CORPORATE GOVERNANCE: INFORMATION SECURITY THE WEAKEST LINK?

KERRY-LYNN THOMSON AND ROSSOUW VON SOLMS
Port Elizabeth Technikon, s9942984@petech.ac.za, rossouw@petech.ac.za

Key words: Corporate Governance, Information Security, Accountability, Responsibility

Abstract: Information is an important asset of any organisation and the protection of this asset, through information security is equally important. This paper examines the relationship between corporate governance and information security and the fact that top management is responsible for high-quality information security.

1. INTRODUCTION

Corporate governance relates to the responsibilities of the Board of Directors and top management of a company. Corporate governance states that an effective Board that can both lead and control the company should head all companies. The Board has a collective responsibility to provide effective corporate governance (von Solms, 2001, p 505). The question is, to what extent is information security part of corporate governance?

Information security is that discipline concerned with the implementation and support of security and control procedures to protect the confidentiality, integrity and availability of electronically stored information (British Standards Institute, 1999, p 1). *Confidentiality* of electronic assets is concerned with ensuring that information of a specific classification is not circulated to persons outside the category for which it is classified. In other words, sensitive information must be prevented from being disclosed to unauthorised parties (Krige, 1999, p 8; Bruce & Dempsey, 1997, p 36).

Integrity of electronic assets 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). *Availability* of electronic assets is concerned with guaranteeing the availability of systems and data on a timely basis such that strategic and business decisions can be effected as rapidly as possible (Bruce & Dempsey, 1997, p 41).

Information and information security has grown in importance in our ever-changing world. The well-being of an organisation depends principally on quality information and the security thereof. Taking the importance of information and information security into account, it can be argued that currently information security forms the weakest link in corporate governance.

The purpose of this paper is to investigate the accountability and responsibility of the top management of an organisation with regard to information security. It will be explored who is responsible and who can be held accountable if there are breaches in information security. This will help accentuate the link between corporate governance and information security.

2. CORPORATE GOVERNANCE

According to Bob Garratt, author of “The Fish Rots from the Head”, corporate governance states that Boards of directors are not there only to manage a company through its day-to-day operations, but also to lead it through "direction giving" and strategy implementation (Planting, 2001, online).

2.1 IMPORTANCE OF CORPORATE GOVERNANCE

First-rate corporate governance is extremely important to shareholders, as is demonstrated by a survey conducted by McKinsey & Co., released in June 2000. McKinsey & Co., working with Institutional Investors Inc., found that more than 84% of the approximately 200 global institutional investors, showed a readiness to pay a premium for the shares of a well-governed company over one deemed poorly governed, but with a equivalent financial record. Three-quarters of these investors specified that Board practices were at least as imperative as financial performance, when assessing companies for possible investment. So by simply developing good governance practices, managers can potentially add considerable stakeholder value (King Report, 2001, pp 14-15).

2.2 PILLARS OF CORPORATE GOVERNANCE

There are four central pillars of corporate governance, namely; accountability, responsibility, fairness and transparency (King Report, 2001, p 17), which are needed to ensure effective corporate governance.

Accountability means that those individuals or groups in a company who make decisions and take actions on specific issues are accountable for their decisions and actions. Mechanisms must be in place to ensure accountability. This provides investors with the means to question and evaluate the actions of the Board and its committees (King Report, 2001, p 14). The modern approach is for a Board to identify the company's stakeholders and to agree to policies that determine how the affiliation with those stakeholders should be controlled in the interests of the company (King Report, 2001, p 8).

Responsibility, with a view to management, relates to the behaviour that allows corrective action to be taken and penalising mismanagement and misconduct. Responsible management would, when required, put in place what it would take to set the organisation on the right path. While the Board is answerable to the company, it must act responsively to and with responsibility towards all stakeholders of the company (King Report, 2001, p 14).

