CORPORATE INFORMATION SECURITY GOVERNANCE: A HOLISTIC APPROACH

Lynette Mears [a] and Rossouw von Solms [b]

[ab]Department of Information Technology, Port Elizabeth Technikon, South Africa
[ab]041 504 3453, Private Bag X6011, Port Elizabeth,6000

[a]lynne@petech.ac.za, [b]rossouw@petech.ac.za,

ABSTRACT

Information is the considered by some to be one of the most valuable assets that a corporation has. The assurance of the protection of this valuable asset should not be left to the chief information officer of a company, but should be treated as a governance issue. Relevant aspects to corporate information security governance include accountability to shareholders, compliance with legal requirements, setting of well-planned security policies, spearheading security awareness and education, defining roles and responsibilities within the organizational structure, contingency planning and instituting of best practice standards. To ensure that all aspects of corporate information security governance are covered adequately, a number of pertinent questions need to be asked by the different levels of authority within the corporation, and reliable, clear answers need to be provided by the organization. What are these questions and what answers will satisfy these questions? This paper will attempt to shed some light on these questions.

KEY WORDS

Information Security, Corporate Governance, Accountability, Responsibility, Awareness, Risk Management, Ethics, and Best Practices

CORPORATE INFORMATION SECURITY GOVERNANCE: A HOLISTIC APPROACH.

1 INTRODUCTION

"*Just as an audit committee does no auditing, a Board of Directors cannot provide information security. But by asking trenchant questions and insisting on clear, responsible answers, the Board can provide a level of needed oversight to this vital business function that is adequate and necessary, and in doing so, exercise its essential duty of care*." (Institute of Internal Auditors, 2001).

Information security has moved away from its technical image and has become a governance issue. It has become "a direct corporate governance responsibility and lies squarely on the shoulders of the Board of the company." (von Solms, 2001a). The Board therefore needs to ensure that their information resource is adequately protected. To facilitate this, they need to ensure that the right questions are asked, to which adequate and complete answers need to be received from various levels of information users, custodians and managers.

A bi-directional relationship of information flow exists between all levels of authority within a corporation, from shareholder to general employee, and within that relationship lies the need for clear, concise, accurate and timeous information and reporting mechanisms. It is imperative therefore that all corporate employees, from Board members to general employees, be aware of the importance of their contribution to the corporation's information security. It is from this holistic standpoint that each level of authority, responsibility and accountability within the corporate structure will be examined, and each level's required contribution to ensure optimum corporate information security governance will be identified.

This paper will focus on:

a) the primary relationships between the relevant parties of the corporation, their functions and information flow,
b) the broad aspects relating to the information security governance, and
c) typical questions to be asked by the different levels of authority to ensure the effective governance of the corporation's information assets.

2 PRIMARY RELATIONSHIPS BETWEEN THE RELEVANT PARTIES WITHIN A CORPORATION

Typically a corporation will have relationships between shareholders and the Board of Directors, and between the Board of Directors and the Chief Executive Officer (CEO). The CEO will in turn have a direct relationship with his/her division heads, who interface with the general employees (King Report, 2002, pp 21-25).

Figure 1 illustrates the flow of information and relationships within the corporation:

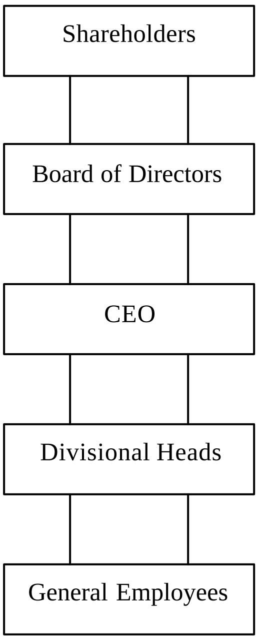

Figure 1: The flow of information and relationships between the different levels of authority within a corporation

As can be seen in Figure 1, the different levels of authority rely almost exclusively on the exchange of information between the parties. A brief description of the relationships follows:

2.1 The shareholders

The shareholders invest in a corporation in expectation of an acceptable return on investment (ROI), which is achieved within a framework of acceptable standards, moral and ethics. Shareholders require accurate information from the Board on these matters (King Report, 2002, p7).

2.2 The Board of Directors

The Board of Directors is, inter alia, responsible for:

a) applying the shareholders' investments to ensure a positive ROI. This must be achieved within a framework dependant on the information received from the shareholders with regard to standards, morals and ethics. The Board is responsible for creating a program for risk management, including information security, and is therefore directly accountable for the successful functioning of the information security system. The Board has therefore to report accurately, openly and promptly on these matters to their shareholders and relevant stakeholders (King Report, 2002, p 21).

b) creating a governance structure, which will achieve these ends (King Report, 2002, p 21).
c) the process of risk management, as well as deciding on the effectiveness of the process within the corporation (King Report, 2002, p 29).
d) ensuring compliance with all relevant laws, regulations and codes of good practice (King Report, 2002, p 21).

