1998, p 18). The Information Security Training program should reinforce all the terms and concepts introduced in the Information Security Awareness Program and employees should apply their learning through hands-on activities. One of the main aims of Information Security Training is to promote personal responsibility for information security amongst employees and to achieve positive behavioural change in terms of information security practices (National Institute of Science and Technology Special Publication 800-16, 1998, p 25). Once employees have participated in the Information Security Training program, and gained the required skills, they are ready to progress to Stage 3.

At Stage 3 of the Information Security Competence Maturity Model, *Conscious Competence*, employees need to consciously focus on the information security practices they need to perform. These practices are performed correctly, but are neither second-nature nor part of the employees' corporate culture.

For employees to progress from Stage 3 to Stage 4, a combination of techniques can be used. Firstly, a mixture of education and experience should be used. For employees to fully appreciate the complexity of information security they should progress from Information Security Awareness to Information Security Training to Information Security Education. Information Security Education provides insight to employees and a deeper understanding of information security practices. Information Security Education provides long-term learning through seminars and in-depth discussion (National Institute of Science and Technology Special Publication 800-16, 1998, p 18).

However, Information Security Education is not enough. A Chinese proverb says "I hear and I forget, I see and I remember, I do and I understand." This proverb loosely tracks the progression of employees through the Information Security Competence Maturity

Model. Employees will only be able to legitimately progress to Stage 4 when they apply the skills they have learnt through Information Security Awareness, Training and Education and have gained Experience by performing the information security practices incessantly and become accustomed to the newly learnt practices. Once employees become experienced in information security practices they will progress to a point where these practices become second-nature and they will advance to Stage 4 through the experience they have gained.

Secondly, positive reinforcement will help promote employees from Stage 3 to Stage 4. Reinforcement should be used as confirmation that the employees are performing the correct information security practices and to solidify the benefit of information security practices to the employees. These reinforcements or incentives do not have to be monetary, as positive reinforcement is widely used in behaviour modification in organisations, and it has been found that praise and social reinforcers are more common and effective than monetary reinforcers (Arnold et al, 1998, p 232).

The ultimate goal of the Information Security Competence Maturity Model is for the employees of an organisation to reach Stage 4, through awareness, training and experience, and become *Unconsciously Competent* in the critical information security practices which support the information security vision of senior management. These practices should adhere to the information security vision of senior management and become part of the *de facto* employee behaviour and, therefore, part of the corporate culture. If this is achieved, then Information Security Obedience, as described by Thomson and von Solms, has been realised. The progression of employees from Unconscious Incompetence to Information Security Obedience is depicted in the Information Security Competence Maturity Model in Figure 1.

Appendix D

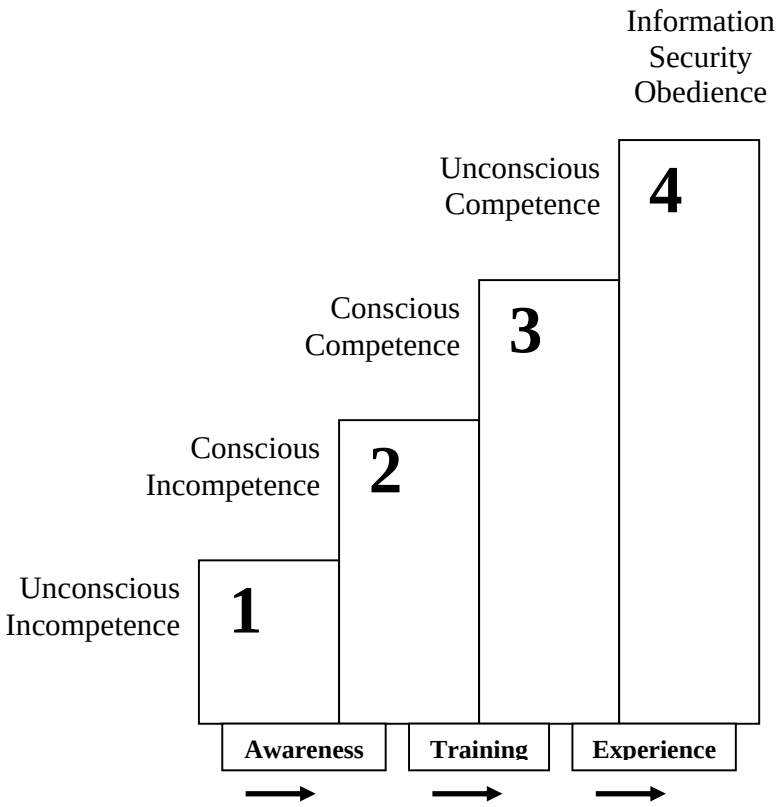

Figure 1: Information Security Competence Maturity Model

Employees progress from Stage 1 of the Information Security Competence Model (Unconscious Incompetence) to Stage 2 (Conscious Incompetence) through an Information Security Awareness Program.