The difference between accountability and responsibility is that, one is liable to provide an account when one is accountable and one is liable to be called to account when one is responsible. In corporate governance terms, one is accountable by law to the organisation if one is a director and one is responsible to the stakeholders identified as relevant to the organisation (King Report, 2001, p 8).

Fairness must be in practice to ensure balance in the organisation. The rights of various groups have to be recognised and valued. For example, minority shareholder interests must receive equal consideration to those of the dominant shareholders (King Report, 2001, p 14).

Transparency is the ease with which an outsider is able to make significant assessment of a company's actions, its economic fundamentals and the non-financial aspects relevant to that business. This is a measure of how good management is at making necessary information available in an open, precise and timely manner – not only the audit data but also general reports and press releases (King Report, 2001, p 13).

These four pillars of Corporate Governance must be put into practice by those responsible for the well-being of an organisation. The next section deals with identifying who exactly is responsible for Corporate Governance and its implementation.

2.3 STRUCTURE OF CORPORATE GOVERNANCE

The company is run by a Board, which consists of the chairperson, managing director, executive directors and non-executive directors. This is the commonly used Board structure South Africa. An executive director is involved in the everyday management and could be in the full-time employment of the organisation. A non-executive director is not involved in the everyday management and is not a paid employee of the organisation. The Board has a joint responsibility to provide effectual corporate governance, which involves a set of relationships between the management of the company, its Board and its stakeholders (King Report, 2001, pp 45, 56).

The Board must set or approve policies for the guidance of the management appointed by it. The duty of the management or directors is to give effect to the policy prescribed by the Board and to attend to the daily conduct and administration of the business of the organisation (Leveson, 1970, p 52).

The Board is subject to the firm and objective leadership of a chairperson. The most important function of the chairperson is to supervise meetings of directors and to ensure the smooth functioning of the Board in the interests of good governance. The chairperson will also preside over the company's shareholders meetings and acts as the informal link between the Board and management (King Report, 2001, p 51).

Now that Corporate Governance has been discussed in general, it can be discussed in relation to information security. This discussion will explore the current management duties of the Board of Directors and their accountability and responsibility towards information security.

3. CORPORATE GOVERNANCE AND INFORMATION SECURITY

Since 1994, information technology has emerged as a key driving force for an organisation's decisions and strategies (King Report, 2001, p 11). Commercial organisations and governments rely heavily on information to conduct their daily activities. For this reason, it is of extreme importance to protect these information resources from loss of confidentiality, integrity and availability. Protection alone is not sufficient, because the security of the information needs to be managed and controlled properly. 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). The process of protecting these information organisational assets is called information security.

Other important organisational assets are the financial resources, required for the successful operations of an organisation. An external auditor is appointed to examine annual financial statements of an organisation. The external auditor ensures that the company has kept proper accounting records and that the annual financial statements are in agreement with its accounting records and returns (Botha, Oosthuizen & De La Rey, 1987, pp 357-358). The external auditor will give their independent opinion on the organisation's financial statements to the stakeholders (King Report, 2001, p 77). The role of the internal auditor is to provide a service to the company and report any problems or discrepancies to management (King Report, 2001, p 77). Just as the financial state of an organisation is properly governed and protected, so should the informational state.

The problem with protecting information assets, in most cases, is that senior management does not take responsibility for information security or information security is given low priority in the organisation, because the seriousness of protecting information is not emphasised. Information security is not given the attention it deserves. Looking at the following statistic highlights this fact. According to Datamonitor's eSecurity analyst, Ian Williams, more than 50% of businesses worldwide spend 5% or less of their IT budget on security (13 April 2002, online).

3.1 EFFECT OF POOR INFORMATION SECURITY

Poor or no information security has a negative effect on the welfare of an organisation. The integrity of information is essential to the business. If unauthorised parties modify the information used by managers, for example, any decisions made by management could be based on inaccurate information. In the event that systems or data is unavailable, opportunities may be lost, deadlines missed or commitments defaulted. Work progress could be impacted if the information is not available when it is needed.

