INTEGRATING INFORMATION SECURITY INTO CORPORATE GOVERNANCE

Kerry-Lynn Thomson and Rossouw von Solms
Port Elizabeth Technikon,South Africa, s9942984@student.petech.ac.za, rossouw@petech.ac.za

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.

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

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

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35691-4_52
D. Gritzalis et al. (eds.), *Security and Privacy in the Age of Uncertainty*
© IFIP International Federation for Information Processing 2003

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 is 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 in 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 shareholder 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 shareholders 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 shareholders 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 in 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 shareholders (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 shareholders (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).

For years, this financial culture has been nurtured in organisations – nearly everyone knows how important the financial assets are to an organisation. It is time for this culture to be extended to information security and just as the financial state of an organisation is properly governed and protected, so should the informational state.

"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" (A Call to Action for Corporate Governance, March 2000, online).

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. 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).

The lack of attention given to information security is also stressed with a comment from KPMG in their Global Information Security Survey – "Without Board level commitment and drive, security will always be seen as a technology issue and not give the necessary resources and attention to ensure that risks are effectively minimised" (CD-ROM, 2002).

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 corporate information security policy is essential.

3.2 Corporate 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 shareholders 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 shareholders must be combined in the corporate 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. This, however, does not mean that the board is no longer responsible for the information security policy.

When directors delegate part of their duties to the ISO, or other managers, these directors should firstly take their duties towards the organisation into account. This is for the reason that directors may only circumvent liability in a court of law if they can prove that they have acted in the *bona fide* interest of the organisation and with the obligatory care, skill and diligence (Coetzee, 2002, online).

If the shareholders are dissatisfied with the level of information security that is being applied in the organisation, then it is the Board that should be 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 should be the Board that is held accountable.

If legal action is taken against an organisation because of information security breaches, it is imperative that the Board of Directors has a 'defence' to protect itself from prosecution. This 'defence' must show that the Board of an organisation is 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 failure to take corrective action once there was a compromise in security (Wood, 1999, p 4).

The corporate information security policy should be used as this 'defence' for the Board of Directors. The corporate 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). The policy should identify all those controls that need to be in place in an organisation to ensure effective information security. Once the policy has been created, the Board must ensure that the necessary resources and manpower are available to enforce those controls identified in the policy.

However, it is not enough for an information security policy to simply be created and implemented in an organisation. If this policy is created internally and not compared to other policies that are effectively working in other organisations or countries, then the policy may not be successful. The organisation should be required to ensure that the policy meets specific requirements and that a certain level of information security is provided. This can be achieved by guaranteeing that the policy complies with certain codes of practices or standards, such as ISO/IEC 17799. If there is breach in security, it is important for the management of the organisation, which 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. 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).

The FBI's Chief Information Officer (CIO) Darwin John, gives his opinion on the role that information technology should play in an organisation. Darwin says that "I have always believed that an IT plan is not standalone but a plank in the larger plan for the enterprise" (15 July 2002, online). This relationship between the Board, the shareholders, the Information Security Officer (ISO) and the court of law and the policy that should bind them is represented in Figure 1.