Employees at Stage 2 progress to Stage 3 (Conscious Competence) once they have undergone Information Security Training and are, not only aware, but skilled in the various information security tasks.

For employees to move from Stage 3 to Stage 4 (Unconscious Competence) the employees must gain sufficient experience in the information security practices. Employees at Stage 4 perform information security practices correctly as they fully understand and are in agreement with the way things are done in the organisation and their behaviour is second-nature to them (Schein, 1992, online). Information Security Obedience could then be observed in those organisations where employees have reached Stage 4.

5. Conclusion

One of the principal problems facing information security is the behaviour and actions of employees towards the information assets. Consequently, employees who understand the benefit of protecting the information assets and their roles and responsibilities, and adhere to the correct behaviour, could be the strongest link in the information security infrastructure. Therefore, senior management of organisations would ideally like its employees to become Unconsciously Competent in information security practices.

This paper focused on how employees should advance from Unconscious Competence through various stages to reach Stage 4 of the Information Security Competence Maturity Model. Initially, the Conscious Competence Learning Matrix was investigated and used to define the Information Security Competence Maturity Model. This model could assist organisations in determining at which Stage employees are currently, and advising the best way to promote employees to Information Security Obedience.

6. References

Arnold, J., Cooper, C.L & Robertson, I.T. (1998). *Work psychology – understanding human behaviour in the workplace.* Edinburgh Gate, England : Prentice Hall.

Beach, L.R. (1993). *Making the right decision. Organizational culture, vision and planning.* Eaglewood Cliffs, New Jersey : Prentice Hall.

Chapman, A. (2001). Conscious competence learning model. [online]. [cited 3 October 2004] Available from Internet: URL http://www.businessballs.com/ProcessofchangeJF2003.pdf

Deloitte & Touche. (May, 2002). *Management briefing – information security*. [online]. [cited 13 January 2003] Available from Internet: URL http://www.deloitte.com/dtt/cda/doc/content/info_security(1).pdf

Drennan, D. (1992). *Transforming company culture.* Berkshire, England : MacGraw-Hill.

Henry, K. (2004). *The human side of information security - information security handbook, fifth edition*. Boca Raton, London, New York, Washington D.C. : Auerbach Publishers.

Leveson, G. (1970). *Organisation directors – law and practice*. Durban, South Africa : Buttersworth.

Martins, A. and Eloff, J. (2002). Information Security Culture. *IFIP TC11, 17th International Conference on Information Security (SEC2002), Cairo, Egypt*. Kluwer Academic Publishers Group, Netherlands : pp. 203-214.

National Institute of Science and Technology Special Publication 800-16 (April, 1998). *Information technology security training requirements: a role- and performance-based model.* Washington D.C. : Superintendent of Documents, U.S. Government Printing Office.

Peltier, T. (2004). *Security awareness program – information security handbook, fifth edition.* Boca Raton, London, New York, Washington D.C. : Auerbach Publishers.

Schein, E.H. (1999). *The corporate culture survival guide.* San Francisco, California, United States of America : Jossey-Bass Publishers.

Schein, E.H. (1992). Organisational leadership and culture. [online]. [cited 12 January 2004] Available from Internet: URL http://www.tnellen.com/ted/tc/schein.html

Schneier, B. (2000). *Secrets & lies: digital security in a networked world.* New York City, New York: Wiley Computer Publishing.

Shaurette, K.M. (2004). *The building blocks of information security – information security handbook, fifth edition.* Boca Raton, London, New York, Washington D.C. : Auerbach Publishers.

Shorten, B. (2004). *Information security policies from the ground up – information security handbook, fifth edition.* Boca Raton, London, New York, Washington D.C. : Auerbach Publishers.

Thomson, K-L & von Solms, R. (2003). *Integrating information security into corporate culture.* Unpublished master's thesis. Port Elizabeth Technikon, Port Elizabeth, South Africa.