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). To attempt to avoid a breach in the confidentiality, integrity and availability of the information of an organisation, a carefully planned Information Security Policy is essential.

3.2 INFORMATION SECURITY POLICY

A good understanding of the risks accepted by a company in the pursuit of its objectives, together with the strategies employed to lessen those risks, is essential to the approval of its affairs by the Board and relevant stakeholders (King Report, 2001, p 96). This process of planning, arranging and controlling activities and resources to minimise the impacts of all risks to levels that are acceptable to stakeholders is called risk management (King Report, 2001, p 97). Internal control is the mechanism used to control risk management. Even though risk management should be practised throughout the company, it is ultimately the responsibility of the Board (King Report, 2001, p 96).

The Board is responsible for risk management and the system of internal control, including the establishment and communication of risk and control policies for the entire organisation (King Report, 2001, p 105). Risk management is essentially about protecting the assets of an organisation and, as has already been said, information is an important asset of the organisation. Therefore, the level of information security that the Board of an organisation is willing to recommend and implement, and the level of information security that is acceptable to the stakeholders must be combined in the Information Security Policy created between them (King Report, 2001, p 96).

The chairperson of the Board will delegate implementation and maintenance of the Information Security Policy to the Information Security

Officer (ISO), who is responsible to the Board, should there be any security breaches or other problems related to information security.

If the stakeholders are dissatisfied with the level of information security that is being applied in the organisation, then it is the Board that is responsible to take corrective action. In addition, if legal action is to be taken against the organisation due to a breach in confidentiality, integrity or availability, it is the Board that is to be held accountable. The Information Security Policy should be based on the agreed corporate security objectives and strategy and is there to provide management direction and support for information security (British Standards Institute, 1993, p 17). This relationship between the Board, the stakeholders, the Information Security Officer (ISO) and the court of law and the policy that binds them is represented in Figure 1.

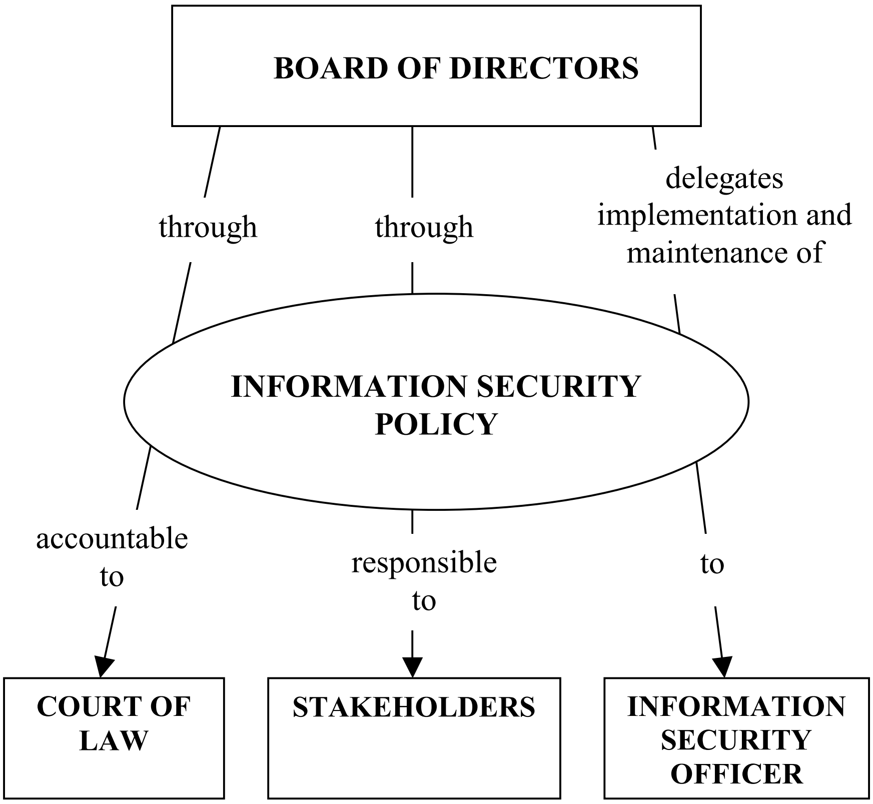
BOARD OF DIRECTORS
through
through
delegates implementation and maintenance of
INFORMATION SECURITY POLICY
accountable to
responsible to
to
COURT OF LAW
STAKEHOLDERS
INFORMATION SECURITY OFFICER

