TOWARDS CORPORATE INFORMATION SECURITY OBEDIENCE

Kerry-Lynn Thomson and Rossouw von Solms
Port Elizabeth Technikon, South Africa
{kthomson; 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.

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.

3.1 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 (Price WaterhouseCoopers, 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.

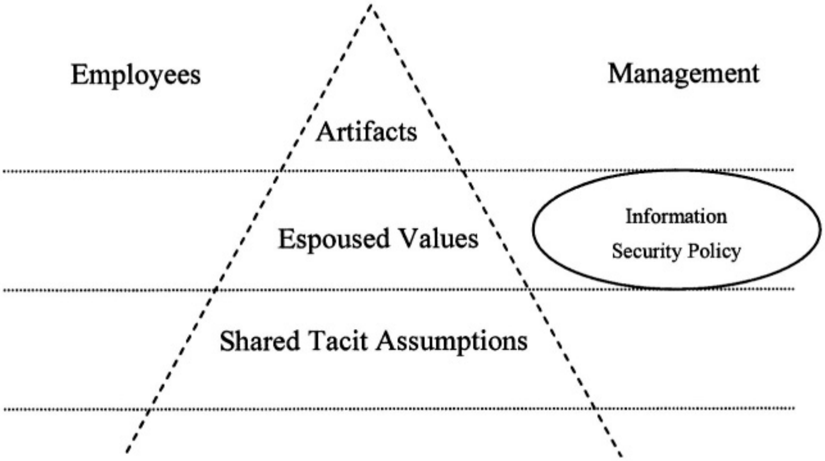

Figure 1. The coercive and utilitarian environments and Schein's model

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).

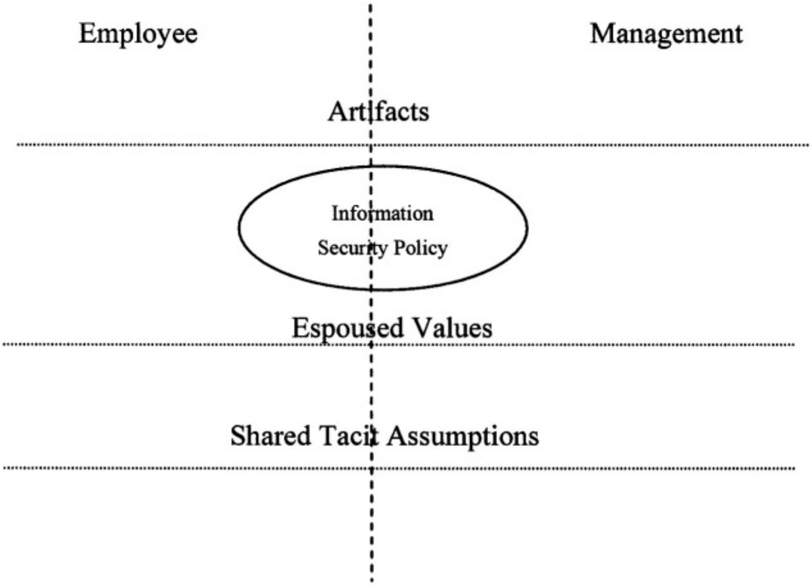

Figure 2. The goal consensus environment and Schein's model

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.

10. 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