Appendix E

Cultivating an Organisational Information Security Culture

Kerry-Lynn Thomson[a], Rossouw von Solms[b] and Lynette Louw[c]

Centre for Information Security Studies,
Nelson Mandela Metropolitan University, South Africa

[a]kerry-lynn.thomson@nmmu.ac.za
[b]rossouw.vonsolms@nmmu.ac.za
[c]lynette.louw@nmmu.ac.za

Abstract

An information security solution should be a fundamental component in any organisation. One of the major difficulties in achieving the assimilation of information into an organisation is the actions and behaviour of employees. To ensure the integration of information security into the corporate culture of an organisation, the protection of information should be part of the daily activities and second-nature behaviour of the employees.

Key Words

Corporate Culture; Information Security; Corporate Information Security Obedience; Conscious Competence Maturity Model; Modes of Knowledge Creation; MISSTEV Model

1. Introduction

"Despite our intellect, we humans – you, me and everyone else – remain the most severe threat to each other's security." This quote from Kevin J. Mitnick (2002, p 8) highlights the issue facing the protection of information that is often overlooked – the human factor. One of the biggest threats to the success of information security in an organisation is the erroneous actions and behaviour of employees when handling information.

In order to guard against this, it is vital that employees learn about, and integrate, acceptable information security practices into their everyday behaviour. This paper will address how employees should learn, develop and integrate the correct information security skills into their daily behaviour and, ultimately, facilitate the protection of information assets.

2. An Information Secure Corporate Culture

Corporate culture is the total of all the shared, taken-for-granted assumptions that a group has learned over time (Schein, 1999, pp 28-29). Every organisation has a corporate culture, whether it is aware of the culture or not, and this culture exists at both a conscious and unconscious level (Hagberg Consulting Group, 2002, online). A balanced corporate culture is essential in an organisation as it is a powerful, underlying and often unconscious set of forces that establishes individual and group behaviour (Schein, 1999, p 14). In terms of information security, employee actions and behaviour are particularly important as almost all information security solutions rely on the human element to a large degree (Berti and Rogers, 2004, p 150-151). Therefore, as the corporate culture of an organisation establishes and influences employee behaviour, it should be used to mould the information security behaviour of employees.

Information security is far more than simply applying an assortment of physical and technical controls (Berti and Rogers, 2004, p 147). Information security solutions have been meticulously developed to attempt to protect the information assets of organisations. However, as mentioned earlier, the most significant vulnerability – the human factor – is often left unaddressed. Organisations may not be able to protect the integrity, confidentiality, and availability of information if they do not ensure that all employees involved understand their roles and responsibilities. It is also vital that these same employees are adequately trained to protect the information assets in their organisation (National Institute of Science and Technology Special Publication 800-16, 1998, p 12). Properly trained and diligent employees can become the strongest link in an organisation's security infrastructure (Henry, 2004, p 664). The understanding of employees, with regard to information security, and the resulting behaviour and actions should become second-nature to employees and part of their daily activities. For that

reason, information security practices should become part of the corporate culture of an organisation.

Corporate culture not only places constraints upon the activities and behaviour of employees, it also prescribes what the organisation and its employees must do. Consequently, the corporate culture guides the activities of the organisation and its employees (Beach, 1993, p 11).

However, the question remains – how can information security be incorporated into a corporate culture? Any prospective change in the current corporate culture requires, in essence, the unlearning of beliefs on the part of the employees and could result in a huge amount of anxiety and resistance to change from employees (Schein, 1999, p 25). To change the culture, employees' values, norms and attitudes must change. This is to ensure they make the 'right' contribution to the healthy corporate culture despite any conflict of individual and group interest (Meek, 1988, p 454). The environment that has the most influence on employees' beliefs and attitudes is the environment within the organisation. Therefore, the power to change the culture of an organisation lies largely with senior management (Drennan, 1992, pp 3-4).

