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

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'.

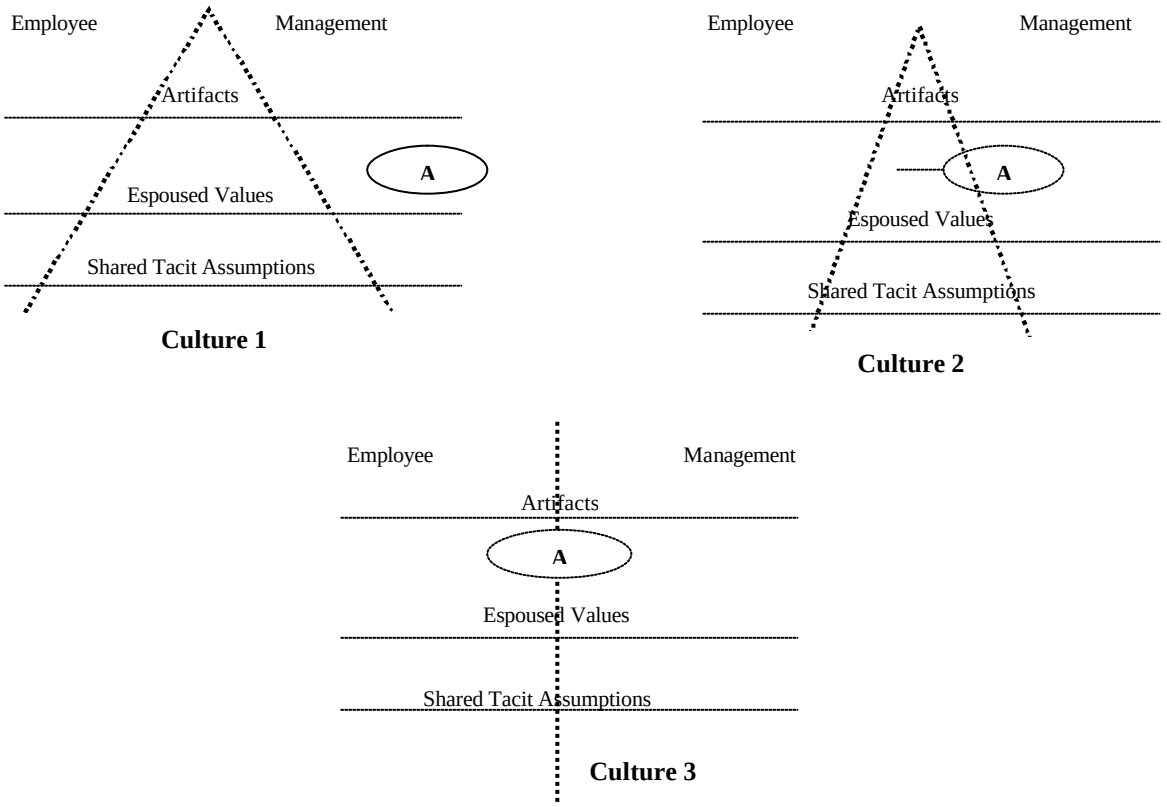

Figure 1: Schein's model expanded into employee and management dimensions

'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.

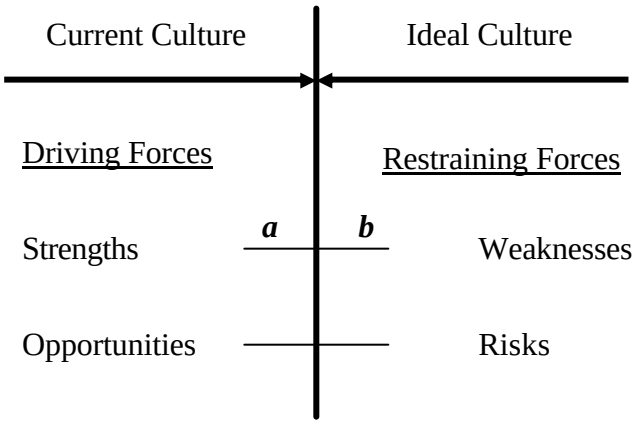

Figure 2: Template for a Force Field Diagram

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).

6.1 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.