Figure 1. Flow of relationships involving the Information Security Policy

The Board of an organisation must demonstrate that they are taking steps to address information security to avoid legal liability. It is becoming increasingly evident that a court of law may go behind the "corporate personality" of the company and find individuals, particularly members of management, who can be held accountable for breaches in the information security policy. The basis for this liability could be negligence, breach of fiduciary duty or failing to take corrective action once there was a compromise in security (Wood, 1999, p 4).

If there is breach in security, it is important for the management of the organisation that is held accountable for the breach, to be able to demonstrate that the procedures and statements outlined in the Corporate Information Security Policy adhere to international standards, such as the ISO/IEC 17799. These international standards ensure that most information security risks are addressed, through internationally accepted means, in the organisation's policy. However, fulfilment of a standard does not provide immunity from legal obligations (BS 7799-1, 1999, p iii).

4. CONCLUSION

Even though information is an important organisational asset and is essential to the continuance of organisations, information security is not given the attention it deserves. In many situations it is still seen as the responsibility of the Information Technology department and not a management concern.

From the discussion above, it is evident that information security is a direct corporate governance concern. The Board of Directors of an organisation can be held responsible by the stakeholders or accountable by a court of law for a lack of information security.

Further research will investigate the Information Security Policy in more detail. The policy will be researched in terms of who should be involved in the creation of the policy and what should be included to make the policy acceptable to all. Various laws applicable to information technology and security will also be investigated, together with the role that management must play in the adherence of these laws.

5. REFERENCES

Barnard, L. (1998). The Development of a Model for the Effective Evaluation of Information Security in an Organization. Unpublished master's thesis. Port Elizabeth Technikon, Port Elizabeth, South Africa.

British Standards Institute. (1993). Code of Practice for Information Security Management (CoP). DISC PD 0003. UK.

Bruce, G. & Dempsey, R. (1997). Security in Distributed Computing – Did you lock the door?. Upper Saddle River, New Jersey : Prentice Hall.

Botha, D.H., Oosthuizen, M.J., De La Rey, E.M. (1987). Corporate Law. Durban, South Africa : Buttersworth.

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.

Datamonitor (2001). [online]. [cited 13 April 2002] Available from Internet: URL http://www.datamonitor.com/viewnewsstory.asp?id=1375

Gerber, M. & von Solms, R. (2001). From Risk Analysis to Security Requirements. Computers & Security, Vol. 20, No. 7, pp. 577 – 584.

Krige, W. (1999). The Usage of Audit Logs for Effective Information Security Management. Unpublished master's thesis. Port Elizabeth Technikon, Port Elizabeth, South Africa.

Planting, S. (2001, March 9). Giving Boards A Workout - The Fish Rots From The Head. Future Company [online]. [cited April 27, 2002] Available from Internet: URL http://www.futurecompany.co.za/2001/03/09/reviewb.htm

South Africa. King Committee on Corporate Governance. (2001). King Report on Corporate Governance for South Africa 2001.

Von Solms, B. (2001). Information Security – A Multidimensional Discipline. Computers & Security, Vol. 20, No. 6, pp. 504 – 508.

Leveson, G. (1970). Company Directors – Law and Practice. Durban, South Africa : Buttersworth.

Wood, C.C. (1999). Information Security Policies Made Easy. Baseline Software.