As part of its corporate governance duties, it is the duty of senior management to define and express the vision it has for the organisation. Vision defines the ideal future for an organisation. This could imply preserving the current culture, or the vision could imply change. That is, the vision may require no more than the natural evolution of the present culture, or it may require radical changes in what the organisation is doing and the resulting culture (Beach, 1993, pp 49-50). It is vital for senior management to outline its vision for the organisation in terms of information security as well. One of the ways to do this is for management to articulate its vision in a policy. Senior management should demonstrate its dedication to information security by providing its support and commitment towards a formally agreed upon and documented Corporate Information Security Policy, as it is one of the controls that is regarded as best practice in terms of information security (BS 7799-1, 1999, p 4). The core objective of any policy is to influence and determine the decisions, actions and behaviour of employees by specifying what behaviour is acceptable and what behaviour is unacceptable (Whitman & Mattord, 2003, p 194). Therefore, by creating the policy through its governance duties, senior management is initiating the shaping of the corporate culture to include information security.

This results in the amalgamation of corporate culture, information security and corporate governance and is termed Information Security Obedience. In previous work, Thomson and von Solms defined Information Security Obedience as 'de facto user behaviour complying with the vision of senior management as defined in the Corporate Information Security Policy' (Thomson and von Solms, 2005, p 74).

The rest of the paper will detail the Model for Information Security Shared Tacit Espoused Values or the MISSTEV Model and its components that could assist organisations in achieving Information Security Obedience. The two components, the Conscious Competence Learning Model and the Modes of Knowledge Creation, will be examined, followed by an explanation of the MISSTEV Model itself.

3. Conscious Competence Learning Model

The first component of the MISSTEV Model is the Conscious Competence Learning Model. The model describes the process and stages of learning a new skill or behaviour and is partitioned into four stages, which progress from Unconscious Incompetence to Unconscious Competence. These four stages will be detailed in the following section (Chapman, 2001, online).

3.1 The first stage is *Unconscious Incompetence*. People at this stage are not aware of the existence of the particular skills that are required from them. In other words, they do not know that they lack particular skills or types of behaviour. It is possible that they might deny the practicality and usefulness of the new skills. In order to learn new skills, it is vital that people become aware of the necessity to learn something new (Chapman, 2001, online). For example, a person who has never attempted driving a car is not aware of all the skills, and knowledge of the road, required to be licensed driver.

3.2 The second stage is *Conscious Incompetence*. At this stage, people become aware of the existence of the relevant skills they should possess. They have realised their inadequacies and should be able to assess the level of skills that is required for their own competence (Chapman, 2001, online). For example, a person who has passed the learner drivers test is now aware of the skills and knowledge required to drive a car, but has not acquired those skills as yet.

3.3 The third stage is *Conscious Competence*. People at this stage have acquired the new, necessary skills. However, people still have to concentrate on performing these skills and, therefore, the skills are not second-nature as yet. In other words, people cannot perform these skills without having to think about them and the skills are not part of their behaviour (Chapman, 2001, online). For example, a person who has recently obtained a driver's license, has acquired the necessary skills to drive a car, but still has to concentrate on changing gears, using the clutch and remembering to look in the rearview mirror.

3.4 The final stage is *Unconscious Competence*. By this stage, the skills learned at the *Conscious Competence* stage have become so practiced that people no longer have to think about how to perform them. The skills have become second-nature or part of the actions and behaviour of people at this stage and have become largely instinctual (Chapman, 2001, online). For example, for a person who is an

experienced driver, the skills required to drive a car have become automatic to a large extent.

Therefore, whenever a new skill or set of skills must be learnt, people will naturally progress through the four stages of the Conscious Competence Learning Model.

4. Modes of Knowledge Creation

The second component of the MISSTEV Model is Nonaka's Modes of Knowledge Creation. The Knowledge Creation process comprises tacit knowledge and explicit knowledge, as well as the knowledge conversion steps that must occur for one type of knowledge to be translated into the other.

Tacit, or implicit, knowledge is subjective and experience based. This knowledge is difficult to formalise and communicate and includes beliefs, attitudes and intuition, as well as technical skills. Knowledge in the tacit form is actionable, or can be used, by the owner (Nonaka, 1994, p 16). Explicit, or overt, knowledge, on the other hand, is objective and rational knowledge that can be communicated in words and sentences and includes theoretical approaches and problem solving (Nonaka, 1994, p 16). The purpose of Nonaka's Modes of Knowledge Creation is to identify existing knowledge and 'convert' it to new knowledge. This is done by classifying four processes of interaction between tacit and explicit knowledge. These processes are classified as Socialization, Externalization, Combination and Internalization (Nonaka, 1994, p 18).