2.3 Chief Executive Officer

The CEO is the individual chosen for the full and proper enactment of the Board's directions, which he/she does by the judicious application of available funds to the chosen factors of production. He/she is also responsible for:

a) reporting progress back to the Board,
b) the oversight and co-ordination of policies,
c) compliance reporting, and
d) providing actions to ensure accountability (Business Software Alliance, 2003, pp 5-6).

2.4 Divisional Heads

The divisional heads are responsible for:

a) the optimum application of their allocated resources via the general employees,
b) reporting progress and deviation back to the CEO,
c) providing information security protection in line with risk and business impact,
d) providing security training and education to all employees responsible for, and
e) reporting on effectiveness of policies, procedures and practices (Business Software Alliance, 2003, p 6).

2.5 General Employees

The general employees are responsible for:

a) the proper execution of their allotted tasks, and
b) reporting to the divisional heads.

Thus, it can be seen that the primary relationships between the different levels within a corporation depend extensively on the flow of information. This information needs to be accurate, concise, valid and timeous, and needs to be adequately protected. Information security governance is based on a number of broad aspects. These aspects need to be addressed by the relevant parties to ensure that information security is implemented effectively and efficiently, thus protecting the corporation's valuable information assets.

3 BROAD ASPECTS RELATING TO INFORMATION SECURITY GOVERNANCE

Information security governance needs to be tailored to the needs of the individual business and industry in which it operates (Business Software Alliance, 2003, p 6). The following aspects have been identified from literature sources as being the main pillars on which information security governance rests, but there may be others due to the dynamic nature of information security (Institute of Internal Auditors, 2001).

3.1 Accountability and Responsibility

Accountability means that those individuals or groups in a corporation, who have the authority to make decisions, must also have responsibility and be accountable for their decisions and actions. Mechanisms to allow for accountability provide investors with the means to query and assess the actions of the Board and its committees. Responsibility pertains to the behaviour that allows for corrective action and for penalising mismanagement. While the Board is accountable to the company, it must act responsively to and with responsibility towards all stakeholders of the company (King Report, 2001, p 21). If management is aware of a specific risk, and chooses to ignore it (called the *ignorantia legis neminem excusat* principle), and it results in serious losses, then criminal liability could occur (Hinde, 2003a).

3.2 Ethics

The company's standards of ethical behaviour need to be structured and then should be translated into a corporate code of conduct. This could then be used to control the behaviour of employees and establish 'moral' codes for the company (Hinde, 2003b). The security of a corporation is only as strong as its weakest link, and this link, which is generally the employees, could put the corporation and its customers at risk, and therefore needs to be well managed and monitored. A code of ethics and conduct will facilitate responsible security awareness, as users will be personally responsible for ensuring sound security practices are implemented, which will lessen the security risks especially in an environment that is highly networked (Institute of Internal Auditors, 2001).

3.3 Security Awareness and Education

According to Jacqueline Wagner, Institute of Internal Auditors International Chairman and General Motors' General Auditor: "Effective information security must be pervasive. A security or controls group no longer owns the task. Security is everyone's job – it must be broad and touch every cubicle and office." (Institute of Internal Auditors, 2001).

Security awareness and education is vital to a corporation if it wishes to ensure that all the stakeholders embrace the 'culture of security' (Pounder, 2002). Corporations spend millions of rands on technology to improve their information security, but if the employees do not take responsibility for their own information security, then the technology will be of no use. Education of employees on an ongoing basis is essential to ensure that security awareness is always topmost in the minds of the employees. This will promote responsible use of computers within the corporation and will minimize the risk of unauthorised access and irresponsible behaviour.

The Board of Directors needs to support learning and growth by sustaining an adequate investment in staff education, development and training for IT operations, security and development.

3.4 Information Security Policies

Information security cannot be enforced if there is no mandate to do so. A corporate information security policy is the company's mandate and contains a series of baseline information countermeasures crucial to the corporation (von Solms, 2001b).

Information security policies are direction-giving documents that define the concepts of information security, and must have the commitment and support of the Board and top management to ensure its success. The Board must ensure that its information security policy is aligned with the corporation's business strategies. All relevant parties need to be given an opportunity to input into this document in order to ensure that there is a general ownership and therefore a commitment to information security from Board level downwards right through the corporation. Information security is only achieved through the combined input of users, owners, and security personnel. It also takes cognizance of the customers, partners, and other stakeholders (Institute of Internal Auditors, 2001).

