Corporate Governance and Information Security

Prof. Basie von Solms

Chairman: Rand Afrikaans University — Standard Bank Academy for Information Technology, Johannesburg, South Africa, basie@rkw.rau.ac.za

Introduction

The purpose of this paper is to try to create a direct relationship between corporate governance and information security. In doing this the paper tries to make a case why senior management in a company has no choice but to be committed and responsible for information security, simply because by law they are committed and responsible for good corporate governance in their companies.

We start off by an overview about the importance of information security to companies, and the essential responsibility of senior management commitment to information security. This overview is based on a number of quotes from related documents.

We then investigate references to information security, directly and indirectly, as it appears in relevant documents on corporate governance. Then, we try to create a relationship between corporate governance and information security, and finally we conclude with a statement that should be included in some way in documents on good corporate government.

The importance of information security

There can be no doubt anymore that information security, seen as the discipline to ensure the confidentiality, integrity and availability of electronic assets, is today an extremely important aspect in the strategic management of any company. This section does, therefore, not promote why information security is important to an enterprise — there should be no need to do that — but only emphasizes this fact by referring to a few relevant quotes.

"(Information) Security is seen as fundamental to SWIFT's business, second only to availability." [1]

"I believe that senior management have never been so dependent on information security as they are today. All signs are that this dependency can only increase." [2]

"In Australia, for example, every company, by law, must have an official (Information) Security Policy and Acceptable Internet Usage Policy in place." [3]

It is also a known fact that the important strategic role of information security is only really established in a company once senior management gives it full support and commitment. Information security has long ago moved away from being only a technical issue, and has really today become a management issue. This can also be supported by many statements, of which the following will suffice.

"Most importantly, it is about ensuring that the policy on information security management has the commitment of senior management. It is only when these procedural and

management issues have been addressed that organizations can decide on what security technologies they need." [4]

"(IT) Security is part of the business and it is imperative to assign responsibility for managing information security to Board level as information it is a valuable and critical corporate Asset." [5]

The author of this paper is of the opinion that information security has even moved past this management issue, and that information security has now become an institutional issue [6].

From the statements above, we can safely assume, without much controversy, that information security is strategically very important, and that senior management has an pivotal role to play in establishing and managing information security in a company.

However, the problem is that in many companies senior management does not have this commitment and responsibility towards information security, making it very difficult for an information security officer to roll out information security on a sustained company-wide basis.

In many cases on senior management and specifically on Board level, information security is seen as a technical issue, which must be delegated to the IT section, and forgotten about. Without this management support, information security managers fight a very difficult, and often losing, battle in implementing and rolling out a enterprise-wide information security plan in the company, taking into account all the different dimensions of information security like the human (personnel) dimension, the awareness dimension, the legal dimension, the policy dimension, the measurement and monitoring dimension etc.

The burning question very often is: "How can senior management be 'forced' to accept this responsibility?"

The next paragraph tries to link this responsibility to the wider responsibility every senior management member of a company has — that of good corporate governance.

Corporate Governance

Let us start off by examining a few statements from internationally accepted documents on corporate governance.

"The quality of information depends on the standards under which it is compiled and disclosed. These Principles support the development of high quality internationally recognized standards, which can improve the comparability of information between countries." [7]

"The Board should ensure that the technology and systems used in the corporation are adequate to properly run the business for it to remain a meaningful competitor. The development of electronic information and technology in the 20th Century has been significant, and the advances in the next millennium are anticipated to be momentous. Competitive advantages may well be derived by a corporation's strategy regarding its use of information technology, and technology generally, is it electronic or otherwise, in the efficient utilization of its assets and processes. Consequently, a Board has the responsibility to ensure that its management information systems, internal controls and technology relevant to the corporations business, are not only updated so that the corporation remains competitive, but are of such a nature that they cope with the planned strategy of the business enterprise in an increasingly competitive world without barriers." [8]

Some questions which the Board may wish to consider...

"Does the company communicate to its employees what is expected of them and the scope of their freedom to act? This may apply to areas such as customer relations, safety and environmental protection, security of tangible and intangible assets, business continuity issues, expenditure matters, accounting and financial and other reporting." [9]

These statements refer, though often indirectly, to the protection and proper operation of information systems — i.e. the protection of the confidentiality, integrity and availability of information and information systems. This is what the discipline of information security is all about.

How can a Board perform the responsibilities mentioned above if they take no responsibility for information security, or delegate it so low down in the organization (because it is a technical issue (sic)!), that they have no idea about the way their information resources is protected? If we can link good corporate governance more directly to information security, senior management will have to face this responsibility more directly. Can we therefore link corporate governance more directly to information security? Let's try!

Corporate Governance, Internal Controls and Information Security

In this paragraph we move from corporate governance, via internal controls, to information security. Again we use a number of statements from relevant publications.

"The corporate governance framework should ensure the strategic guidance of the company, the effective monitoring of management by the board, and the board's accountability to the company and the shareholders. To achieve this, the board should 'ensure the integrity of the corporation's accounting and financial reporting systems, including independent audit, and that the appropriate systems of (internal) control are in place'..."[7]

From the quote above, and from those found in many related documents, it is very clear that a proper system of internal controls is an essential part of corporate governance.

The following quote builds the bridge we need.

"Following widely publicized failings, there have been other moves to make directors and senior executives personally accountable for the consequences of failure of internal controls. Internal controls ultimately relies on information security..." [2]

Using the simple transitive rule, because corporate governance includes the responsibility for solid internal controls, and internal controls rely on information security, information security is an integral part of corporate governance, be it indirectly.

The following quote also makes a very direct link:

"The information possessed by an organization is among its most valuable assets and is critical to its success. The Board of Directors, which is ultimately accountable for the organization'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." [10]

Everything discussed above makes it abundantly clear that good corporate governance directly includes total commitment and responsibility towards information security, and justifies the following statement:

"Information security is a direct corporate governance responsibility and lies squarely on the shoulders of the Board of the company."

Why then do we not find any direct reference to information security in the most documents on corporate governance? Is it because of this indirect relationship? *Should* we find more direct reference to information security in documents on corporate governance?

Conclusion

The reason for the lack of direct reference to information security in good corporate governance documents, may be because when they were complied, information security had not been such an important issue. Whatever the reason, whenever they are rewritten and updated, the role and importance of information security as an integral part of information security should be clearly noted.

From the discussion above, the author has no doubt that information security should be addressed directly, and by name, in all documents describing good corporate governance. This will clearly indicate the role senior management and the Board have to play, and will greatly simplify the efforts of information security managers.

References

[1] Eric Guldentops, Director of Global Information Security of SWIFT (The Society for World Wide Interbank Financial Telecommunications), Reference unknown.
[2] *Computers & Security*, 15, 1996.
[3] *Computerweek*, South Africa, 16 October 2000.
[4] UK Department of Trade and Industries, Information Security Breaches Survey 2000.
[5] 'Time to elevate IT Security to the Boardroom', eSecure, South Africa, August 2000.
[6] Information Security: The Third Wave? *Computers & Security*, 18, 2000.
[7] OECD Principles of Corporate Governance, April 1999.
[8] Principles for Corporate Governance in the Commonwealth, 1999.
[9] Turnbull Report on Corporate Governance (Internal Control: Guidance to Directors on the Combined Code), 1999.
[10] A Call to Action for Corporate Governance, March 2000, IIA, AICPA, ISACA, NACD, Reference unknown.