4.1 *Socialization* is the process whereby one person's tacit knowledge is transferred to tacit knowledge in another person. Socialization involves capturing knowledge through direct interaction with individuals both inside and outside an organisation. Socialization depends on having shared experience, and results in acquired skills and common mental models. Socialization is primarily a process between individuals (Nonaka, 1994, p 19).

4.2 *Externalization* is the process whereby tacit knowledge is made explicit. One way to do this is through 'articulation' of tacit knowledge by expressing beliefs and values in words, metaphors or analogies. A second way is through 'eliciting and translating' the tacit knowledge of others into an understandable form or explicit knowledge. Dialogue and discussion are important means for both methods. During such communication, people share beliefs and can learn how to better articulate their thinking. Externalization is a process among individuals within a group (Nonaka, 1994, p 19).

4.3 Once knowledge has become explicit, it can be transferred to explicit knowledge through a process Nonaka calls *Combination*. Explicit knowledge can be conveyed in, for example, documents and email, as well as through meetings and

training. The collection and dissemination of relevant information becomes very significant in this process. Combination allows knowledge transfer among groups across organisations (Nonaka, 1994, pp 19-20).

4.4 *Internalization* is the process of understanding and absorbing explicit knowledge into the tacit knowledge held by an individual. Internalization is largely practical as explicit knowledge is transferred to tacit through the actual doing of a task or skill or through simulations. The internalization process transfers organisation and group explicit knowledge to the individual (Nonaka, 1994, p 20).

The four processes of interaction between tacit and explicit knowledge are represented in Figure 1. It shows that the Socialization process transfers Tacit Knowledge to Tacit Knowledge. The Externalization process transfers Tacit Knowledge to Explicit Knowledge. The Internalization process transfers Explicit Knowledge to Tacit Knowledge. And the Combination process transfers Explicit Knowledge to Explicit Knowledge.

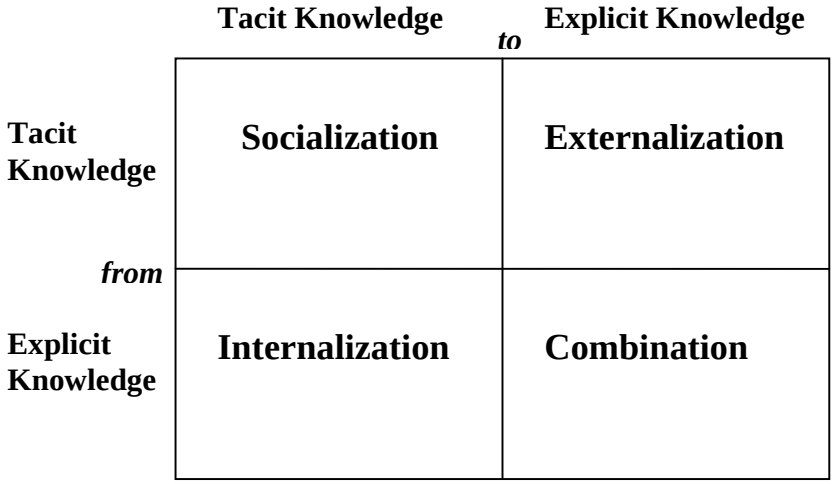

Figure 1: Nonaka's Modes of Knowledge Creation

The interactions between tacit knowledge and explicit knowledge will tend to become larger in scale and faster as more individuals in the organisation become involved in the knowledge conversion or creation processes. Therefore, organisational knowledge creation can be seen as an increasing spiral process, starting at the individual level moving up to the collective or group level, and then, ultimately, to the organisational level (Nonaka, 1994, p 20). Therefore, through Nonaka's Modes of Knowledge Creation, an organisation can create and disseminate new knowledge.

5. Model for Information Security Shared Tacit Espoused Values or MISSTEV Model

As detailed previously, if the de facto employee behaviour complies with the vision of senior management, which should be detailed in the Corporate Information Security Policy, then Corporate Information Security Obedience is evident in the organisation. The following section integrates the Conscious Competence Maturity Model and the Modes of Knowledge Creation, both discussed in previous sections, into the Model for Information Security Shared Tacit Espoused Values or MISSTEV Model. This MISSTEV Model details the progression from the development of the Corporate Information Security Policy to the realization of Corporate Information Security Obedience. The MISSTEV Model is shown in Figure 2.