3.5 Resource Allocation and Management in the IT Security Arena

Resource management and allocation includes optimizing knowledge and infrastructure. It includes people, applications, technology, facilities and data (IT Governance Institute, 2003). Often decisions on how information risks should be dealt with, are made by competent IT managers who are not involved in, or responsible for, the strategic management of the company. This can result in the purchase and deployment of information security technology that is inappropriate in the light of the real risks faced by the company (Business Software Alliance, 2003).

"The goal of resource management is to optimize the utilization of IT assets, lower the total cost of ownership, improve IT investment decisions and unlock the promise of computing by making knowledge resources more productive. Resource management is therefore a cornerstone of good IT governance." (InfoSec, 2001). Resource management and allocation could also include outsourcing, which in turn needs to be managed effectively and efficiently to ensure that it adds value to the corporation, and the corporation needs to ensure that the required level of security is maintained within the outside companies that have been recruited for outsourcing.

3.6 Best Practice Standards

Good examples of best practice documents include the ISO 17799 document, ISO 13335, and the Guidelines for the Security of Information Systems document by the Organisation for Economic Cooperation and Development (OECD). These documents can be seen as reference frameworks that corporations can implement to ensure that they are addressing most of their information security risks without necessarily going through a comprehensive risk analysis exercise (von Solms, 2001b).

Implementing a best practice standard ensures that the company can have the assurance that they are on a par with other international corporations who have implemented these best practice standards. One of the objectives behind BS 7799's idea of information security certification is to secure inter-organisational business trust, to evaluate the level of information security in that corporation, and to increase customer confidence and trust (von Solms, 2001b).

3.7 Risk Management, its Measurement and Control

In risk management, the first step is to know what the information security risks are and to actively manage these risks to keep them within acceptable levels according to the company's risk appetite (von Solms, 2003). Risk appetite is the level of risk that is acceptable, ignored, or managed by a company.

Roles and responsibilities for information security risk management need to be assigned to ensure accountability. Accepting that information security structures exist within the corporation, some form of deviation analysis needs to be in place to identify security breaches, and this analysis must contain executive level planning to counteract these deviances, and in so doing protect the corporation's information asset. This is an ongoing exercise that requires the highest level of commitment to ensure the minimization of both technical and non-technical risk.

3.8 Compliance with Legal Requirements

Standards for the compliance, review, monitoring and oversight functions must be incorporated into the overall security infrastructure to ensure that all legal requirements are met (Institute of Internal Auditors, 2001). Examples of legislation in South Africa governing information include the Electronic Communications and Transactions Act (ECT Act) of 2002, the Promotion of Access to Information Act, and the Regulation of Interception of Communications Act.

3.9 Information Sharing

Information sharing is important because the corporation can learn from the successes and failures of other corporations, which can significantly help in minimizing and managing risk for that corporation. This sharing can be achieved by interacting with industry groups, attending briefings, meetings and conferences, and working actively with regulatory bodies. Transparency and disclosure as far as failures in a company are concerned is important not only at Board level to shareholders, but could also aid peers in combating threats as they arise (Institute of Internal Auditors, 2001). This should be encouraged at industry level.

These broad aspects form the pillars upon which information security governance is built. To ensure that all these aspects are implemented adequately, pertinent questions need to be asked by the relevant levels of authority, and actions need to be instituted to ensure adequate answers to these questions are delivered.

4 PERTINENT QUESTIONS RELATING TO CORPORATE INFORMATION SECURITY GOVERNANCE

Modern corporate survival and growth depends mainly on the value and accuracy of the information used for decision-making. In today's business environment, the sheer volume of information required is such that only modern information technology (IT) is capable of coping with the requirements of the corporation. Corporate governance should therefore elevate IT security governance to the level of corporate information security governance. The following questions need to be asked by and of the corporate governance team, which includes the IT governance personnel, to ensure that all the broad aspects of information security governance are being addressed effectively and efficiently.

4.1 Accountability and Responsibility

- Who is responsible for information security?
- How are roles and responsibilities allocated to ensure a system of accountability?
- Is the Board regularly informed of major IT initiatives, their status and issues?
- Is IT a regular item on the agenda of the Board and is it addressed in a structured manner?

4.2 Ethics

- In what way can we ensure the ethical use of our information assets and administration of information security?
- Has a company code of conduct been implemented in this regard?

4.3 Security Awareness and Education

- How do we engender security awareness within the company and so ensure that everyone understands the importance of information security?
- Have strategies and goals been communicated effectively to everyone who needs to know, within the company?
- Does the corporation have and sustain an ongoing education program designed to promote information security awareness and responsibility at all levels?

