Computers & Security (2005) **24**, 69–75

ELSEVIER

Computers & Security

www.elsevier.com/locate/cose

Information security obedience: a definition

Kerry-Lynn Thomson, Rossouw von Solms*

Department of Information Technology, Port Elizabeth Technikon, Private Bag X6011, Port Elizabeth 6000, South Africa

Received 9 September 2004; accepted 18 October 2004
Available online 28 January 2005

KEYWORDS
Corporate governance;
Information security;
Corporate culture;
Information security obedience

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.

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

* Corresponding author. Tel.: +27 41 504 3604; fax: +27 41 504 9604.
E-mail addresses: kthomson@petech.ac.za (K.-L. Thomson), rossouw@petech.ac.za (R. von Solms).

0167-4048/$ - see front matter © 2005 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2004.10.005

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 got 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.

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 well-being 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 and Touche, 2002, online).

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 et al., 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 and 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 and 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 and Mattord, 2003, p. 194).

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 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 have 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.

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 Fig. 1.

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,

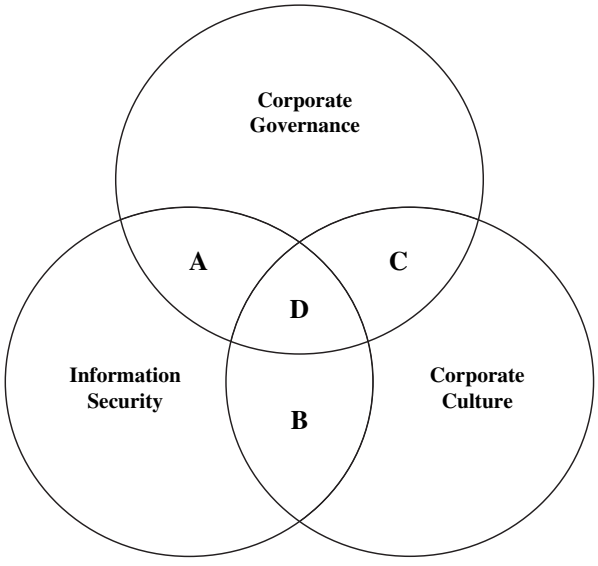

Figure 1 The relationships between information security, corporate governance and corporate culture.

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 and 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 between information security and corporate culture is represented by 'B' in the diagram. 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; the 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 and 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 *shared 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 values* 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 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 and 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 between the three fields of information security, corporate governance and corporate culture is represented by 'D' in the diagram. To be genuinely valuable, information security needs to become part of the way everyone conducts their daily tasks, from senior management, right throughout the entire organisation (Deloitte and 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'.

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 changes 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.

References

Atkinson P. Creating culture change — strategies for success. Bedfordshire, England: Rushmere Wynne; 1997.

Beach LR. Making the right decision. Organizational culture, vision and planning. Eaglewood Cliffs, New Jersey: Prentice Hall; 1993.

Beveridge CAR. Behaviour in organisations. [online] [cited 23 January 2003]. Available from: <http://www.carb.fsnet.co.uk/bio97.pdf>; December, 1997.

Beyer JMHandbook of organizational design. New York: Oxford; 1981.

Blackwell Publishers. [online] [cited 12 January 2002]. Available from: <http://www.blackwellpublishers.co.uk/journals/corg>; 2000.

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

Brooks J. Converging cultures — trends in European corporate governance. [online] [cited 12 February 2003]. Available from: <http://www.tiaa-cref.org/pressroom/corpgov.pdf>; April 1997.

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

Buren A, van der Meer B, Shahim A, Barnhoorn W, Roos Lindgreen E. Information security at top level. In: Information security management and small systems security; 1999. p. 75—6.

Deloitte, Touche. Management briefing — information security. [online] [cited 13 January 2003]. Available from: <http://www.deloitte.com/dtt/cda/doc/content/info_security(1).pdf>; May 2002.

Dictionary.com. [online] [cited 3 July 2003]. Available from: <http://dictionary.reference.com/search?q=obedience>; 2003.

Gordon G. Dozens of threats beset your data. Sunday Times, Business Surveys 2002, May 2;. [online] [cited 17July 2002]. Available from: <http://www.suntimes.co.za/2002/05/12/business/surveys/internet/survey10.asp>.

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

Hagberg Consulting Group. Corporate culture/organisational culture: understanding and assessment. [online] [cited 25 January 2003]. Available from: <http://www.hcgnet.com/html/articles/understanding-Culture.html>; 2002.

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

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

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

Lane VP. Security of computer based information systems. London: Macmillan; 1985.

Martins A, Eloff J. Information security culture. In: IFIP TC11, 17th international conference on information security (SEC2002), Cairo, Egypt. Netherlands: Kluwer Academic Publishers Group; 2002. p. 203—14.

PriceWaterhouseCoopers. Information security breaches survey technical report. [online] [cited 5 January 2003]. Available from: <http://www.security-survey.co.uk>; 2002.

Schein EH. The corporate culture survival guide. San Francisco, California, United States of America: Jossey-Bass Publishers; 1999.

Smith MR. Commonsense computer security. London: McGraw-Hill; 1989.

Whitman ME, Mattord HJ. Principles of information security. Thomson Course Technology, Kennesaw State University; 2003.

World Bank Group. Corporate governance: a framework for implementation — overview. [online] [cited 23 December 2002]. Available from: <http://www.worldbank.org/html/fpd/privatesector/cg/docs/gcgfbooklet.pdf>; 1999, September 20.

Further reading

Bruce G, Dempsey R. Security in distributed computing — did you lock the door? Upper Saddle River, New Jersey: Prentice Hall; 1997.

Drennan D. Transforming company culture. Berkshire, England: MacGraw-Hill; 1992.

Kerry-Lynn is currently a 1st year full-time Doctoral student at Port Elizabeth Technikon. In August 2004, at the 10th IFIP WG 11.1 Annual Working Conference on Information Security Management held in Toulouse, France, she presented the paper 'Towards Information Security Obedience'. In May 2003, at the 18th IFIP International Information Security Conference held in Athens, Greece, she presented the paper 'Integrating Information Security into Corporate Governance'. At the ISSA Conference in 2004, she presented the paper 'Cultivating Corporate Information Security Obedience'. At the ISSA Conference in 2003, she presented the paper 'Creating a Security Conscious Culture through Effective Corporate Governance'. At the ISSA Conference in 2002, she presented a paper entitled, 'Corporate Governance: Information Security the Weakest Link?'. She is a qualified CCNA Instructor for the Cisco Networking Academy Program.

Professor Rossouw von Solms is the Head of Department of Information Technology at Port Elizabeth Technikon, in South Africa. He holds a PhD from the Rand Afrikaans University. He has been a member of the International Federation for Information Processing (IFIP) TC 11 committee since 1995. He is a founder member of the Technikon Computer Lecturer's Association (TECLA) and is an executive member ever since. He is also a vice-president of the South African Institute for Computer Science and Information Technology (SAICSIT). He has published many papers in international journals and presented numerous papers at national and international conferences in the field of Information Security Management.