Appendix E

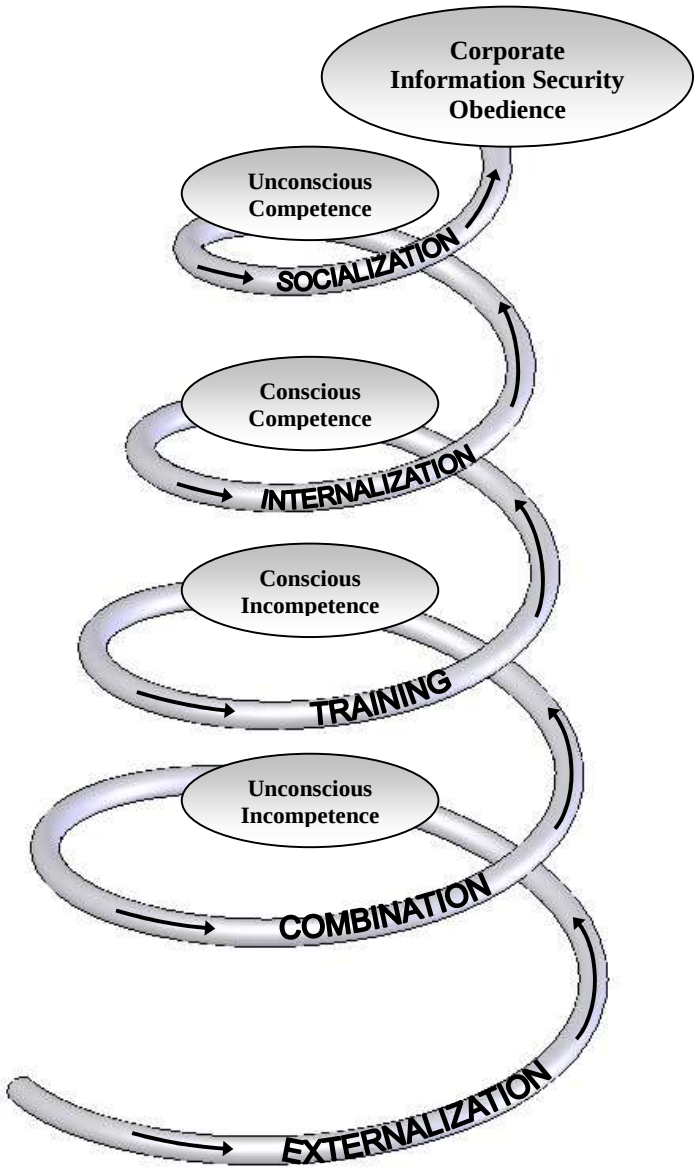

Figure 2: MISSTEV Model

The foundation of the MISSTEV Model is the Corporate Information Security Policy. As described previously, it is through this policy that senior management should illustrate its vision for information security within its organisation.

The tacit knowledge, or vision, of senior management should be translated into explicit knowledge through the creation of the Corporate Information Security Policy and through the process of *externalization*.

Once the vision of senior management has been externalized, the Corporate Information Security Policy must be introduced to the employees of the organisation. In terms of information security, these employees are at the *Unconscious Incompetence* stage, as shown in Figure 2, as they are unaware of their information security roles and responsibilities.

The information security vision of senior management should now be explicit knowledge through the Corporate Information Security Policy and should be transferred to employees through the process of *combination*. As detailed previously, *combination* allows knowledge transfer among groups across organisations. The explicit knowledge of senior management, or in other words, the Corporate Information Security Policy, should be transferred to the explicit knowledge of employees through an Information Security Awareness Program. The purpose of an Information Security Awareness Program is merely to focus attention on security and make employees aware of the skills they need to adequately protect information assets (National Institute of Science and Technology Special Publication 800-16, 1998, p 15). It is vital at this stage that employees realise what is required from them, and why the protection of information is so vital to the protection of an organisation. Therefore, through the process of *combination*, employees should realise their inadequacies when it comes to the protection of information and should move to the *Conscious Incompetence* stage of the MISSTEV Model.

Once at the *Conscious Incompetence* stage, and in order to progress to the next stage in the MISSTEV Model, employees must be trained in information security practices. All employees need basic training in information security concepts and procedures. The National Institute of Science and Technology (NIST) recommends three levels of training: Beginning, Intermediate and Advanced, with each level linked to the roles and responsibilities of the employees (National Institute of Science and Technology Special Publication 800-16, 1998, p 5). Once employees have been trained in their particular information security roles and responsibilities, and have acquired the necessary skills, they should progress to the *Conscious Competence* stage of the MISSTEV Model.