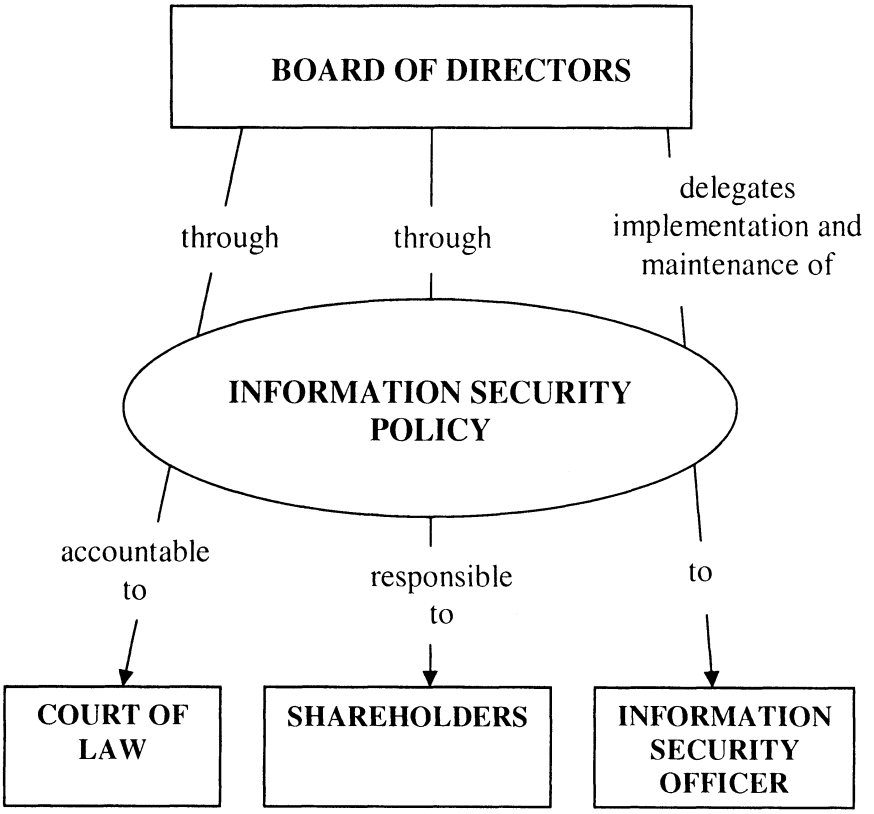

Figure 1. Flow of relationships involving the information security policy

The relationship between the Board of Directors, the court of law and the shareholders through the corporate information security policy should be strengthened if the policy adheres to an international code of practice. The Board must provide the necessary resources to the information security officer to enable the officer to fulfill security tasks. Once successful information security relationships between the Board of Directors and the various parties have been established through the security policy, the entire information security implementation and process needs to be audited. The information security auditing process of any organisation is of extreme importance in guaranteeing that information security controls are achieving their purpose and is continually evolving (National State Auditors Association and US General Accounting Office, 2001, p 8). The Board of Directors must make certain that the information security auditing process is

functioning properly and that the information they receive as a result of this process is put to good use.

Michael Cangemi, President of Etienne Aigner Group Inc., has the following to say about the level of consideration that must be given to information security. Cangemi says that, "In today's economy, and with reliance on IT for competitive advantage, we simply cannot afford to apply to our IT anything less than the level of commitment we apply to overall governance" (14 July 2002, online).

Increasingly, trends around the world are moving in the direction that laws are being passed to protect, for instance, client information. The Healthcare Industry Privacy and Accountability Act (HIPAA) from the USA, protects the confidentiality and integrity of health information during both, storage and transmission. Legal action can be taken against those organisations that do not adhere to the conditions of the act. This would mean that the Board of Directors would, at least, have to explain the breaches in information security in a court of law (Von Solms, 2002, online).

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 shareholders or accountable by a court of law for a lack of information security.

5. REFERENCES

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.

Coetzee, J. (2002). Presentation on King II at ISSA 2002. [online]. [cited 31 July 2002] Available from Internet: URL http://csweb.rau.ac.za/ifip/issa2002/presentations/Johan%20Coetzee.doc

Corporate Governance Institute (2002). [online]. [cited 14 July 2002] Available from Internet: URL http://csweb.rau.ac.za/ifip/issa2002/presentations/Basie%20von%20Solms.ppt

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

Farber, D. (2002, July 15). Unplugged: FBI CIO Darwin John. *ZDNet* [online]. [cited 25 July 2002] Available from Internet: URL http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2874158-2,00.html

Global Information Security Survey [CD-ROM]. (2002). South Africa: KPMG.

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

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.

McKinsey & Company (USA) (2000, June). Investor Opinion Survey. [online]. [cited 22 April 2002]. Available from Internet: URL http://www.gcgf.org/docs/72CGBrochure.PDF

National State Auditors Association and US General Accounting Office (2001, December 10). *Management planning guide for information systems security auditing* [online]. [cited 11 October 2002] Available from Internet: URL http://www.gao.gov/special.pubs/mgmtpln.pdf

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

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

South Africa. King Committee on Corporate Governance. (2001). *King report on corporate governance for South Africa 2001.*

Von Solms, B. (2002). *Corporate governance, IT governance and information security.* [online]. [cited 16 July 2002] Available from Internet: URL http://csweb.rau.ac.za/ifip/issa2002/presentations/Basie%20von%20Solms.ppt

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.