4.4 Information Security Policies

- When developing our Information Security Policy, do we ensure that all the relevant parties are taken into account, and
- Have all stakeholders been identified, considered and informed of the roles and responsibilities required of them?
- Has a gap reporting system been implemented between the minimum level of controls and the actual level?
- Does the Board approve the information secur ity strategy?
- Has the Board taken ownership of the information security policy and do they actively encourage compliance?

4.5 Resource Allocation and Management in the IT Security Arena

- How do we ensure that our security investments are aligned with our risks?
- Does a mechanism exist which allows IT management to capitalise and act upon opportunities or shortcomings recognised?
- Have we identified the corporation's capital expenditure requirements in the area of information security (including IT security), in line with known and assumed risks?
- How well is IT security positioned to meet future needs and do we have the resources to meet the opportunities as they arise?

4.6 Best Practice Standards

- How do we ensure that effective measures are in place so that IT failures do not endanger the company, its ability to perform, its business units, customers, partners, nor its information assets?
- How do we match up with other companies with regard to information security?
- Should a best practice policy be instituted before we do business with other corporations?
- Can we trust other corporation's information?
- Do we need to comply with international standards and does this compliance warrant the expense?

4.7 Risk Management, its Measurement and Control

- Does a potential deviation analysis exist within the corporate structure and more specifically the IT environment?
- Have we ensured that information security is an integral part of all the corporation's policies?
- How far should the corporation go in risk mitigation and does the cost justify the benefits?
- What is the potential economic impact if we are attacked and our systems fail in terms of lost revenue and investor confidence and relationships?

- ♦ Have responsibilities for risk management been allocated to the proper levels of authority within the corporation to ensure adequate levels of accountability?
- ♦ How can we ensure that all users comply with the corporation's security policies?
- ♦ Does the corporation know how many attacks were made on it during the year?
- ♦ What IT risks should be accepted or transferred?
- ♦ Are the operating results communicated to the Board of Directors in such a manner as to ensure clarity of information in order to minimize the potential for incorrect decision making, without requiring detailed technical knowledge.

4.8 Compliance with Legal Requirements

- ♦ How do we ensure that all our information security measures are compliant with the legal regulations of the country?
- ♦ Are we up to date with the new legal requirements?
- ♦ Are our employees aware of their rights and responsibilities, and educated on an ongoing basis to ensure security awareness and compliance with the policies as instituted by the corporation?

4.9 Information Sharing

- ♦ Do we share information with our peers and governmental entities to enable us to learn from each other's successes and failures, and thus minimize and manage risk more effectively?
- ♦ Do infrastructures exist that will facilitate and support the creation and sharing of vital business information without the loss of competitive advantage?

5 Conclusion

Information security governance is of vital importance to a corporation. Information security needs to be taken seriously not only by the IT department, but also by the Board and senior management, to ensure that the information asset is adequately protected. A definite responsibility and reporting structure needs to exist between the different levels of authority within the corporation. Specific aspects exist that need to be addressed to ensure holistic Information Security Governance. Specific questions need to be asked by the Board and senior management, and adequate answers need to be provided by the organization. Typical answers and reporting mechanisms still need to be researched.

References

Business Software Alliance. (2003). *Information Security Governance: Toward a Framework for Action*. Retrieved March 15, 2003 from the Internet: URL http://www/bsa.org.

Hinde, S. (2003a). *The law, cybercrime, risk assessment and cyber protection.* Computers and Security, 22(2): pp. 91-95.

Hinde, S. (2003b). *It was Déjà vu all Over Again.* Computers and Security, 21(3): pp. 214-216.

Institute of Internal Auditors. (2001). *Information Security Governance: What Directors Need to Know*. Retrieved March 07, 2004 from the Internet: URL http://www.ciao.gov.

InfoSec. (2003). *Executive Summary*. Retrieved March 11, 2004 from the Internet: URL http://www.infosec.co.za.

IT Governance Institute. (2003). *Board Briefing on IT Governance Second Edition.* Retrieved March 06, 2004 from Internet: URL http://www.cisecurity.org/Documents/26904_Board_Briefing_final.pdf.

King Committee on Corporate Governance. (2001). *King report on corporate governance for South Africa 2001.* Available from Internet: URL http://www.iodsa.co.za/IoD%20Draft%20King%20Report.pdf.

Pounder, C. (2002). *Security policy update*. Comp uters and Security, 21(7): pp. 620-623.

Von Solms, B. (2001a). *Corporate Governance and Information Security*. Computers and Security, 20: pp. 215-218.

Von Solms, B. (2001b). *Information Security – A Multidimensional Discipline.* Computers and Security, 20: pp. 504-508.

Von Solms, B. (2003). *Governance, Risk & Ethics, Module 7: Information Technology Governance and Risks.* Financial Mail.