Once the necessary information security skills have been transferred to employees through training, the process of *internalization* will facilitate the absorbing of this explicit knowledge into the tacit knowledge of employees. The *internalization* process is, for the most part, practical as explicit information security knowledge is transferred to tacit through employees actually performing a task or skill. However, employees will not internalize these skills and their responsibilities if they are not committed to and do not fully understand their role in the protection of information.

Internalization guides employees to the *Unconscious Competence* stage of the MISSTEV Model. Through *internalization*, employees should fully understand and support the information security vision of senior management and, by this stage, the information

security skills should have become so practiced that they are second-nature to the employees. In order for employees to remain at the *Unconscious Competence* stage, the tacit information security knowledge that has been learnt and absorbed through the MISSTEV Model should be transferred to the tacit knowledge of other employees through the process of *Socialization.* Over time, this should ensure the evolution of the *Unconscious Competence* stage into Corporate Information Security Obedience as shown in Figure 2. Once Information Security Obedience has evolved in an organisation, success has been achieved. The ultimate vision of senior management for information security has been realised in the organisation.

6. Conclusion

One of the biggest issues facing an organisation's information is the lack of knowledge, skills and commitment by employees when it comes to the protection of information. In order for employees to become more knowledgeable about and committed to the protection of information, knowledge creation and transferal is necessary. This is possible through Nonaka's Modes of Knowledge Creation between tacit and explicit knowledge as discussed in the paper. In addition, as knowledge is created and disseminated, employees move through the stages of the Conscious Competence Learning Model. In terms of information security, Nonaka's Modes of Knowledge Creation and the Conscious Competence Learning Model have been integrated into the Model for Information Security Shared Tacit Espoused Values or MISSTEV.

Through the MISSTEV Model, employees should be informed about the information security vision of senior management and their roles and responsibilities to protect information. Further, by following the spiral of the Model, employees should be made aware of and trained in the correct skills necessary to protect information asset, and these skills should become part of the everyday practices of the employees. Ultimately, if all employees follow the spiral of the MISSTEV Model, Corporate Information Security Obedience should become evident in an organisation and the vision of senior management has been realised.

7. References

Beach, L.R. (1993). *Making the right decision. Organizational culture, vision and planning.* Eaglewood Cliffs, New Jersey : Prentice Hall.

Berti, J. and Rogers, M. (2004). Social engineering: the forgotten risk. Information security management handbook – fifth edition. Boca Raton : Auerbach Publications.

Appendix E

BS 7799-1. (1999). *Code of practice for information security management (CoP).* DISC PD 0007. UK.

Drennan, D. (1992). *Transforming company culture.* Berkshire, England : MacGraw-Hill.

Hagberg Consulting Group (2002). *Corporate Culture/Organisational Culture: Understanding and Assessment* [online]. [cited 25 January 2003] Available from Internet: URL http://www.hcgnet.com/html/articles/understanding-Culture.html

Henry, K. (2004). *The human side of information security*. Information security management handbook – fifth edition. Boca Raton : Auerbach Publications.

Chapman, A. (2001). Conscious competence learning model. [online]. [cited 3 October 2004] Available from Internet: URL http://www.businessballs.com/ProcessofchangeJF2003.pdf

Meek, V.L. (1988). Organizational culture: origins and weaknesses. *Organization Studies*, Vol. 9, No. 4, pp 453-473.

Mitnick, K.D. and Simon, W.L. (2002). *The art of deception – controlling the human element of security.* Indianapolis, Indiana : Wiley Publishing, Inc.

National Institute of Science and Technology Special Publication 800-16 (April, 1998). *Information technology security training requirements: a role- and performance-based model.* Washington D.C. : Superintendent of Documents, U.S. Government Printing Office.

Nonaka, I. (1994). A dynamic theory of organizational knowledge creation. *Organization Science*, Vol. 5, No. 1, pp 14-37.

Schein, E.H. (1999). *The corporate culture survival guide.* San Francisco, California, United States of America : Jossey-Bass Publishers.

Thomson, K.L. and von Solms, R. (2005). Information security obedience: a definition. *Computers & Security*, Vol. 24, pp 69-75.

Whitman, M.E. & Mattord, H.J. (2003). *Principles of Information Security*. Kennesaw State University : Thomson Course Technology.